IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Computing in the Perspective of Ulrich Beck's Theory of Risk: An Exploratory Discourse

SOMPURNA BHADRA

PhD scholar, Department of Computer Science and Engineering

Techno India University

Kolkata, West Bengal- 700091

ABSTRACT:

In the elaboration of his discourse on the development of risk society form the 1980s, Beck's theoretical and methodological argument is that the 'risk calculus' links the natural, technical and social sciences. It can be applied as much to highly diverse phenomena in public health – from the risk of smoking to the risk posed by nuclear power stations – as to economic risks, risks of unemployment, of traffic accidents, of ageing, and so forth'. It has been approvingly emphasized by Rosa who says that the 'the risk field is an inherently interdisciplinary activity', and in this one needs to acknowledge 'the central role of the social sciences' in deciphering the nature and different dimensions of risk. Against this backdrop, the present paper offers a preliminary/exploratory examination of Cloud computing in the context of Beckian thesis of risk society. Although a comparative assessment between the two sets of risks in two contrasting fields is long overdue, the instant paper is in a way an offshoot of, and motivated by, the unanticipated outburst of COVID-19 pandemic which is of local origin but of global consequences. It only attests to the fact that, as Arias-Maldonado puts it, 'there is risk where there is not yet enough knowledge' –a message that Beck conveys in his formulations of the emergence of late-modern industrial risk society due the dynamic and autonomous process of modernization since the last few decades of the twentieth century. This comparative, interdisciplinary and exploratory discourse on the risks of Cloud computing and late modern industrial society points to the preliminary conclusion that Cloud computing risks as a sub-set of a whole series of risks that pervade and are perceivable both objectively (materially) and subjectively (socio-culturally) in today's risk society.

Keyword: Risk, Cloud Computing, Risk Society, Covid-19

I. INTRODUCTION

'Risk is everywhere. ... Risk need not be harmful, however, and is not always a burden. In many cases, people hoping to improve their standards of living may voluntarily take on risk. Indeed, risk taking is essential to the pursuit of opportunity. But those opportunities may bring their own risks. ... An enterprise that upgrades to more advanced technologies to enhance its profitability may also become more indebted and financially vulnerable. ...As the world changes, new opportunities and possibilities, as well as risks and complications, continually arise. Rejecting or ignoring change can lead to stagnation and impoverishment. In contrast, embracing change and proactively dealing with risks can open the way to sustained progress. Risk management should therefore be a central concern at all levels of society. By improving resilience, risk management has the potential to bring about a sense of security and the means for people in developing countries and beyond to achieve progress' [1].

Indeed, risk is everywhere. It is also more than that. It has not only been part of human existence at all times and risk research began, in a way, when humans started to circumvent dangers to the possibility of physical harm in general and death in particular. While systematic and scientific study of risk of society and the emergence of risk professionals are of recent origin, it is no less interesting to note that the mathematical tools for risk assessment developed more than a century earlier than when actual risk analysis on technical systems was carried out. And, risks, which refer to " the *possibility that human actions or events lead to consequences that affect aspects of what humans value*', continues to persist and pervade humans and societies due to, *inter alia*, increasing complexity of technologies and associated social institutions, in almost remarkable succession [2]. Britain's first nuclear reactor, Windscale (1957), the Thalidomide tragedy (1962), Three Mile Island nuclear accident (1979), Bhopal (1984), Chernobyl (1986), the Challenger space Shuttle(1986), the Exxon Valdez oil spill in 1989, the arsenic poisoning of people a year in Bangladesh from the early 1990s onwards and more recent pharmaceutical, nuclear, nutritional, and space-related catastrophes such as the arthritis drug Vioxx in 2004, the Tokaimura chain reaction in 1999, the BSE outbreak from 1986 to 1996, and the Columbia space shuttle in 2003, Fukushima Daiichi nuclear disaster (2011) are events that point to, as Taylor-Goodby and Zinn may poignantly remind, how 'risk has accompanied technical development and revealed the weaknesses of institutions for managing the resulting uncertainty' [3]. In this digital epoch, cyber risks including Cloud computing risks, are ubiquitous because the omnipresent Internet technology along with the widespread use of Windows, Mac OS, iOS and Android operating systems are so entrenched in the information and communication domains that it is hardly possible to enter into 'a new 'Clean Slate Internet'

that includes all the security measurements that we are currently lacking'. It is only transparent and obvious that technologies can not only offer new opportunities but also, more importantly, bring down and ruin a business concern with a targeted DDoS attack. Numerous security vulnerabilities in the software and hardware used today can be easily be exploited by any attacker from any location, without getting caught. Under the circumstances, 'the risk of becoming the victim of malicious cybercriminals and unscrupulous competitors has grown especially dramatically in recent years. A new awareness of the risks is needed in order to hold one's ground against these new threats' [4]. Postman states in a straight forward manner that technological innovations are not a one-dimensional phenomenon. Technology is double-sided. It is both 'friend and enemy' or both a 'burden and a blessing'. It is 'not either-or, but this-and that' [5]. Mishra is quite explicit in characterizing the inherent nature of technology: 'Almost every new technology developed has brought great benefits attached with some risks. To each 'technology', there is an 'antitechnology', making it a double edged weapon. But whatever be the risks, the progress just carries on, and new methods are found to tackle the risks. The phenomenal growth of computer and communication technologies, or ICT, is no exception and the main risk it has brought along with its benefits is that it has provided terrorist organizations great advantage in their nefarious activities' [6]. However, the paradox is that 'people do not accept risks, but technologies, one of whose significant features may be their risk' [7]. A very popular example of this is the acceptance of car as a technological convenience, but the fact is that it is associated many risks that are not acceptable as such. The following Table 1 shows both benefits and risks of owning a car [8].

Risks associated with owning a car	
Opportunities of owning a car (events you hope will happen, but could fail to occur)	
1	You can travel more easily than depending on others
2	Enhanced job opportunities because you will be more mobile
3	Save money on other forms of public transport
Uncertainties of owning a car (events that you know will happen, but impacts are variable)	
1	Cost of borrowing money to buy the car could change
2	Price of fuel (petrol or diesel) could go up or down
3	Maintenance, breakdown and repair costs will vary
Hazards of owning a car (events that you do not want to happen and that can only be negative)	
1	You pay too much for the car or it is in poor condition
2	You are involved in a collision or road accident
3	The car gets stolen or vindictively damaged
Compliance requirements of owning a car (events that could result in regulatory enforcement)	
1	Insufficient and/or inadequate third-party car insurance
2	Inattentive or aggressive driving results in traffic offence(s)
3	Tyres in poor condition and other maintenance obligations

Table 1: Risks Related to Owning a Car

Virilio, while characterizing the nature and character of technology, argues persuasively that 'every technology produces, provokes, programs a specific accident. For example: 'when they invented the railroad, what did they invent? An object that allowed you to go fast, which allowed you to progress-a vision à la Jules Verne, positivism, evolutionism. But at the same time they invented the railway catastrophe. The invention of the boat was the invention of shipwrecks. The invention of the steam engine and the locomotive was the invention of derailments. The invention of the highway was the invention of three hundred cars colliding in five minutes. The invention of the airplane was the invention of the plane crash. I believe that from now on, if we wish to continue with technology (and I don't think there will be a neolithic regression), we must think about both the substance and the accident-substance being both the object and its accident' [9]. The truth of the matter is that, as implicit in the above, technologies are always of dual use, and they can bestow great benefits while, simultaneously 'imposing grave risks ranging from malicious use to exacerbating socioeconomic inequalities' [10]. Cloud Computing is based on the internet which itself is an example of a technology with dual use and as such it has potential and real risks as a new technology which is characterized by three features: 1. Complexity as a product of 'many variables with unknown or unknowable consequences'; 2. Uncertainty**,** that is, 'inability to produce usable risk versus benefit assessments; and 3. Ambiguity often involving 'conflicts over ethical and professional values' [11].

In fact the risks are as old as the society itself. Human beings confronted different types of danger since the time immemorial from floods, earthquakes, volcanic eruptions, diseases, hunting, working, leisure activities, traffic accidents, technological hazards like electricity, dams, cars, chemical factories, and so on and so forth [12]. The most recent example of risk (health and epidemiological) is the novel Coronavirus disease (COVID-19)-- SARS-CoV-2--first reported on 31 December 2019 in the Wuhan, Hubei Province, China and its exponential escalation signified 'a perfect epidemiological storm' [13] and created 'a calamitous situation throughout the world' [14]. It was a risk, though not totally in Beckian sense because it was not human-manufactured by science and technology [344]. In any case, consequences of this in the global society are multidimensional and created what may a called a 'culture of fear' all around when 'when shaking hands becomes a risk' [15] or 'touch me not' becomes new normal, putting everyone in the 'same boat' [16] but staying 'away from each other' [17]. Knorr quips, 'despite all our progress and technology over recent centuries, we are still susceptible to the tiniest of things—a virus. In fact, because of our technology, we might be even more vulnerable'18]. Some relevant examples in the context of this paper can be cited by way of introducing themes of the paper. Tables 2 and 3 illustrate the **evolving** Global Risks Landscape, 2015–2020 [19]. What should be

noted in both Tables 2 and 3 is the cyber security issues are at the top of global risks in terms of likelihood, along with other issues relating to climate. Figure 1 shows the responses of 341 of survey conducted by *World Economic Forum* concerning how they rank the likelihood of major risks in the aftermath of the pandemic Covid-19 for the next 18 months. It points to 31 risks classified into five categories: (1) Economic: 10 risks; (2) Societal: 9 risks; (3) Geopolitical: 6 risks; Technological: 4 risks; and

Top 5 Global Risks in Terms of Likelihood						
	2015	2016	2017	2018	2019	2020
1st	Interstate Conflict	Involuntary Migration	Extreme Weather	Extreme Weather	Extreme Weather	Extreme Weather
2nd	Extreme Weather	Extreme Weather	Involuntary Migration	Natural Disasters	Climate Action Failure	Climate Action Failure
3rd	Failure of National Governance	Climate Action Failure	Natural Disasters	Cyberattacks	Natural Disasters	Natural Disasters
4th	State Collapse or Crisis	Interstate Conflict	Terrorist Attacks	Data Fraud or Theft	Data Fraud or Theft	Biodiversity Loss
5th	Unemployment	Natural Catastrophes	Data Fraud or Theft	Climate ActionFailure	Cyberattacks	Human-Made Environmental Disasters

Table2: Top Global Risks 2015-2020

Top 5 Global Risks in Terms of Impact						
	2015	2016	2017	2018	2019	2020
1st	Water Crisis	Climate Action Failure	Weapons Of Mass Destruction	Weapons Of Mass Destruction	Weapons Of Mass Destruction	Climate Action Failure
2nd	Infectious Diseases	Weapons of Mass Destruction	Extreme Weather	Extreme Weather	Climate Action Failure	Weapons of Mass Destruction
3rd	Weapons of Mass Destruction	Water Crisis	Water Crisis	Natural Disasters	Extreme Weather	Biodiversity Loss
4th	Interstate Conflict	Involuntary Migration	Natural Disasters	Climate Action Failure	Water Crisis	Extreme Weather
5th	Climate Action Failture	Energy Price Shock	Climate Action Failure	Water Crisis	Natural Disasters	Water Crisis

Table 3: Impact of Top Global Risks 2015-2020

(5) Environmental: 2 risks. Technological risks are as follows (1) Cyberattacks and Data fraud due to sustained shift in works patterns (37.8%) in 9th rank; (2) Additional unemployment from accelerated workforce automation (24.8%) in 11th rank; (3) abrupt adoption as follows (1) Cyberattacks and Data fraud due to sustained shift in works patterns (37.8%) in 9th rank; (2) additional unemployment from accelerated workforce automation (24.8%), in 11th rank; (3) abrupt adoption and regulation of technologies , i.e., e-voting, telemedicine, and surveillance (38%8); and (4) breakdown of IT infrastructure and networks (6.9%) [20].

How does Covid -19 affect the business enterprises? The following Table 4, illustrating the most important global risks, is based on the insight of 2,718 risk management experts from 102 countries and The *Allianz Report* (2020) points out that cyber incidents ranks as the most important business risk for companies globally after receiving 39% of responses from risk management experts-- the largest number of respondents ever. Seven years ago in 2013 cyber risks enjoyed only 15th rank with just 6% of experts' responses. It goes on to say that 'Businesses face a growing number of cyber challenges including larger and more expensive data breaches, an increase in ransomware and business email compromise (spoofing) incidents, as well as the prospect of litigation after an event. Political differences between nation states being played out in cyber space brings added risk complexity, while even a successful merger or acquisition (M&A) can result in systems problems'. The main causes of cyber incidents are three in number: 1 Data or security breach (e.g., access to/ deletion of personal/confidential information) amounted to 77% of all cyber incidents.2. Espionage, hacker attack, ransomeware, and denial of service totaled 63% of those incidents. 3. Forty-two percent (42%) incidents were due to the errors or mistakes committed by the employees. The *Report* also outlines the trends in cyber incidents. First, data breaches are becoming larger and more expensive. Second, business email compromise (BEC) – or spoofing – attacks are becoming more frequent and also more expensive. Third, the ransomware threat, the most prominent cyber crime, is becoming more damaging, and is increasingly targeting big companies with sophisticated attacks and making large extortion demands. Fourth, litigations are rising because more consumers, business partners and investors are being affected and dragged into litigation in view of increasing cyber attacks. Finally, mergers and acquisitions (M&A) have exposed the companies to greater cyber attacks. Sixth, political factors are assuming increasing role in launching cyber attacks. 'The involvement of nation states in cyber-attacks is increasing risk for companies, which are being targeted for intellectual property or by groups intent on causing disruption or physical damage' [21].

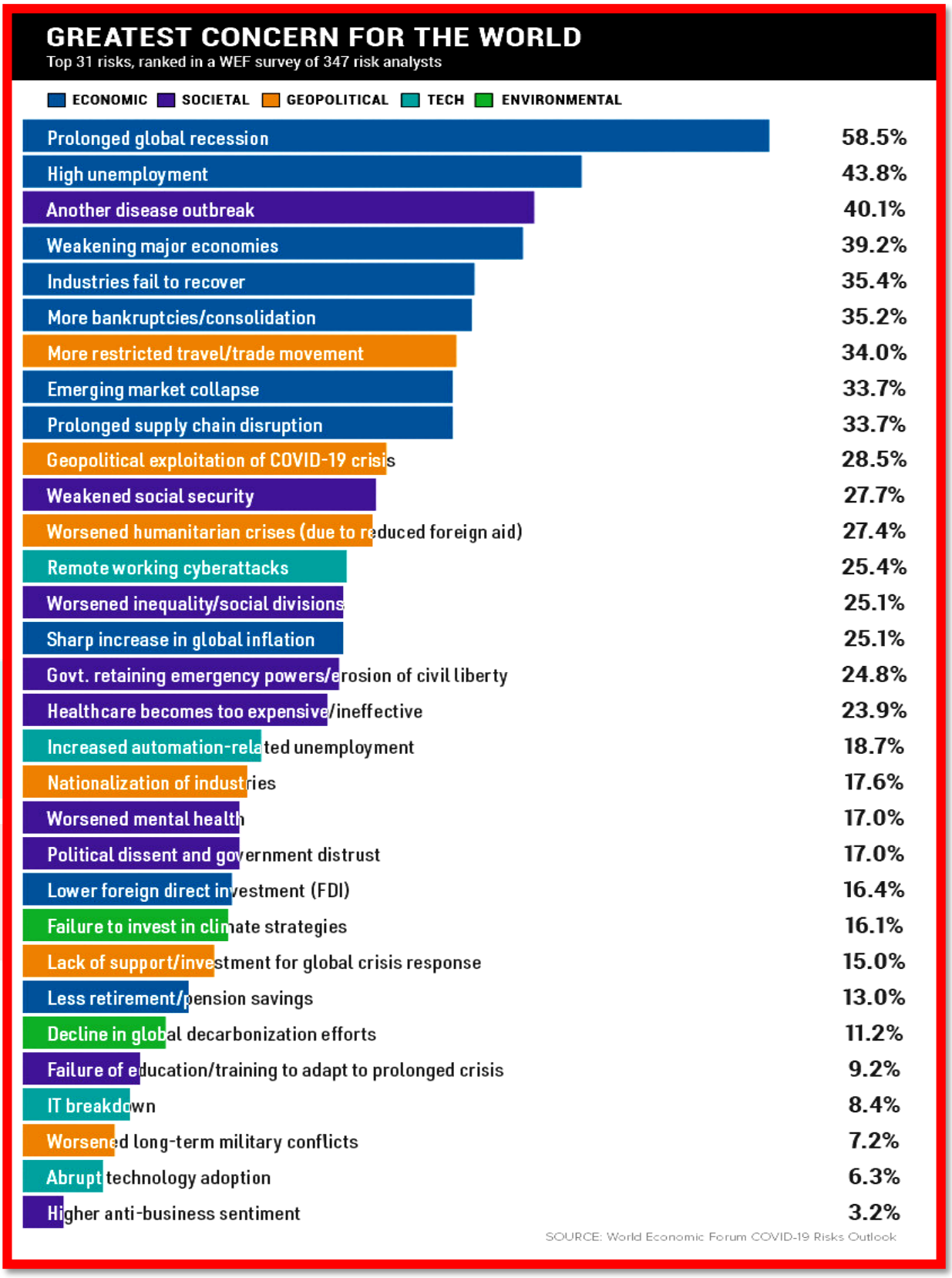


Figure 1: The greatest concern for the world from COVID-19

Gartner recently drew attention to the top ten (10) "emerging risks" in its report. It surveyed 131 senior executives across most industries and geographies regarding the top concerns facing their businesses during the third quarter of 2020. It says that 'the "second wave" of COVID-19 topped executives' concerns for a second consecutive quarter, with the majority of the top 10

Rank	Global Business Risks 2020	Percent	2019 rank	Trend
1	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	39%	2 (37%)	^
2	Business interruption (incl. supply chain disruption)	37%	1 (37%)	v
3	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	27%	4 (27%)	^
4	Natural catastrophes (e.g. storm, flood, earthquake)[1]	21%	3 (28%)	v
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	21%	5 (23%)	=
6	Fire, explosion	20%	6 (19%)	=
7	Climate change/increasing volatility of weather	17%	8 (13%)	^
8	Loss of reputation or brand value	15%	9 (13%)	^
9	New technologies (e.g. impact of artificial intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)	13%	7 (19%)	v
10	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	11%	13 (8%)	^
11	Political risks and violence (e.g. geopolitical conflict, war, terrorism, civil commotion)[2]	9%	11 (9%)	=
12	Shortage of skilled workforce	9%	10 (9%)	v
13	Critical infrastructure blackouts (e.g. disruption of power)[3]	8%	17 (2%)	^
14	Product recall, quality management, serial defects	8%	12 (9%)	v
15	Theft, fraud, corruption[4]	7%	15 (7%)	=
16	Environmental risks (e.g. pollution)	7%	14 (7%)	v
17	Health issues (e.g. pandemic outbreak)	3%	16 (3%)	v
	Other	3%		

Table 4: Most Important Global Business Risks, 2020

^Risk higher than in 2019; vRisk lower than in 2019; = No change from 2019; (1) 2019 risk ranking

Note: 1. Natural catastrophes ranks higher than market developments based on the actual number of responses
2. Political risks and violence ranks higher than shortage of skilled workforce based on the actual number of responses
3. Critical infrastructure blackouts ranks higher than product recall based on the actual number of responses
4. Theft, fraud and corruption ranks higher than environmental risks based on the actual number of responses

emerging risks having 'a direct connection to the pandemic and the response to it'. The second top concern relates to the emergence of 'the new working model' whereby the enterprises are struggling to return to the traditional pattern of work organization pattern because of the need for social distancing, augmented work schedules and accompanying workplace transformation. The third emerging risk is the remote talent management because of a hybrid remote work/in-office workforce will tend to accentuate 'talent management and resource allocation issues. The emerging risks were ranked with highest impact and velocity' [22] [23]. In this connection it needs to be remembered that the concept of emerging risk is an important category which can hardly be ignored in the risk discourse. These risks are newly arising or changing whose potential damaging or whose implications and consequences are not reliably known and thus they cannot be managed by the traditional methods. Carpenter says that 'emerging risks can be new and unforeseen risks whose potential for harm or loss is not fully known. In looking at the universe of emerging risks it becomes increasingly clear that a significant portion are by their nature not observable by traditional methods, even though their impact will no doubt at some point be felt'. However, improved understanding emerging risks should be viewed as an opportunity but not as a threat because 'ultimately, greater knowledge will mean these are, by definition, no longer emerging risks, any more than aviation risks are now' [24]. The examples merging risks are climate changes, natural catastrophes, Pandemic, terrorism, impact of government regulation, etc. [25].

What is the role of Covid-19 in respect of generating the emerging risks for the business organizations? The IT has now taken on a central place in operations such as healthcare, business, education, governance, judiciary, community service, and so on. The Table 5 also shows not only how society changes with the hitherto unknown risk but also how technology, IT specifically, plays a positive role in the adaptation of the society to the challenges posed by this risk. In doing so, the covid-19 pandemic has offered new opportunities by exposing both 'weaknesses and vulnerabilities of IT systems and IT planning and implementation' and presented at the same time quite a few challenges to the IT industry, professionals, government, and non-government organizations and also concerned individuals [26]. Figure 2 shows how the covid-19 is affecting the humans both socially and technologically [27].

Having introduced the contemporary relevance of risk in the society, the analysis of the issues raised in the instant paper is as follows. The section II discusses briefly different generic dimensions of cloud computing. The focus in section III is on the analysis of risks and their multidimensional facets. In section IV an interpretative discourse on Ulrich Beck's theory of risk is undertaken in order to characterize the different aspects of risk theoretical framework as a backdrop for reviewing the Cloud computing technology in terms of risk analysis. Thus, the focus of section V is on risk analysis of cloud computing in the light of risk management and risk assessment issues along with their related dimensions. The final section VI contains concluding remarks to the effect that while risk theory is macro perspective, cloud computing falls as a micro-perspective within the overarching macro-perspective of risk theoretical canvas. In so far as conceptual, theoretical and methodological dimensions of the present study are concerned, the current paper is engaged in what is called risk research perspective. Risk research, which is essentially multidisciplinary in its study of risk, has been defined as the 'the multidisciplinary study of risk, addressing topics such as how risks should be analyzed and assessed, how they are perceived and understood, and how they are and should be communicated and managed' [28]. In this regard, the main task of the researcher to emphasize 'the necessity of integrated risk assessment and the development of innovative risk management strategies that build upon the insights of the natural, technical and social sciences' [29]. The present research is thus, in its conceptual and theoretical aspects, interdisciplinary in nature and is based on current literature and printed publications. Methodologically speaking, this kind of research work is known as exploratory study. Its scope is as follows: "Exploratory studies consist of collecting, analyzing, and interpreting observations about known designs, systems, or models, or about abstract theories or subjects. These studies are largely an inductive process to gain understanding. ... Exploratory studies observe specific phenomena to look for patterns and arrive at a general theory of behaviour. The emphasis is on evaluation or analysis of data, not on creating new designs or models. The emphasis is on perspective and relative importance' [30].

II. CLOUD COMPUTING: AN OUTLINE OF ITS GENERIC DIMENSIONS

In the recent decades Cloud computing has brought about remarkable changes in the computing environment. Because cloud computing enables individuals and organizations to avail its services on demand at a lesser capital and operational expenses, there is little reason to doubt why the growth of cloud computing is becoming progressively exponential. The noticeable trend is that more and more companies, individuals and even government sectors are adopting Cloud computing for the advantages (viz. rapid scalability, ease of development, unlimited storage, and ubiquitous accessibility, etc) it offers to its consumers' [31]. Cloud computing can offer on demand computing services such as hardware ,viz., storage, servers and networking as well as software, viz., 'databases, applications and analytics' [32]. It is therefore no surprise that Cloud computing has become one of 'the most transformative computing technologies' that flourished in the wake of the rise of other technologies such as main-frames, minicomputers, personal computers, the World Wide Web, and smartphones. Montasari is not far off the mark when he remarks that 'Cloud computing is drastically transforming the way in which information technology services are created, delivered, accessed, and managed' [33]. While the main purposes of using Cloud computing are to maintain data and get applications, there is no unanimity on the definition of cloud computing, its characteristics, threats, vulnerabilities or risks among the concerned researchers [34].

Vaquero and others propose that 'Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs. On the other hand, looking for the minimum common denominator would lead us to no definition as no single feature is proposed by all definitions. The set of features that most closely resemble this minimum definition would be scalability, pay-per-use utility model and virtualization' [35]. The NIST defines cloud computing as 'a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'. Five characteristics are On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service [36]. Reviewing recent definitions of Cloud Computing, Elazhary recently offers a more comprehensive definition: 'Cloud computing is a computing paradigm for providing anything as a service such that the services are virtualized, pooled, shared, and can be provisioned and released rapidly with minimal management effort. For the users, the services can be accessed conveniently, ubiquitously, across the network, dynamically, and on demand; can be configured with minimal interaction with the service provider; and are elastic and metered on a pay-per-use basis' [37].

According to Sharma, the most common benefits of adopting cloud computing are (1) drop of information communication technology (ICT) costs; (2) the shift of IT costs from capital expenditure (capex) to operating expenditure (opex); (3) Scalability and adaptability; (4) faster time to market for organizations and their products or services; (5) easier management (e.g., time efficiencies, automation, outsourcing of tasks); (6) reduction of costs; (7) performance; and (8) high availability and disaster recovery options. According to Cisco Global Cloud Index 2016–2021, Global Cloud Workloads Surpass Traditional Workloads in millions is poised to surpass traditional workloads. Between 2016 and 2021 cloud data center workloads increased from 83% to 94%, whereas traditional data center workloads decreased from 17% to 6% [38]. According to the same source, the share of the

Global Impacts of Covid-19 and Uses of Technology				
No	Industry	Response/Impact	Response	Underlying Technology/ Operation
1	Education	Widespread closure of educational institutions; access to labs is restricted; projects have been mothballed; and fieldwork interrupted	Virtual learning environment (online teaching, presentation, assessment, and consultation); convocation online	Online video conferencing software, virtual labs on cloud
2	Healthcare	Overcrowded hospitals, inability to meet the demands on them	Contact tracing, forecasting resource requirements, allotment of scare resources based on a patient's survivability, COVID-19 vaccine development, telehealth (online consultation with a doctor or medical professional); automated diagnosis	AI, ML, cloud computing, chatbot
3	Business	Closure of business, avoidance of in-person retail shopping	Adherence to social distancing, services online, work from home	Chatbot, drone delivery, online meeting software, virtual office/desktop, remote access to work
4	Industry	Closure of some industries	Work from home, remote operations, automation and autonomous operation	Robots, automation, 3-D printing
5	Retail	Stores closed, only online service, avoidance of retail shopping	Online shopping, home delivery	The Web, online payment, contactless payment
6	Government	Spike in demands from citizens for assistance, disruption to normal operations	Migration to online services	Cloud, the Web, online meeting application
7	Entertainment	Entertainment venues (parks, cinema) closed, sports without spectators	Viewing online	Audio and video streaming, virtual reality
8	Personal life and social interaction	Lockdown	Indoor activities	Phone, audio and video chats, streaming, online gaming
9	Spirituality and religious practices	Places of worship closed	Online participation, prayers from home, worship through live stream	Audio and video streaming, virtual reality
10	Conferences	In-person conferences banned; virtual conferences	Online presentation and discussion	Video streaming, virtual conference software

Table 5: Global Transformations Caused by the Coronavirus

pubic cloud will be 56% in comparison with 44% of private cloud by 2019. By the same year the shares of the cloud service delivery models are 59% for SaaS, 11% for PaaS, and 30% for IaaS. The global cloud traffic is predicted to grow from 2.1 ZB (Zettabyte) per year to 8.6% ZB per year [39]. The Figure 3 shows the report of RightScale in respect of responses concerning the benefits of cloud computing shared across organizations and countries. It clearly points out that the benefits of faster access to infrastructure, greater scalability (e.g., compute and storage capacity), higher availability (e.g., uptime of services and applications), and faster time to market (e.g., application development, speedier product or service development accelerated by cloud computing) are ranked as the top four essential benefits of cloud' [38].

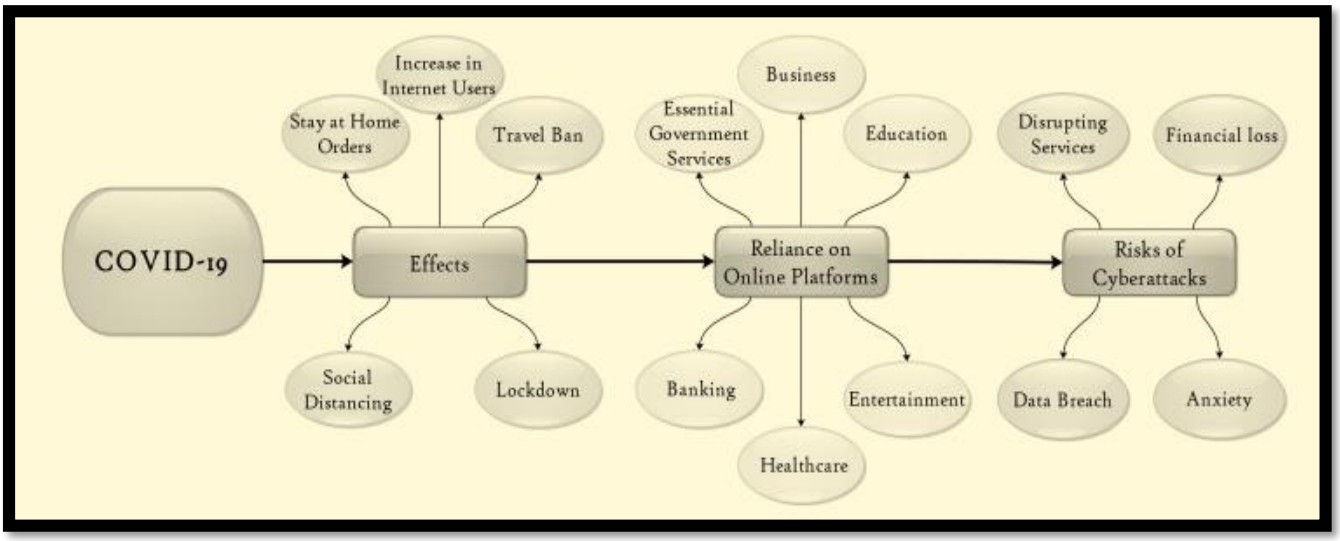


Figure 2: Effects of Covid-19 Pandemic

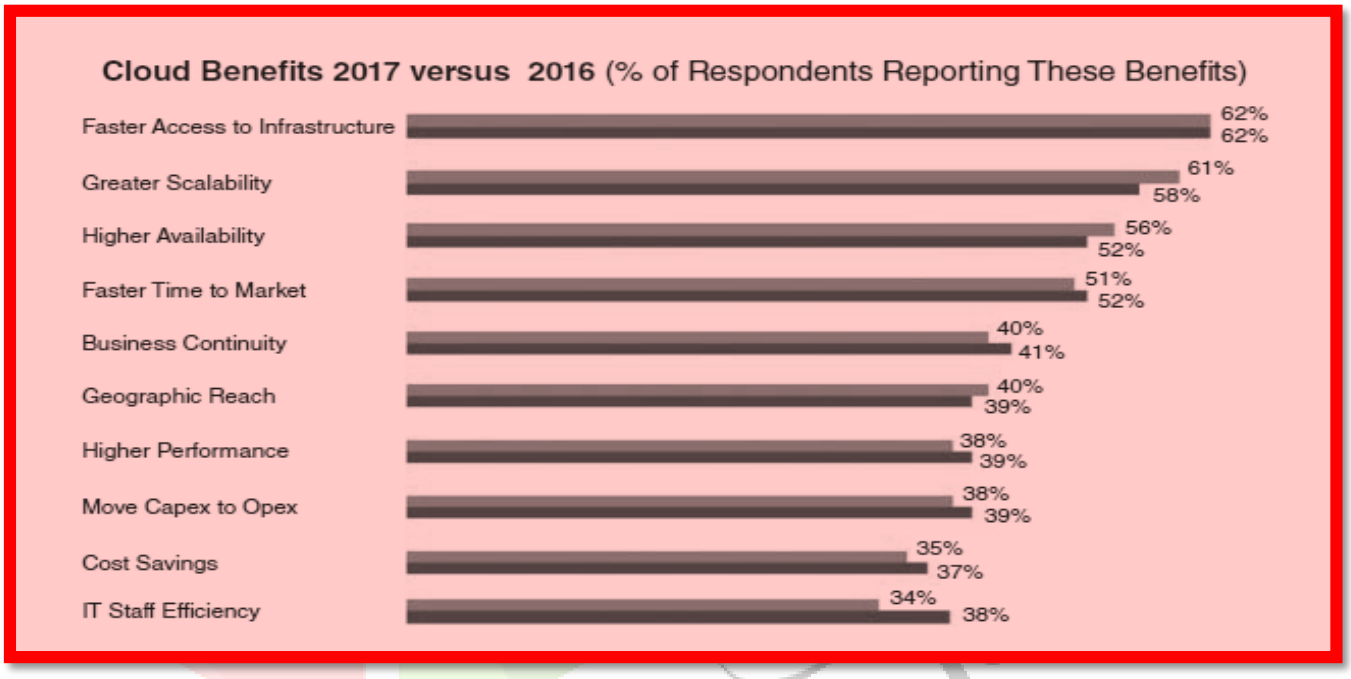


Figure 3: Cloud Computing Benefits

Cloud Service models are of three types: Software as a Service (SaaS), Infrastructure as a Service (IaaS)) and Platform as a Service(PaaS). Their main features may be briefly described. Software as a service offers an application that is equipped with all necessary hardware, software, operating system and network. SaaS can be accessed over the internet by consumers anywhere regardless of their geographical location. It is the most advanced among the cloud service models. The cloud providers take on management and responsibilities for the IaaS services and hence the consumers can use the application without worrying about deployment or management of the underlying infrastructure or the application. The cloud provider takes care of the application maintenance and updates. Some example of IaaS providers are Amazon EC2, Google's Compute Engine (GCE), Microsoft Azure, Dorpbox etc. Some examples of SaaS services are 'Email & Office Productivity, Content Management, Document Management, Collaboration, Sales, Financial, ERP, Billing, Human Resources, Social Networks' [40] [38] [41]. Platform as a Service is sometimes called 'middleware', because it conceptually sits between SaaS and IaaS. It is mainly a developmental platform which offers developers' requirements such as 'software tools, libraries, programming languages' and also services by which consumers can develop, install, test or organize the different applications for their own software and applications for business ends, for instance. The cloud applications are then transferred to the consumers through the internet. In a way, it is like the IaaS since it allows self-service of resources by the consumers. Examples of PaaS providers include Google AppEngin, Microsoft Azure etc. Some examples of PaaS services are 'Application Deployment, Database, Development & Testing, Integration, Business Intelligence' [40] [38] [41]. Infrastructure as Service puts forward numerous capabilities to the consumers such as processing, servers, storage, networks, along with virtualization technology with which they can deploy and run their operating systems and applications. In other words, IaaS delivers physical resources such as CPU, storage, memory, etc. in terms of virtualized resources like virtual machines which possesses computing capability to perform certain operations according to the user requirements. The IaaS model is basically pre-figured hardware resources that are delivered by the provider to the consumer via virtual interface. That is, it is essentially a virtual provision of computing resources in the cloud platform Hence, the consumer has control only over operating system, storage, and deployed applications but has no control and management over the concerned physical infrastructure. The example of IaaS providers are Amazon EC2, IBM SoftLayer, Google's Compute

Engine (GCE), GoGrid etc. The examples of IaaS services are 'Backup & Recovery, Compute, Storage, Platform Hosting, Services Management, Content Delivery Network (CDN)' [40] [42] [43] [41]. The following Figure 4 shows the extent of controls over the cloud service models by the customers or providers [44].

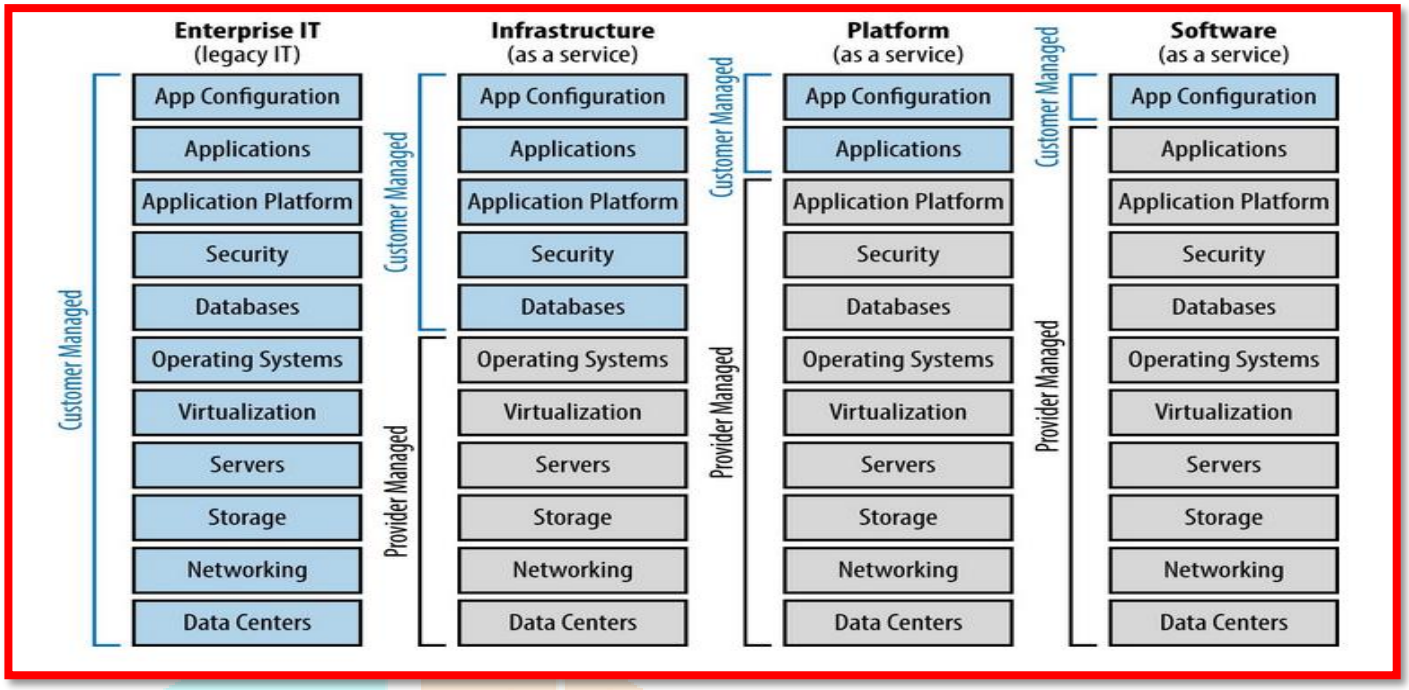


Figure 4: Cloud service models

Cloud computing has four different types of cloud deployment, and each type has its own rationale for deployment. Each deployment model is defined in terms of where the infrastructure for the deployment resides and who controls this infrastructure. It then becomes a matter of deciding the right deployment model – a decision which satisfies the specific tasks or goals of the concerned organization. 'Perhaps even more important is the fact that each cloud deployment model has a different value proposition and different costs associated with it [45]. NIST identifies four cloud deployment models: Private cloud, Public cloud, Hybrid cloud and Community cloud. Private Cloud offers a secure cloud environment which can be completely operated, managed and maintained only by a specific consumer - an in organization or an individual. It permits only the authorized users who have direct control over the data [46]. Public Cloud is deployed by service providers over a public network (wireless or wireline) and its services can be accessed by any pubic user who pays for its services. Public cloud is a cost-effective way to organize IT solutions and it involves applications such as customer relationship management (CRM), messaging and office productivity services. Public cloud providers include Google APP Engine, Amazon AWS, Microsoft Azure and IBM Blue Cloud [41] [47] [43]. In a Community cloud, the cloud is shared by multiple organizations that have a common interests or goals such as shared objectives, security, privacy or compliance policy. It has benefits, viz., sharing the cost to purchase of the infrastructure, multitenancy helping to take advantage of some economies of scale, and allowing the organizations to share support and maintenance activities [41] [45]. Hybrid cloud is usually a mixture of two or more cloud deployment models (private, public or community) which interoperates. The advantage of this cloud deployment model is that combined clouds are connected together enabling transfer of data and application without affecting partnering organizations [43] [40]. Figure 5 below shows cloud deployment models [38]. To sum up the brief outline of Cloud Computing in the words of Montasari, who is not far wide off the mark when he remarks that 'Cloud computing is drastically transforming the way in which information technology services are created, delivered, accessed, and managed'[48].

III. ANALYSING RISKS AND ITS MUTLIDIMENSIONAL FACETS

III. I. DEFINING RISKS

In appreciation of the receipt of the Distinguished Award from the *Society for Risk Analysis* in 1996 Stan Kaplan acknowledged the fact that the Committee set up by the Society laboured in vain for 4 years to define the word of 'risk' and consequently gave up the task, as Rausand and Haugen report, 'saying in its final report, that maybe it's better not to define risk. Let each author define it in his own way, only please each should explain clearly what way that is define it in his own way, only please each should explain clearly what way that is' . The problem of defining the concept of risk is surely intractable in point of fact since different disciplines define it in different ways 'bringing different starting points, perspectives, and terminologies into the discussion. In addition, risk is a term that is commonly used in everyday language, often without a precise meaning attached to it'. The following two Tables 6 and 7 bear out the diversity of risk arenas as well as cross-disciplinary areas of risk [49][50]. It has been aptly commented thus that the plentiful of faces of risk and its murky origins are nothing short of 'a testament to its elusive character as a conceptual phenomenon' [51]. Moreover, ICTs are causing immense changes in the 'landscape in global risks' [52]. Historical origins of the concept are not very decisive, as is the meaning of risk [53]. Kelley traces the origins back to the Greek classical age when the word 'rhizikon' referred to the 'difficulty to avoid in the sea' (a danger) and to Latin word 'riscus' has the same meaning and it passed on to the into Arabic as 'rizk' meaning 'fate' or uncertain outcome. In the 1500s the German meaning of the word 'rysigo' included an upside (benefit): 'to dare, to undertake, enterprise, or hope for economic successes in the mid-17th century, the word risk was derived from the French *risqué* and Italian *risco* ('danger'). He divides the risk-thinking into three periods (1) pre-mid-20th century; (2) the second half of the 20th century; and (3) the 21st century. The

Figure 6 shows the evolution of the concept in its historical aspects [54]. Nacol reminds that the term 'risk' appeared in English dictionary in 1661, when the Oxford English Dictionary defined it as meaning 'peril, jeopardy, danger, hazard, chance', referring to the persistent association between risk and harm or loss. This initial characterization also included 'chance', thereby starting also 'a link between risk and probability'. By the 17th century 'probabilistic calculation—the basis of risk—began to gain traction in contentious epistemological debates about how human beings could best determine what an unknowable future might bring and how to respond' [55]. The word 'risk' is also derived, as stated above, from the French 'risqué' of the 17th century and was defined by 'the French explanatory dictionary *Le petit Larousse* as danger, the more or less likely inconvenience to which we are exposed or exposure to a hazard, loss or failure' [56]. By the end of the eighteenth century risk-taking implied a painful process and thus the age of fear begun [57]. A review of the risk literature in various disciplines reveals that the definition of risk shows

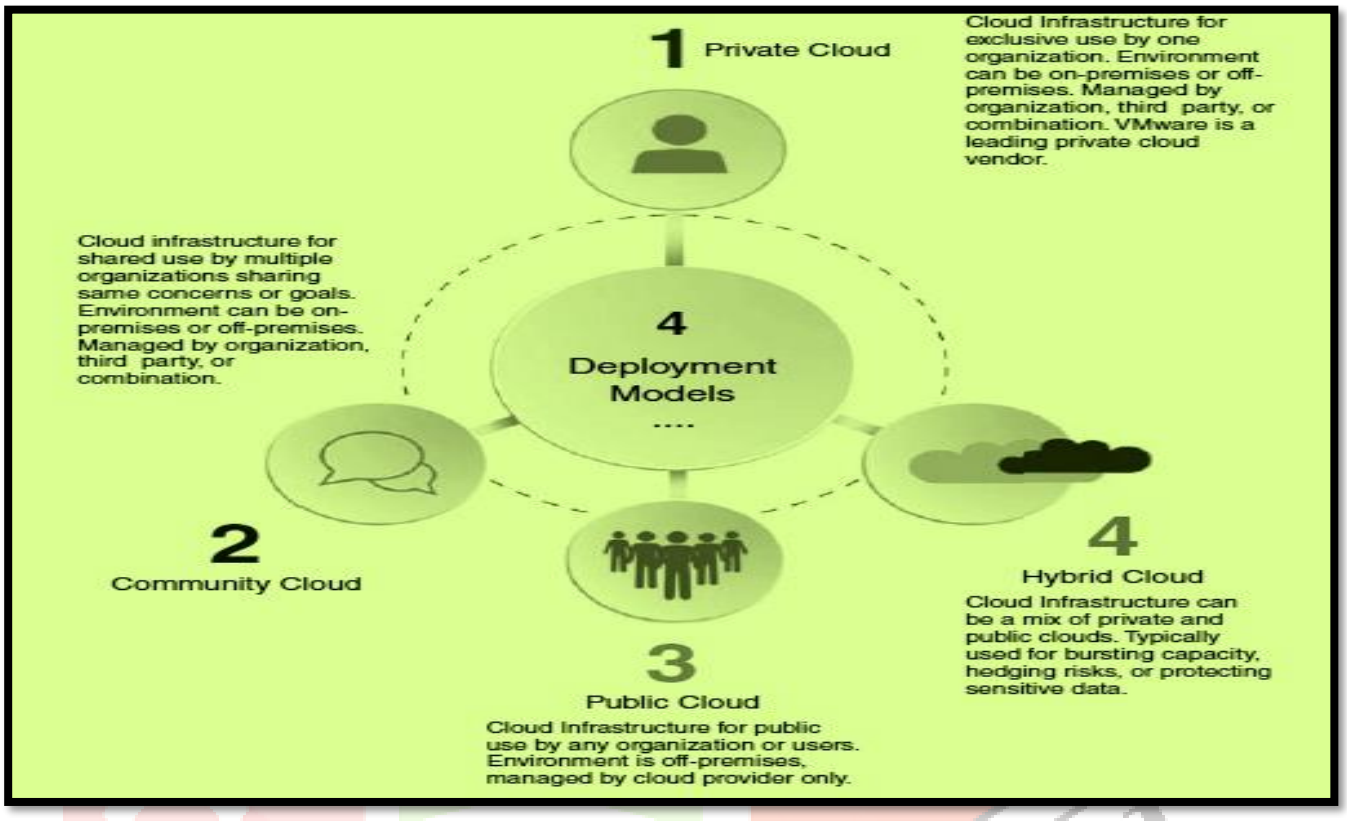


Figure 5: Cloud Deployment models

that it varies from author to author and from discipline to discipline. Several lists have been proposed and analyzed by risk analysts to come to grips with a risk definition for his/her purpose.. For instance, Flaus cites seven (7) definitions, [58], Šotić and Rajić cite twelve (12) definitions [59], Moller analyses five (5) definitions [60], Zinn quotes five (5) examples of the definition of risk, [61], Outreville mentions eight meanings of risk in addition to an additional one (risk as also defined as a chance of loss or a combination of hazards) [62], Boholm et al., cite five concepts of risk [63], and, finally, Aven and Renn cite ten (10) definitions to frame their own definition. They define risk as 'uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value'. [64]. Alexandru describes risk as follows:' the risk has the following features: is a possible, predictable or unpredictable event - the risk originates in uncertainty; is a generally negative event, whose definitions contain the terms of uncertainty and loss, but can also refer to the term of opportunity, denoting a positive connotation; is an event in all human activities, whose effects can no longer be removed; represents the distribution of the expected results; is the result of choices made' [56]. These two definitions can be adopted for purposes of this paper along with the characterization risk described by Garland in more generalized terms: 'Risk is a calculation. Risk is a commodity. Risk is a capital. Risk is a technique of government. Risk is objective and scientifically knowable. Risk is subjective and socially constructed. Risk is a problem, a threat, a source of insecurity. Risk is a pleasure, a thrill, a source of profit and freedom. Risk is the means whereby we colonize and control the future. Risk society is our late modern world spinning out of control' [65].

III. II. HAZARDS AND UNCERTAINTY

The concept of risk is related especially to two other concepts: hazard and uncertainty. Risk and hazard are often confused and are used synonymously. But the two, though related, are distinct concepts. Risk" may signify circumstances of exposure to hazard. 'The notion of risk is thus connected to the notion of hazard, a hazard being that which may produce damage in the future, in an uncertain manner' [58] . Natural hazards are storms, hurricanes, floods, forest fires, and earthquakes. These can cause loss of life, property damage, economic loss, etc. But there are 'human-made hazards by the scores: tools, weapons, vehicles, chemicals, technology, and activities. They can pose risks to life, property, environment, economies, and the like. Health hazards comprise their own category and include pathogens, disease, and all manner of personal health difficulties and accidents thatcan arise. These risks of adverse consequences are traditional examples of risk'. Hazardous events include incidents such as 'terrorism, infrastructure failure, crimes, fires, hurricanes, wars, explosions, seismic events, hydraulic fracturing, automobile accidents, and so on', and hence 'a hazard is the thing that causes the potential for an adverse consequence'. or 'anything that is a potential source of harm to a valued asset' [66]. One should first distinguish between hazard and risk. Hohenemser et al. introduce a

quantitative dimension into the relationship between risk and hazards. Hazards eventually result in harmful risk consequences. As they argue 'hazards are threats to humans and what they value, whereas risks are quantitative measures of hazard consequences that can be expressed as conditional probabilities of experiencing harm. Thus, we think of automobile usage as a hazard but say that the lifetime risk of dying in an auto accident is 2 to 3 percent of all ways of dying. We conceive of technological hazards as a sequence of causally connected events leading from human needs and wants to the selection of a technology, to the possible release of materials and energy, to human exposure, and eventually to harmful consequences' [67].

Risk arenas that may be subject to risk analysis		
Nos.	**Risk arena**	**Application or problem area**
1	Hazardous substances	Chemical/process industry, petroleum industry (incl. pipelines), explosives industry, nuclear industry
2	Transport	Air traffic (airplanes, helicopters, drones), railways, marine transport, road transport.
3	Space industry	Space equipment and projects.
4	Product safety	Technical products, such as machinery, cars, robots, autonomous systems.
5	Critical infrastructures	Drinking water supply, sewage systems, power grids, communication systems, hospitals and health-care, banking and financial systems.
6	Medical sector	Medical equipment, robotic surgery, bacteria/viruses.
7	Work, activity	Industry, agriculture, forestry, sport.
8	Environmental protection	Pesticides, CO2, temperature increases, ocean level increases.
9	Food safety	Contamination, infection.
10	Health safety	Cancer, tobacco, alcohol, radiation.
11	Project risk	Time and cost of large projects (e.g. construction, software development).
12	Economic/financial	Insurance, investment, financial, enterprise, and project risk.
13	Security	Sabotage, theft, cyberattacks, espionage, terrorism

Table 6: Risk Arenas

The concept of uncertainty as inherent to human life and knowledge originated historically long ago, going back Roman stoic philosopher Seneca who wrote in 49 CE that 'all things that are still to come lie in uncertainty' [68]. And even today uncertainty still continues: 'Unable to slow the mind-boggling pace of change, let alone to predict and control its direction, we focus on things we can, or believe we can, or are assured that we can influence: we try to calculate and minimize the risk that we personally, or those nearest and dearest to us at that moment, might fall victim to the uncounted and uncountable dangers which the opaque world and its uncertain future are suspected to hold in store for us' [69]. As one remarks: 'uncertainty is everywhere' [70]. The meaning of the word uncertainty is however imprecise and uncertainty is defined by different researchers in different ways [71]. The Merriam-Webster dictionary defines uncertainty as 'the state of being indefinite, indeterminate, unreliable, unknown beyond doubt, not clearly identified or defined, and/or not constant'. Politi et al., having cited quite a few definitions of uncertainty and its different types, assert that 'fundamental uncertainty about the future occurrence or non-occurrence of a given outcome lies at the core of the notion of risk. Risk estimates describe this uncertainty in probabilistic terms and are derived from empirical observations of an outcome's occurrence within a given population. Yet risk estimates embody additional uncertainties as well' [72]. The concept of uncertainty is integrally related to the concept of risk. According to International Organization for Standardization (ISO) 31000 risk is the '*the effect of uncertainty on objectives'*. For Allen and Derr, 'risk is uncertainty' or 'risk is *uncertainty* that surrounds actual events and outcomes that may (or may not) take place. The uncertainty surrounds *actual* events and outcomes for future events and *actual* events' [73]. Flaus quotes the definition of risk by the *International Risk Governance Council* as 'the uncertain consequence of an event or an action on something with a given value' [58]. Aven and Renn associates risk with uncertainty when they define risk as referring to 'uncertainty about and severity of the events and

The Disciplines, Risk, and Knowledge Forms Applied to the Unknown that Determine Disciplinary Epistemological Definitions of Risk		
Discipline	**How It Views Risk**	**Knowledge Applied to the Unknown**
Logic and Mathematics	Risk as a calculable phenomenon	Calculations
Science and Medicine including physical, biological, natural, and technological sciences	Risk as an objective reality	Principles, postulates, and calculations
Social Sciences		
Anthropology	Risk as a cultural phenomenon	Culture
Sociology	Risk as a societal phenomenon	Social constructs or frameworks
Economics	Risk as a decisional phenomenon, a means of securing wealth or avoiding loss	Decision-making principles and postulates
Law	Risk as a fault of conduct and a judicable phenomenon	Rules
Psychology	Risk as a behavioral and cognitive phenomenon	Cognition
Linguistics	Risk as a concept	Terminology and meaning
History and the Humanities		
History	Risk as a story	Narrative
The Arts (literature, music, poetry, theatre, art, etc.)	Risk as an emotional phenomenon	Emotion
Religion	Risk as an act of faith	Revelation
Philosophy	Risk as a problematic phenomenon	Wisdom

Table 7: Disciplinary Concepts of Risk

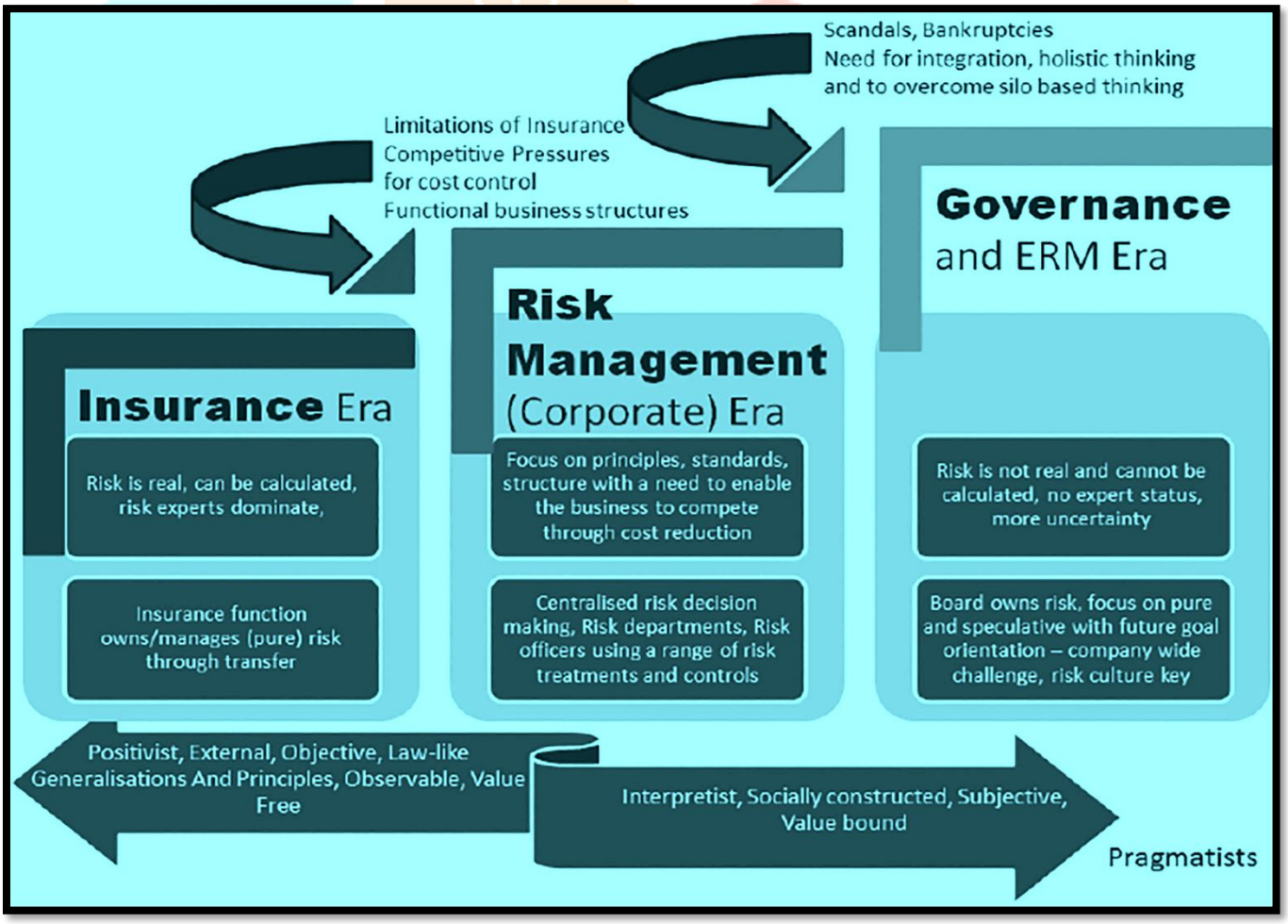


Figure 6: Eras of Risk-Thinking in Organizations

consequences (or outcomes) of an activity with respect to something that humans value' [64]. Uncertainty, as 'a mental concept' is a feature of the notion of risk [74]. According to the economist Frank Knight, uncertainty that is measurable is risk, while uncertainties that cannot be measured or quantified are 'true' uncertainties [75]. It is he who, in his book, (viz., *Risk, Uncertainty and Profit*) introduced the distinction between risk and uncertainty [76].

If uncertainty is non-measurable, as Knight says, then it resembles to Donald Rumsfeld's notion of the 'unknown unknowns' i..e., 'there are things we don't know we don't know' and thus 'uncertainty tends to be associated with anxiety about the unknown, whereas risk is associated with fear of failure' [77]. In 2002 the US Defence Secretary said, in connection with lack of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups, that 'there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tends to be the difficult ones' [78].In Figure 7, afour-quadrant classification of risks is shown [79]. *Known-knowns* refer to things 'we are aware of and understand', i.e. manageable facts; *Known-Unknowns* refer to facts 'we are aware but do not comprehend', i.e. classic or known risks which can be addressed by the knowledge of probabilistic methods; *Unknown-knowns* indicate 'things we understand but are not aware of', i.e. they refer to' hidden facts' or 'untapped knowledge'; and *Unknown-Unknowns* ,i.e., things 'we are neither aware of nor understand' or simply unknown risks [80] [81]. Rawson and others rightly state that in this age of evidence policy decisions are justified on the basis of known-knowns at one end, whereas more troubling is the terrain of unknown-unknowns at the other end [82].These are Nassim Nicholas Taleb's 'Black swans' which are not likely to be discovered by risk assessment [95]. However, Lindaas and Pettersen 'favor an extension of the Black Swan domain so that it includes unknown knowns in addition to unknown unknowns' [106].

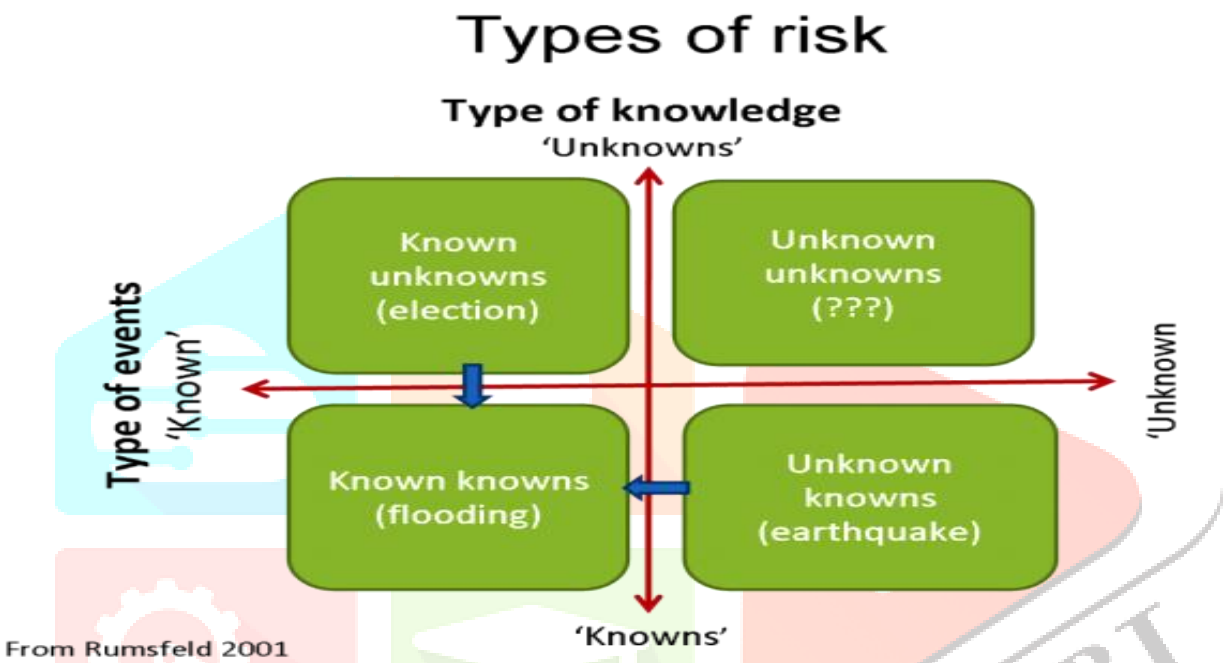


Figure 7: Typology of Known Risks and Unknown Risks

At bottom, risk theoretical discourse in different disciplinary areas is quite vast, if not confusing at the same time. It is rightly asserted that uncertain dimension of risk is 'problematic'. Detailed surveys of what uncertainties and risks really are and their classifications only produce complicated structure rather than useful tool for working in this area. There can be different levels of uncertainty as well as different types of risk scenarios [83]. Politi and others differentiate between five (5) main types or sources of uncertainty such as '1) risk, or uncertainty about future outcomes; 2) ambiguity, or uncertainty about the strength or validity of evidence about risks; 3) uncertainty about the personal significance of particular risks (e.g., their severity, timing); 4) uncertainty arising from the complexity of risk information (e.g., the multiplicity of risks and benefits or the instability of risks and benefits over time); and 5) uncertainty resulting from ignorance' [84]. However, it must be kept in mind that the terms ' risk' and 'uncertainty' are not equivalent or synonymous, but are distinct entities although related' [85]. It is uncertainty that is the seedbed of risk and uncertainty is main rationale for risk analysis, and the pervasiveness of uncertainty has caused 'the use of risk analysis to spread so quickly in recent years' [66]. Table 8 shows the summary of differences between risk and uncertainty in contradiction to risk [86].

Figure 8 shows how possible future events with known adverse outcomes precipitate into risks on the one hand and danger on the other. The decisive difference between danger and risks is that 'a danger is present regardless of choice, whereas a risk is either optionally accepted or imposed' [87]. If Figure 7 illustrates risks in the continuum between known-kowns and unknown-unknowns, Figure 8 shows, within continuum of uncertainty, continuum between open knowledge and open ignorance leading eventually to risk and danger. Closed ignorance leads Galileo effect (i.e., rejection or ignoring available knowledge deriving from closed ignorance) and nescience (i.e., closed ignorance or absence of knowledge) to danger (i.e., threat neither accepted nor imposed), while closed knowledge generates risks (i.e. threat accepted or imposed). In any case, one need not take a pessimistic view of uncertainty. At the end of the day, the role of uncertainty is constructive in that it is uncertainty that drives science to advance by continually, searching for new evidence. 'If we are certain, we stop searching for further evidence. Such evidence can provide us with even better support for the theories we accept, or it can lead us to new theories and discoveries' [88].

III. III. RISK THEORETICAL PERSPECTIVES: AN OVERVIEW

Risk as a concept has become over the years a fertile ground and dynamic subject of intensive research and analysis in different disciplines even though an overall consensus over a integrated concept of risks, it nature and characteristics has remained a goal yet to be achieved in future, if at all that is possible , rather than a reality in the domains of multiple theoretical discourses. In the area of social scientific disciplines this is type case, as is evident from the next two Tables, 9 and 10, which contain differential facets of risk and also a comparison of risks along with certain specified dimensions as available in the concerned literature [89].Renn has attempted to provide an integrated perspective on risk such as social amplification of risk, as shown in Table 11 [90]. The social amplification of risk approach takes account of both technical risk and sociological risk for seeking knowledge on risk and its impacts on society. 'The social amplification approach proposes a division of labor in which technical risk analysis is concerned with investigating the original signal whereas social science in general and sociology in particular analyze how this signal is transformed by society'. It puts emphasizes on the attention and intensification of the original risk at the same time. The notable feature of this approach is that this 'approach contributes an understanding of why certain hazards and events that experts assess as low risk may receive public attention, whereas other hazards that experts consider more severe receive less attention' [91]. Elsewhere he argues that, while risk concepts are different in the natural, engineering, psychological, social, and cultural disciplines, 'what is needed, is therefore a comprehensive risk concept that spans the different perspectives and provides an integrated approach for capturing the physical and socio-cultural aspects of risk. Such a concept should be guided by the rigor and specificity of the technical and natural science approaches and inspired by the richness and plurality of the economic, psychological and social science approaches' [92]. Another attempted integrationist theory has been contributed by Wong and Lockie who strongly argue that 'the conventional division of labour between the natural/technical and social sciences is ill-equipped to provide the insights and innovations needed to face the risks of our time. From climate change and global pandemics to nano/biotechnology and energy security, these challenges demand new ways of doing science and new

Summary of the Differences between Risk and Uncertainty		
	Risk	**Uncertainty (in contradiction to risk)**
1	**It can be made certain assumptions aboutevents that may occur and the associatedprobability of their occurrence.**	**It is described the situation when the decision maker cannot identify all or none of the possible events likely to occur and much less is he able to predict the likelihood of their occurrence, having the mathematical meaning of incompletely defined variable.**
2	**A condition in which there is the possibility of undesired changes to a desired outcome that is expected or hoped for.**	**When defining uncertainty, one thing is sure: "nothing is sure or predictable".**
3	**Uncertainty affecting the outcome.**	**A situation is uncertain when the decision should be taken but subsequent developments and associated probabilities are not known enough or at all.**
4	**Combination of circumstances including losing opportunities.**	**The mental state opposite to certainty is a simple reaction to the lack of knowledge about the future.**
5	**Creates uncertainty for some persons when risk is realized.**	**The state of uncertainty, characterized by doubt, because of lack of knowledge of what will happen or not in the future.**
6	**Whether risk is recognized or not, this does not change its existence.**	**An action is uncertain when several results may be achieved, without knowing the likelihood of occurrence of any of them.**

Table 8: Differences between Risk and Uncertainty

ways of analyzing risk' and, accordingly, propose a material-semiotic approach to risk [93]. What Wong advancesis an integrative approach called material–semiotic approach in her case study of India's nuclear technology – a technology that is surrounded by most contested concept of what is at risk at the end of the day. In this approach risk is not treated as social product or construct, but as a 'simultaneously material/objective reality' and hence 'the various *units* or *subjects of analysis* in macro-theories (i.e. markets, governance systems, political systems, etc.), meso-theories (i.e. organizations, governments, corporations, etc.), and micro-theories (i.e. individual perception, cognition, cultures, etc.) are no longer assumed to be intrinsically social in nature, but hybrids, constituted by both social and material actors and processes' . She conceives, on the foundations of the Actor Network Theory (ANT), risk as a material–semiotic network effect, meaning that it is constituted by both material (including ecological and technological) and social entities and processes. What we call the "objects" and "subjects" that constitute risk are, in fact, *hybrids*, constituted by both social and material elements. The job of a material–semiotic enquiry into risk, therefore, is to discover, as much as possible, its hybrid nature and to uncover previously invisible, hidden or unknown connections and connectors. 'Underlying the concept of risk are myriad social–material practices associated with risk calculation (risk assessment, probability modelling, actuarial science, etc.), risk consideration (deliberation, standards development and implementation etc.), and risk enactment (project implementation, monitoring, reporting, communication, etc.). These practices transform vague threats of harm into altogether more knowable and manageable entities. Unpredictable and/or uncontrollable events are, in principle, corralled and domesticated'. The argument is illustrated by pointing to the fact that, by themselves, nuclear reactors and atoms do not produce nuclear energy. They require nuclear scientists and engineers to create a suitable environment to produce it through nuclear fission. They also require also need 'the know-how of scientists and engineers, capital from the government and industrialists to finance atomic research and a network of laboratories, power plants, electric grids, etc. But scientists, the State and industrialists by themselves also cannot produce atomic energy, neither are they in complete control of nuclear fission when a reactor goes live. They rely on the natural resource endowments of uranium; the kinetic potential within these metals; the velocity of atomic reactions to stay within thresholds of the containment building; the valves, turbines and cooling systems to operate as planned; and operating manuals to condition the actions and practices of staff around the technology'[94].On the basis of Wong's

conception of risk as a material–semiotic approach to nuclear technology it is quite conceivable that this approach may also be fruitfully applied to the study of cloud computing and its risks since they also require intervention of other actors including computer scientists and cloud technologists – a research arena that is not explored as yet.

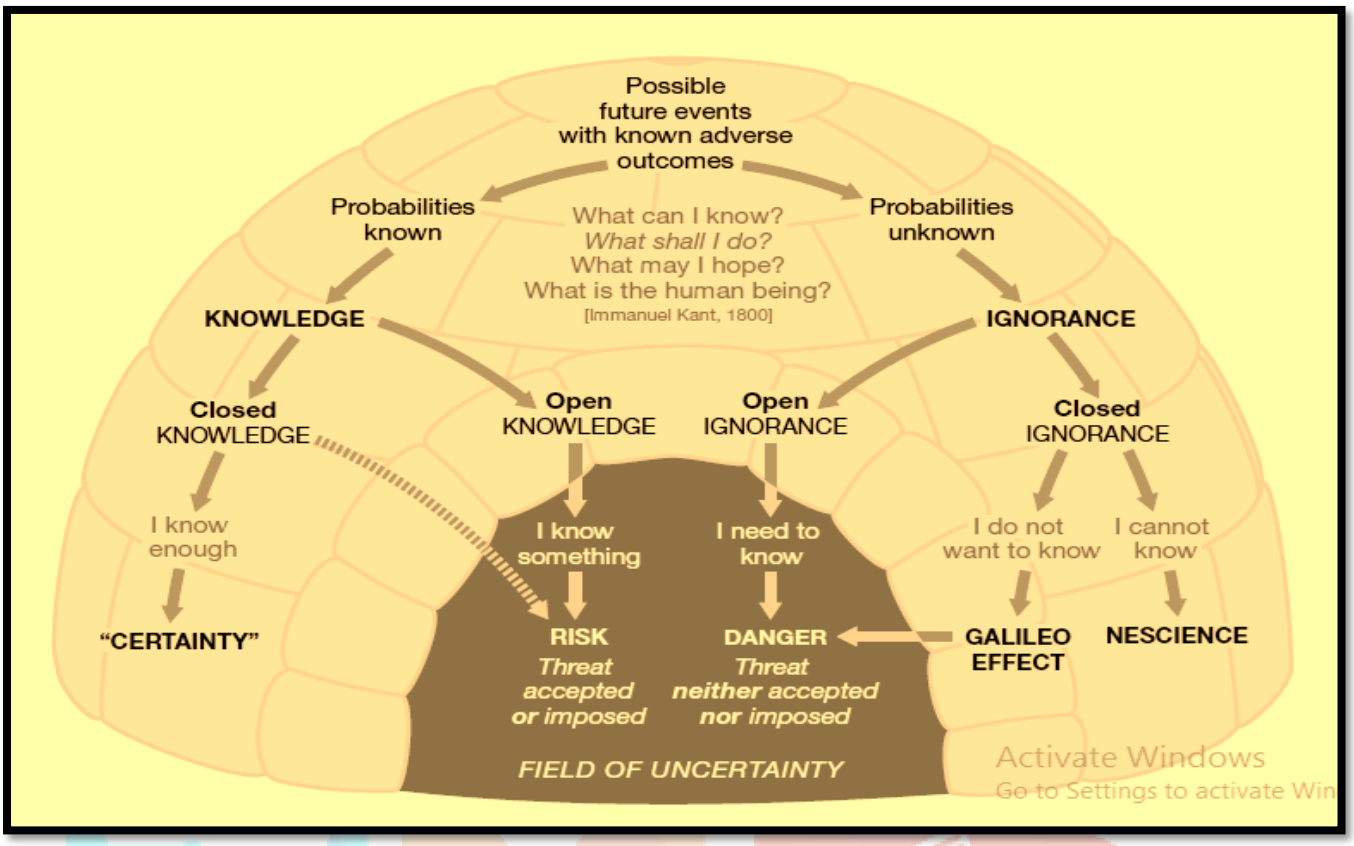


Figure 8: The Igloo of Uncertainty

III. IV: An Overview of Risk Analysis

Risk being ever present in human life, risk studies began as soon as human beings pondered over their impending death and avoiding dangerous or hazardous circumstances. Risk issues are not abating, but rather multiplying in the society and the recent example is Covid-19 pandemic. It cannot be gainsaid that risks are not trivial issues and it indeed requires constant vigil and serious efforts to understand, describe, analyze, manage and communicate these risks'[96] [97]. However, the first systematic work on risk analysis was possibly by Girolamo Cardano (1500–1571) who first employed mathematical tools for risk analysis. After Renaissance, as Gardoni writes, , the theoretical foundations of the modern principles of risk analysis were laid down by many others such as Pascal and Fermat in the 1600s, Leibniz, Bernoulli, de Moivre and Bayes in the 1700s, Galton in the 1800s, and Markowitz in the 1900s. Later on, risk analysis was further strengthened by contributions from other disciplines like engineering, philosophy etc. which contained basically individual disciplinary viewpoints [98]. From the 1950s onward risk studies gradually proceeded in many areas such as space exploration programs, chemical or nuclear power plants for reasons of securing safety. In any case, regardless of the date one chooses to trace the origins of risk analysis, the fact is that ,the preoccupation with risk is 'a rather recent phenomenon' in the present day society' [99]. Aven defines Risk Analysis in broad terms as 'risk understanding, risk assessment, risk characterization, risk communication, risk management, risk governance, and policy relating to risk, in the context of risks which are a concern for individuals, public and private sector organizations, and society at a local, regional, national or global level'. He divides risk analysis in two broad divisions: (A) Applied risk analysis as a specific activity in the real world (e.g. the use of a medical drug, the operation of an offshore installation, etc) which supports 'support risk knowledge generation and communication, and the handling (management, decision-making) of risk problems and issues'; and (B) generic risk analysis that aims to 'development of generic risk analysis concepts, theories, frameworks, approaches, principles, methods and models, i.e. development of generic concepts, theories, frameworks, approaches, principles, methods and models to understand, assess, communicate, manage and govern risk'. Risk analysis science, in these two dimensions, generates 'scientific knowledge'. Risk analysis is a science that is contributed by experts from various disciplines such as natural sciences, social sciences, statistics etc, and is therefore multidisciplinary in character[96].Another risk researcher, Yoe contends that, as a science and a paradigm' risk analysis has these characteristics. First, as a good science, it is based on 'scientific facts, evidence, and good analytical techniques' which 'separates what we know (the science) from what we don't know (the uncertainty), and it focuses appropriate attention on what we don't know and how that might affect decision outcomes and, therefore, the decision itself'. For instance, risk analysis requires to be based on sound evidence, whether qualitative or quantitative, identified with certainty or shaded by uncertainty. Second, risk analysis is not value free altogether, for social values invariably go into the risk analysis process when tasks of risks management are undertaken. Third, risk analysis directly confronts uncertainty. 'Risk assessors address uncertainty in the assessment of risks, risk managers address it in their decision making, and risk communicators convey its significance to interested parties as appropriate' .Fourth, collecting relevant

Understanding of Risk and its Embeddedness in Theorizing				
Theoretical Perspectives	**What is the aim of theorizing?**	**How is risk involved?**	**What is risk?**	**Epistemological status of risk**
Systems theory	**Understanding the logics of social "evolution" in functionally differentiated societies**	**"Risk" is the form in which modern societies describe themselves as decision-based**	**The attribution of an undesired event to a decision**	**Constructivist**
Governmentality	**Reconstructing the practices and changes of governmental strategies**	**Concerned with how calculative techniques (risk) are used and how they are embedded and constituted in social discourse and practice**	**A specific way to manage uncertainty by calculative techniques and a specific way to govern society by allocating responsibility to a prudent subject**	
Cultural turn	**Reconstructing the production and reproduction of culture**	**"Risk" describes the transgression of meaning (e.g. regarding identity, the constitution of social groups)**	**A danger for or transgression of symbolic orders**	
Sociocultural theory	**Explaining the constitution of societies and social groups**	**Risk is a real danger transformed into a transgression of social values of a social group**	**An objective harm transformed into a symbolic danger for a social entity**	**Weak constructivist**
Risk society	**Understanding the fundamental changes within modernization**	**New risks are unforeseen side-effects of modernization which contribute to the self-transformation of modernization**	**A hybrid or quasi-subject. It is a real danger, constructed as objective issues as well as a social construction of future possibilities and thereby hypothetical**	**Realist and constructivist**
Edgework	**Explaining the increase in high-risk-taking activities**	**High risk taking is a form of immediate embodied experience of a real self. The motivation to take high risks is increased by social changes**	**There is a real danger of crossing a material boundary (life and death)**	**Weak realist**

Table 9: Understanding of Risk and its Embeddedness in Theorizing

information from numerous sources, risk analysis makes the attempt 'to make good decisions by finding and defining the right problem', without which it is hardly possible to have any successful solution for the problem at hand. Finally, since risk assessment is based on the presumption of uncertainty and its reduction, risk analysis is necessarily a continuous process that aims to improve decisions continuously. But, to note, risk analysis is' neither a magic bullet, nor a black box' [66]. Hubbard provides long definition of risk analysis by saying that it is 'the detailed examination of the components of risk, including the evaluation of the probabilities of various events and their ultimate consequences, with the ultimate goal of informing risk management efforts' [100].Below are Figures9 and 10, provided by Delogu, concerning (a) definitions of hazard, risk and harm/damage; and (b) the structure or tasks of risk analysis [101].

COMPARISON OF RISK APPROACHES ON FIVE DIMENSIONS					
	Values	*Knowledge*	*Rationality*	*Power*	*Emotion*
Cultural approaches	Risks are threats for the value system of social groups and social identities	Specific socioculturally mediated forms of knowledge/ knowledge production	Sociocultural rationales of risk management	Socio-cultural forms of power	Dichotomy of rationality and emotions; but emotions as a resource for social change as well
Risk society	Individualized culture and self-culture; survival and ecological values	Limits of knowledge and control as well as the fragmentation of knowledge production produce risks Loss of class knowledge and other traditional knowledge produces uncertainties	Calculative scientific or expert-rationality meets its limit and is challenged by social and subjective rationalities	New power of "subpolitics," ad-hoc coalitions between the formal political organization and the nonpolitical. Political consumers and other new organized actors populate the public arena of subpolitics	Negative emotions as a resource for political existence. Emotions enforce a new political subject, "the coalition of anxiety"
Systems theory	Culture as the realm of possible meanings communication can refer to	Only the scientific functional system describes risk as a problem of "true knowledge"	"Risk" is the core concept of modern, functionally differentiated societies to describe themselves. Since an overall integrating social rationality is lost, risk conflicts increase	Power/non-power as the code of the political system	Dichotomy of rationality and emotions. Unsteady emotions endanger modern society
Governmentality	Culture as background against which societies are governed	Socially available risk-knowledge structures individuals' behavior	Instrumental rationality and social rationalities are connected within governmental practice	Power is understood as "discursive power," which structures individuals' sense making and behaviour. Risk is a specific rationale to govern societies connected to (Neo-) Liberalism.	Governmental strategies use people's desires for self-improvement
Edgework	Duality of sociocultural context and subject. Culture contradicts or meets individuals' desires	Embodied, practical knowledge; ability to manage risks even beyond learnable skills	Situated, subjective, and embodied rationale which has its origins beyond the social	Power to resist (or to master) social demands by direct embodied experiences of a "real self"	The motivation for high risk taking is its emotional attraction, which can be heightened by specific social contexts of living

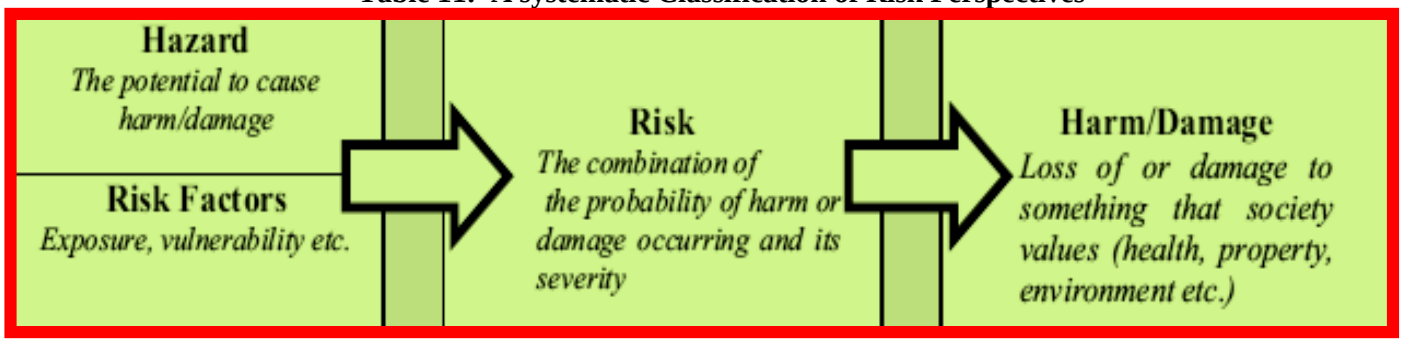
Table 10: Comparison of Risk Approaches on Five Dimensions

Let me now turn to a brief discussion of selected dimensions of risk analysis. Let me first begin with **'risk management'** - a term that appeared in the 1990s [109]. Hubbard goes on to say that 'a weak risk management approach is effectively the biggest risk in the organization', thus emphasizing the role of spot on risk management [100].Briefly stated, risk management comprises 'comprise coordinated activities to direct and control an organization with regard to risk' and it needs a framework, such as ISO 3100, to be 'adequate, efficient, and effective'. Risk management Framework defines 'the mandate and commitment of the risk management, the risk management policy and responsibilities, the integration of the risk management into the organizational processes, and the mechanisms for internal and external communication and reporting. The risk management framework should be continuously monitored, reviewed, and improved'[95].The purpose of management is to prevent transformation of digital risk society into 'digital danger society' in which digital risks of all types are 'expanded and reproduced throughout the social system as a whole'. Yoo thus elaborates risk management as a multifaceted regulatory process divided into four steps such as preventive, preparedness, response, and recovery. 'Prevention and preparation based on time can be classified into pre-activities, while responses and restoration can be classified into post-activities. Prevention is an activity that evaluates the actual risks or potential risks, and reduces the risks. Contrast refers to the development of response plans based on risk assessment, training of response personnel, preparation of necessary resources, and clarification of responsibilities. Responses include enforcement of the plan, reduction of the possibility of secondary damage, and preparation for the recovery phase. The restoration refers to the reconstruction of the system, such as support until returning to a normal state' [102]. Hubbard divides the risk management into a simplified scheme consisting of five successive steps: (1) identification of risks; (2) assessment of risks; (3) identification of risk mitigation approaches; (4) assessment of expected risk reduction and cost of risk mitigation methods; and (5) selection and implementation methods [100]. ISO 31000: 2018 Framework , an updated the version of ISO 21000: 2009 in 2015 and published in 2018, is a general framework that applies to all organizations irrespective of type, size, activities and location, and covers all types of risk in all organizations. Dedicated to in improving an organization's governance and, ultimately, its

performance as well as offering positive opportunities, ISO 31000: 2018 empowers organizations 'to develop a risk management strategy to effectively identify and mitigate risks, thereby enhancing the likelihood of achieving their objectives and increasing the protection of their assets. Its overarching goal is to develop a risk management culture where employees and stakeholders are aware of the importance of monitoring and managing risk'. It defines risk management as 'the' program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time' [103]. ISO 3100: 2018 contains eight (8) Principles including consideration of Risk management as an integral part of all organizational activities anticipating, detecting, acknowledging and responding to changes and, at the same time, explicitly recognizing any limitations of available information and also the impact of human and cultural factors on all aspects of risk management. ISO 31000: 2018, concerned

	INTEGRATED APPROACHES (such as the social amplification of risk)						
	Actuarial approach	Toxicology/ epidemi-ology	Probabalistic risk analysis	Economics of risk	Psychology of risk	Social theories of risk	Cultural theories of risk
Base unit	Expected value (EV)	Modelled expected value	Synthesized expected value	Expected utility (EU)	Subjectively expected utility	Perceived fairness & competence	Shared values
Predominant method	Extrapo-lation	Experiments Health surveys	Event & fault tree analysis	Risk–benefit analysis	Psycho-metrics	Surveys Structural analysis	Grid–group analysis
Scope of risk concept	Universal One-dimensional	Health & environment One-dimensional	Safety One-dimensional	Universal One-dimensional	Individual perceptions Multi-dimensional	Social interests Multi-dimensional	Cultural clusters Multi-dimensional
Basic problem areas	Averaging over space, time, context			Preference aggregation		Social relativism	
	Predictive power	Transfer to humans Intervening variables	Common mode failures	Common denominator	Social relevance	Complexity	Empirical validity
Major application	Insurance	Health Environm. protection	Safety engineering	Decision-making	Policy-making and regulation Conflict resolution (mediation) Risk communication		
Instrumental and Social function	Risk sharing	Early warning Standard setting	Improving systems	Resource allocation	Individual acceptance	Equity fairness Political acceptance	Cultural identity
	Assessment	Risk reduction and policy selection (coping with uncertainty)					Political legitimation

Table 11: A systematic Classification of Risk Perspectives



. **Figure 9: Hazard, Risk and Harm/Damage**

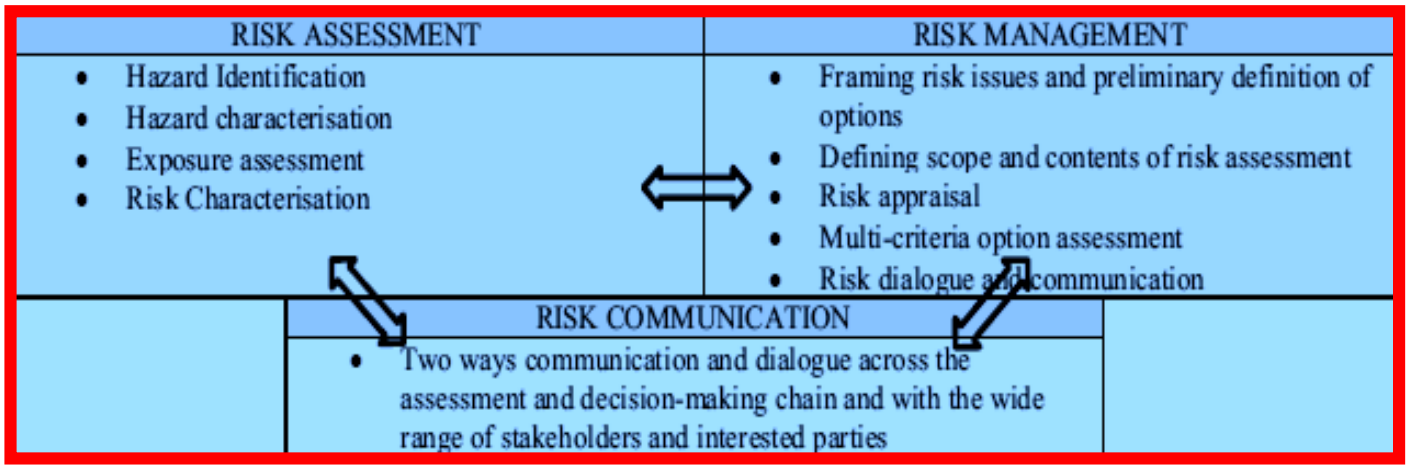


Figure 10: Structure of Risk Analysis

with the continual risk management process, describes risk assessment and risk treatment as being at the centre of the risk management process and also contains guidance on (1) scope, context and criteria; (2) communication and consultation; (3) monitoring and review; and (4) recording and reporting aspects. Figure 11 reproduces the ISO 31000: 18 Framework [104] .Another useful generic frameworks in Figure 12 has been provided by Yoe who has listed five steps in the risk management process: (1) risk identification; (2) risk estimation; (3) risk evaluation; (4) risk control; and (5) risk monitoring, along with explanatory requirements [105]. Risk management is integrally connected with risk analysis and the job of a risk manager is this attached to the responsibilities underlying the above-mentioned five tasks. It is for the risk manager to facilitate decision making under conditions of uncertainty by gathering and analyzing the best available evidence. 'Carefully considering the instrumental uncertainties encountered in a risk management activity and seeing that their potential effects are carefully communicated to all interested parties is a primary responsibility of the risk manager' [105]. Besides ISO 21000: 2018, there are other risk management standard and frameworks such as (1) Institute of Risk Management (IRM): Standard produced jointly by Airmic, Alarm and the IRM (2002); (2) COSO ERM cube: Framework produced by the Committee of Sponsoring Organizations of the Treadway Committee (2004); (3) CoCo (Criteria of Control): Framework produced by the Canadian Institute of Chartered Accountants (1995), etc. [107]. On a related note, just as there could be flaws in the risk management (viz., inadequate protection against security threats, additional maintenance required, supply chain risks due to pandemic etc.), so there are challenges as well to risk management (viz. confusion regarding the concept of risk, completely avoidable human errors in subjective judgments of risk, problems with popular methods, misconceptions that block the use of better methods, and recurring errors in even the most sophisticated models) [100]. It is not out of place to remember here a specific type of management that is characteristic of enterprises: enterprise risk management(ERM), which has been defined by Lam as 'an integrated and continuous process for managing enterprise-wide risks—including strategic, financial, operational, compliance, and reputational risks—in order to minimize unexpected performance variance and maximize intrinsic firm value. This process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting' [108].

Let me now pass on to another vital component of risk management process: **risk assessment** which answers the risks manager's questions (viz. were the key risk factors identified? did risk management affect risk/return positively? and so on) about risks in the organization. According to NIST's definition, risk assessment refers to 'the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis' [103], it is an orderly, step-by-step approach process for comprehensive evaluation of risks embedded in the collected data for a specific facility or system requirement. The process results in 'determining the probability of a risk occurring and the consequence of that risk. It is a fundamental component of an effective risk management program, which is a basic management tool consisting of risk Assessment and risk control. **Risk assessment** is the data gathering component, while risk control is the application of the risk assessment evaluation' [25] [110]. For general purposes risk assessment is a 'systematic evidence-based process for describing (qualitatively or quantitatively) the nature, likelihood, and magnitude of risk associated with some substance, situation, action, or event that includes consideration of relevant uncertainties'. As Yoe argues, it answers four questions: What can go wrong? What are the consequences? How can it happen? How likely is it to happen? Accordingly, he summarizes four tasks of a generic risks assessment: (1) Trying to find the hazards or opportunities involving identification of hazards that 'can cause harm or the opportunities for gain that are uncertain'; (2) Consequence Assessment involving collecting and analyzing relevant data to find out who are likely to harmed or benefitted in what ways in the light of 'the consequences and their uncertainty qualitatively or quantitatively'; (3) Likelihood Assessment aimed at assessing likelihood of the various adverse and beneficial consequences and simultaneously describing 'these likelihoods and their uncertainties qualitatively or quantitatively'; and (4) Risk Characterization by estimating 'the probability of occurrence, the severity of adverse consequences, and the magnitude of potential gains, including attendant uncertainties, of the hazards and opportunities identified based on the evidence in the preceding steps' as well as by distinguishing ' the risk qualitatively or quantitatively with appropriate attention to baseline and residual risks, risk reductions, transformations, and transfers'. Furthermore, he breaks down risk assessment within the risks analysis process into eight steps or tasks, viz., understanding the questions, identifying sources of risk, doing consequence assessment, undertaking likelihood assessment, charactering risks, assessing effectiveness of risk management options (RMOs), communicating uncertainties, and, finally, documenting the process. All these tasks are not linear but rather interlinked. It is of importance to note that there is no single model or technique of risks assessment for it varies from discipline to

discipline or even one application to the other in the concerned discipline [105].However, below is Figure 13 illustrating the process of risk assessment as cited in the relevant document of NIST [111]. Table 12 shows that there is also a variety of risk assessment tools that can be used by the risk assessors [25].

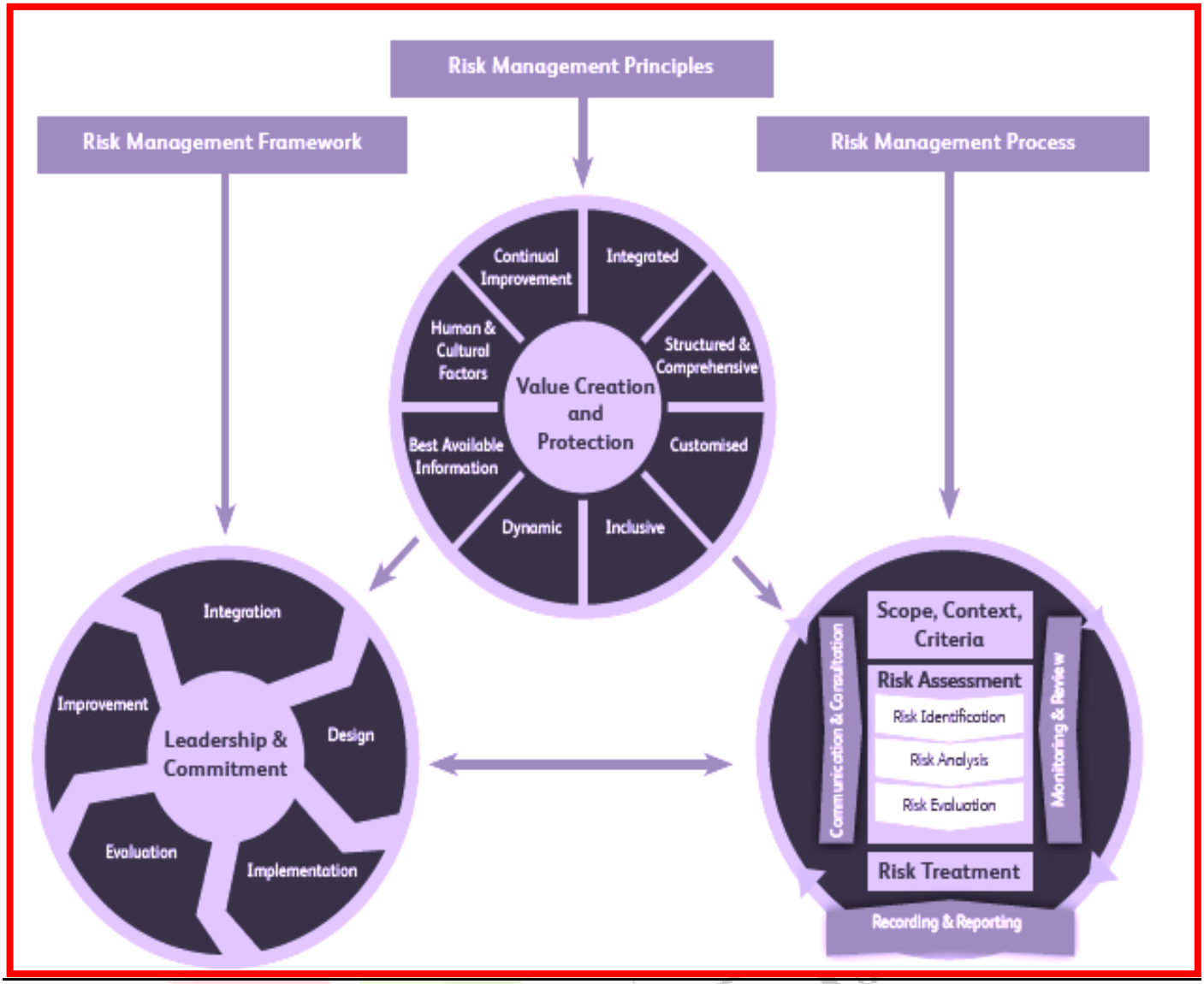


Figure 11: Principles, framework and risk management process from ISO 31000: 2018

What are benefits or reasons behind undertaking risk assessment, aside from the arguments made above? First, the risk assessment plays a crucial role in the decision-making process by providing objective information. as is illustrated in Figure 14 by Rausand, He says that: 'from the decisions, the required input can be defined, and this determines the objectives and scope of the risk assessment. When the assessment is completed and results are ready, this feeds back to the decisions again, together with other relevant information that is taken into account (e.g. feasibility and cost)'[49]. Second, one should require risk assessment because the information is a valuable asset which needs to be protected since it is exposed to various dangers or risks that might stand in the way of delivering services , say, by cloud computing technology. This explains why risks assessments come into play in order for handling concerned dangers or risks affording protection to the valuable asset, the information, among other things [112]. Finally, a good risk assessment is necessarily interdisciplinary in character drawing on multidisciplinary expertise. 'A transdisciplinary team dissolves the boundaries among disciplines and moves beyond integration to assimilation of perspectives', and good risk assessments 'can have educational value', in the sense that it can point out the limits of existing knowledge. It can tell 'the truth about what is known and not know' about the risks, and hence can indicate directions of future research[66].

Let me pass on to **data governance** and **risk governance** as components of risk analysis. In today's data- and information-intensive digital age of globalization, the role data governance has taken on new importance in view of the cumulative technological innovations and their employment in generating, accumulation, storing, processing, and transmission of volumes of data for their application and use in different organizations for diverse purposes including promoting business within and beyond national frontiers. **Data governance**, by improving data quality, data consistency, data safety and security , by enabling compliance with data related regulations, and by reducing uncertainty and risks due inaccuracy of data and simultaneously increasing accountability for data, helps to manage data efficiently for the organizations and eventually deliver a 'unified view of the world' [113]. In Figure 15 Engels illustrates in brief description different dimensions and functions of data governance.

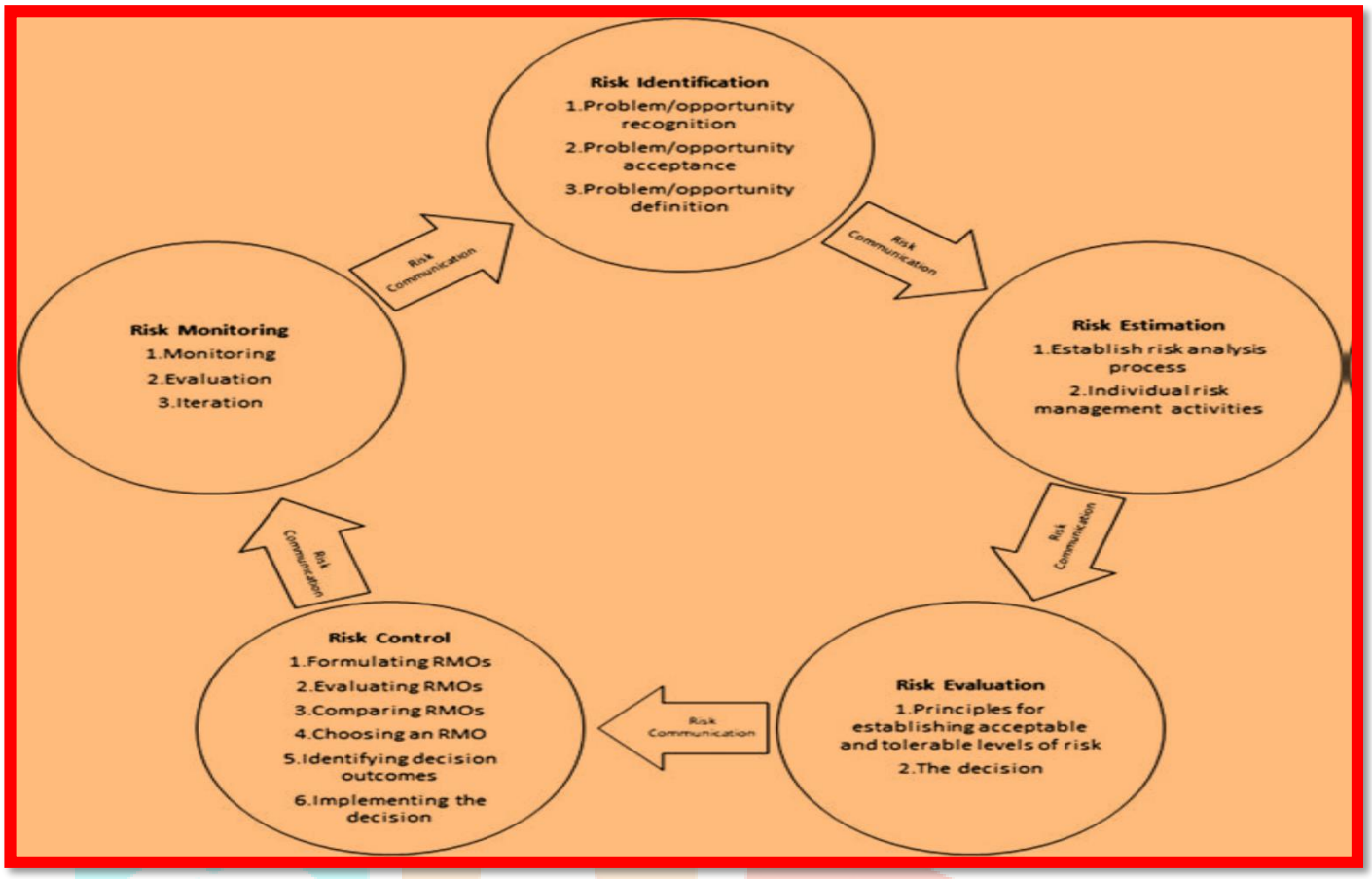


Figure 12: A generic risk management process comprising five tasks

'The key function of data governance is hence to ensure data availability and data quality (accuracy, completeness, reliability) for all possible management tasks and operations that contribute to the vision, mission and strategy of the company. The goal of data governance is to ensure interpretability correctness, completeness, trustworthiness, security, accessibility and traceability of enterprise data in an efficient and effective manner' [114]. **Risk governance**, according to the Society for Risk Analysis (SRA) Glossary, risk governance is basically 'the application of governance principles to the identification, assessment, management, and communication of risk'. While governance refers to 'the actions, processes, traditions, and institutions by which authority is exercised and decisions are taken and implemented', risk governance refers to 'the totality of actors, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analyzed, and communicated, and management decisions are taken. Consequently, processes and outcomes of standardization elements in risk governance influence the way we try to manage risks'. [115].The following Tables 13 and 14, taken from Delogu, depict the benefits of participatory risk governance as well as problems in risk governance practices in the business organizations' [101]. The final requisite in the

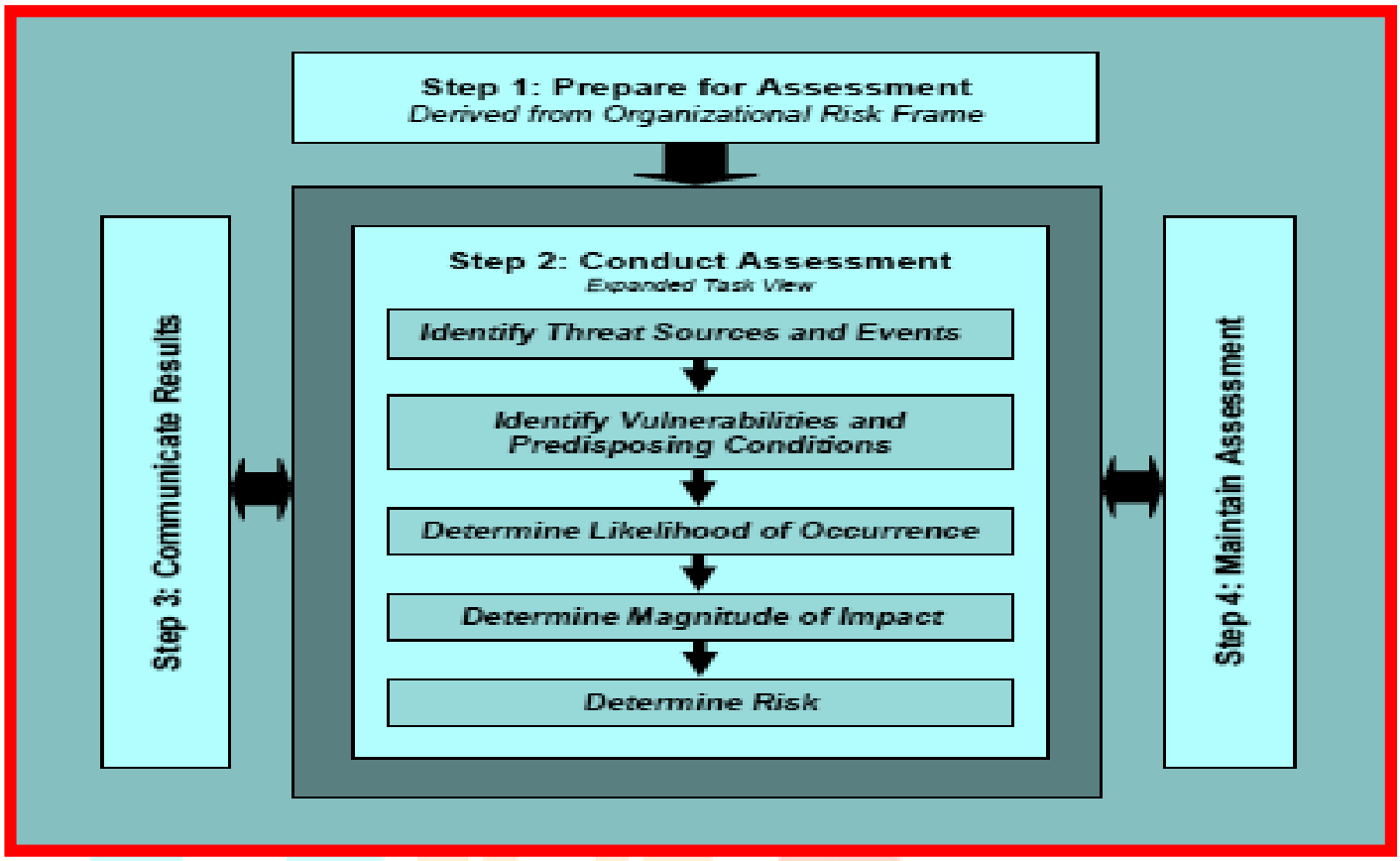


Figure 13: Risk Assessment Process

risk analysis process is the constituent of **risk culture –** a concept that implies that risk and culture are, **'**whether implicitly or explicitly recognized, are inextricably intertwined in organizations' [116].A vibrant and well cultivated risk culture gives the business enterprise competitive advantage over their rivals in the market and is thus an integral component of any effective risk management. The concept of risk culture slowly entered the risk management arena after the financial crisis of 2008. Even though ISO 31000:2018, the international standard on risk management, does not define 'risk culture, it does refer to the principle of "Human behavior and culture"[117].

What is risk culture and how is it related corporate culture? According to the *Chartered Institute of Management Accountants* (CIMA), risk culture refers to a company's 'norms, collective attitudes and behaviours' that influence the risks and impact outcomes. Risk culture is concerned with the enterprise risk-taking and risk control activities. Risk culture can be defined as an element of corporate culture which emerges as a "result of shared values, basic, underlying assumptions and business experiences, behaviour and beliefs, as well as strategic decisions." 118]. For Deloach, risk culture is 'the glue that binds all elements of risk management infrastructure together, because it reflects the shared values, goals, practices and reinforcement mechanisms that embed risk into an organization's decision-making processes and risk management into its operating processes. In effect, it is a look into the soul of an organization to ascertain whether risk/reward trade-offs really matter'. [119]. In Deloitte's view risk culture includes 'the general awareness, attitudes, and behaviors of an organization's employees toward risk and how risk is managed within the organization. Risk culture is a key indicator of how widely an organization's risk management policies and practices have been adopted' [120].Emphasizing' risk awareness (knowledge of, and respect for, risk) and an automatic, arguably almost subconscious, dealing with risk matters (embedded in daily thoughts and actions)', Banks defines 'risk culture to be *an internal sensibility, reflected in the daily thoughts and actions of all of an institution's employees, that reflects knowledge of, and respect for, risk'* . He enunciates a number of general characteristics that mark out risk culture's 'unique, and sometimes subjective, nature'. These are: (1) *Risk culture can be a nebulous concept;(2)Risk culture is qualitative, not quantitative; (3) Risk culture is changeable and evolutionary; (4) Acceptance and implementation of risk culture will vary by firm* ; (5) *Risk culture is a journey with no end; (6) Risk culture will determine success in aligning business strategy and risk strategy; (7)Risk culture cannot be a box-checking exercise; (8) Risk culture should be shaped by the needs of the institution, not the demands of stakeholders; (9) Risk culture must allow for national cultures; and (10) Risk culture relies on good governance, but it does not come solely from good governance*[121]. McKinsey's Working Paper defines risk culture as 'the norms of behaviour for individuals and groups within an that determine the collective ability to identify and understand, openly discuss and act on the organization's current and future risks'. Risk culture consists of six critical and mutually reinforcing elements such as (1) 'clear and well communicated risk strategy', (2) 'high standards of analytical rigour and information-sharing across the organization', (3) 'rapid excalation of threats and concerns', (4) 'visible and consistent role-modeling of desired behaviours and standards by senior managers', (5) 'incentives that encourage people to "do the right thing" about the overall health of the whole organization', and (6) continuous and constructive challenging of actions and preconceptions at all levels of the organization' [122]. Recent research demonstrates that risk culture, as integral component of Enterprise Risk Management, can be evaluated for measuring its values and behaviours that are present in the organization enabling it to shape risk decisions [123]. Wood and Lewis summarize the importance by stating that risk culture (1) facilitates better decision-making by improving an organization's 'ability to make transparent, well-coordinated, strategic decisions which are in alignment with its goals'; (2) enables adherence to rules and policies guaranteeing

that 'employees operate within the boundaries of acceptable risk'; (3) promotes enhanced governance enabling the organization to 'reduces the need for onerous governance control mechanisms which can stifle creativity and incur expenses'; (4) assists

Traditionally Used Risk Assessment Tools		
Nos.	**Tool**	**Traditional use**
1	**Preliminary hazard analysis (PHA)**	**This tool is used in the very beginning of a risk assessment and/or on a conceptual design of a new system, process, or operation. It is used to determine the potential hazards associated with or the potential threats poised to a system, process, or operation. This tool is also useful for organizations to evaluate processes that have been performed for years to determine the hazards associated with them**
2	**Failure mode and effects analysis (FMEA)**	**This tool is used in system, process, or operations development to determine potential failure modes within the system and provides a means to classify the failures by their severity and likelihood. It is usually performed after a PHA and before more detailed analyses**
3	**Failure mode, effects,and criticality analysis (FMECA)**	**FMECA extends FMEA by including a criticality analysis that is used to chart the probability of failure modes against the severity of their consequences. FMECA can be used instead of an FMEA, in conjunction with an FMEA, or after an FMEA has been performed**
4	**Event trees**	**Event trees are very useful tools to begin to analyze the sequence of events in potential accident sequences. They also have utility in analyzing accidents themselves. Many variations of event trees have been developed. This book presents some of the more common ones**
5	**Fault tree analysis (FTA)**	**FTA is a risk analysis tool that uses Boolean logic to combine events. The lower-level events are called basic events, and they are combined with Boolean logic gates into a tree structure, with the undesired event of interest at the top. This event is called the top event. Though this analysis tool is used to quantitatively determine the overall probability of an undesired event, it is also useful from a qualitative perspective to graphically show how these events combine to lead to the undesired event of interest. FTA has a wide range of use from determining how one's checking account was over drawn to determining why a space shuttle crashed**
6	**Human reliability analysis (HRA)**	**HRA is related to the field of human factors engineering and ergonomics and refers to the reliability of humans in complex operating environments such as aviation, transportation, the military, or medicine. HRA is used to determine the human operators' contribution to risk in a system**
7	**Probabilistic risk assessment (PRA)**	**PRA is a systematic and comprehensive methodology to evaluate risks associated with complex engineered systems, processes, or operations such as spacecraft, airplanes, or nuclear power plant. PRA uses combinations of all the other risk assessment tools and techniques to build an integrated risk model of a system. A fully integrated PRA of a nuclear power plant, for instance, can take years to perform and can cost millions of dollars. It is reserved for the most complex of systems**

Table 12: Risk Assessment Tools

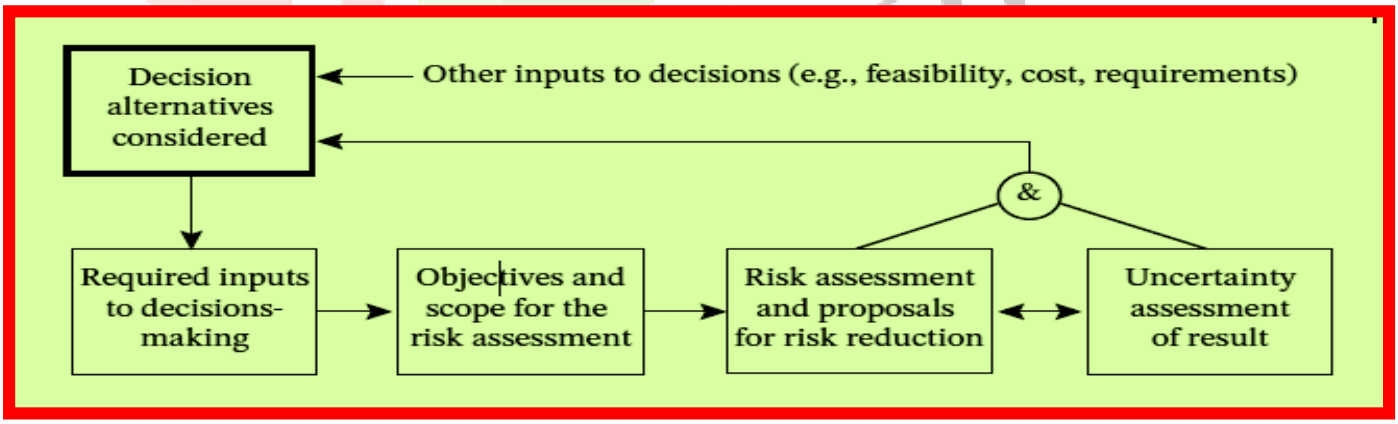


Figure 14: Risk Assessment in the Decision-Making Process

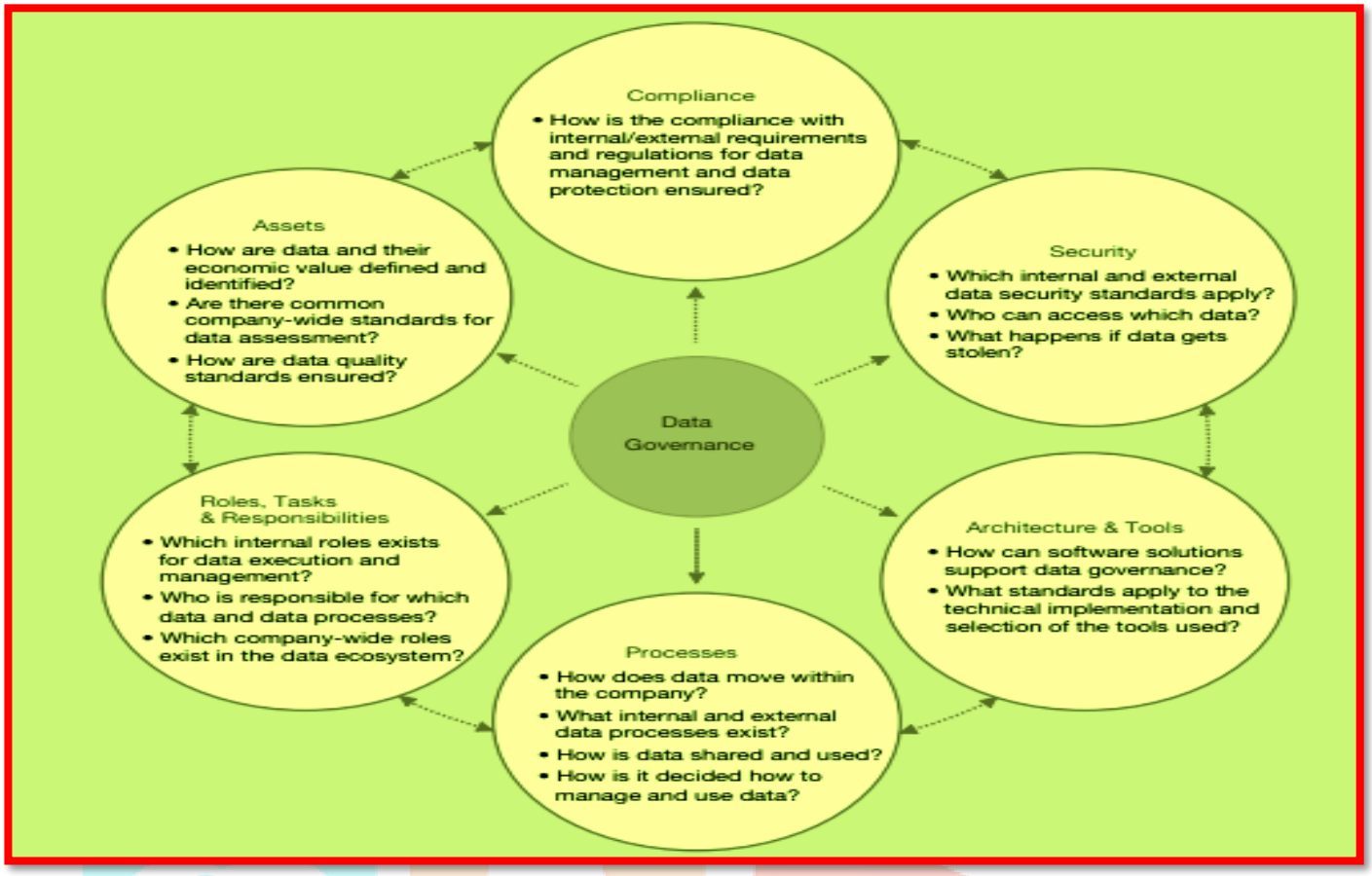


Figure 15: Dimensions of data governance

information sharing 'which encourages a unified awareness of risks and risk management, and this enables effective risk control'; (5) enforces greater accountability so that 'employees at all levels are motivated to contribute to the risk management process. Escalation of threats and concerns are handled in a more efficient manner'; and (6) imposes good regulatory relationships whereby 'organizations will find it easier to be in compliance with regulatory requirements and can benefit from enhanced credit ratings'. Figure 16 reproduces the underlined importance of risk culture [124].

Finally, it should be remembered that embedding risk culture in the organization is critical for governance and, accordingly, organization needs to develop a robust risk culture in such a way that it is embedded in all its areas and activities that ensure accountability for risk management as a priority for the entire organization. [125]. Furthermore an effective risk management strategy requires three elements to build an effective organization risk culture: First, *risk awareness* in the organization that recognizes the existence of risk within and beyond the business of the organization; Second,, organization risk culture need to be *risk mature* at all levels and ready to take on 'a proactive approach to risk management in all aspects of the business, makes active use of risk information to improve business processes and gain competitive advantage, and learns from its experience'. Third,, it should be an accepted norm that the management must be willing to *encourage and reward appropriate risk taking* that may eventually strengthen the both the organization and its risk culture [126]. It is no exaggeration to say that, in the general context 'risk-taking is an end in itself, a means to an end, and a response to vulnerability'. In a way it is not unreasonable to conclude here that 'biggest risk in life is not taking a risk at all. Life is all about risk as we do not ever know the outcome of any situation, so there is always a risk in it not working out at all' [61].

IV: ULRICH BECK (1944-2015): MACRO-SOCIETAL THEORY OF RISK

'Risks are all around us, appearing in many forms. We face risks in new technologies (nuclear power, genetically modified crops) and old ones (dams, ladders), in modern medicine (stem-cell therapy, colonoscopy) and home remedies (herbs, diets), in familiar personal relationships (heartbreak, betrayal) and novel ones (online predators, identity theft), in simple savings (inflation, illiquid pension funds) and esoteric investments (collateralized mortgages, hedge funds), in familiar violence (robbery, sexual assault) and inventive forms (dirty bombs, anthrax attacks). Some risks have immediate effects (tainted food) and others delayed ones (saturated fats). Some affect us directly (personal losses) and others indirectly (employers' losses). Some are material (personal injuries) and others psychological (injury to loved ones). Some affect people (accidental poisoning) and others affect the natural environment that supports them (pesticides). Some are voluntary (skiing) and others are not (terrorism). Some involve one event (eating forbidden food) and others repeated events (eating unhealthy food) [2]'. This quote from Fischhoff and Kadvany say it all about omnipresence of risk–-both macroscopic and microscopic—all around us in our day to day lives in the modern society of risk averse culture. Beck's risk society perspective does not necessarily negate it but comes to regard quite boldlythe contemporary society as risk society, a sort of 'lingua franca' among critical risk researchers and in the risk research literature. 'What makes matters worse in Beck's reading is that the very institutions and instruments responsible for risk management are now part of the problem, wedded as they are to the frames of reference and types of solutions that produced the problems in the first place'[127].

Benefits of participatory risk governance	
Risk identification, framing and assessment	
1	Earlier and more complete identification of risk issues
2	Wider access to and use of diffused relevant information
3	Early warning on public sensitivity of certain risk issues
4	Identification and assessment of concerns and of interests, views and values at stake
5	Framing and focusing risk assessment on the most relevant issues and questions
6	More transparent, credible and accepted scientific risk assessment, providing a better view of uncertainties and value-laden assumptions
7	More robust common ground among authorities and stakeholders on the factual and scientific facts
8	Better chance to achieve a wider consensus on the relevance, relative weight and implications of the various dimensions and attributes of the risk in presence, as well as the benefits and risk-risk balance
Risk management	
1	More complete identification of policy options
2	More fairness in risk distribution
3	More legitimate assumptions on acceptable or tolerable residual risk, balance between risk and benefits and justification for the introduction of the technology, product, project etc. in question
4	Better chance to identify balanced solutions, overcoming/ reconciling conflicting interests
5	Better, more productive management of confrontational interlocutors trying to interfere with the risk management process
Risk communication	
1	More complete identification of stakeholders and publics to communicate/exchange with, and more direct and effective channels and processes for two-ways communication
2	Better and more relevant common ground of knowledge and facts as a basis for dialogue
3	More on-substance and less tactical stakeholder dialogue
4	Better mutual understanding between stakeholders and with the institutions
5	Better chance to dispel misunderstandings, prejudices, biases and correct wrong information and assumptions
6	Two-ways, structured communication contributing to better informed, more effective and consensual decisions
Implementation of risk policies and measures	
1	More collaborative and effective approach to policy implementation, notably on complex risk issues
2	More timely and more effective feedback on the results, problems, impacts and needs for revision of the measures applied

Table 13: Benefits of participatory risk governance

What is the rationale of examining Cloud computing technology against the backdrop Beck's perspective of risk society? Indeed there quite a few reasons, not being limited to seeking equivalence of Cloud computing risks to risks outlines by Beck in his risk society thesis or simply drawing parallel between Cloud computing risks and risks in the (late) modern or contemporary society. It is more than that in the sense that Cloud computing risks are not exceptional realities beyond Beck's explanation and amplification of worldwide risks grounded on two central technologies of governing: 'risk and uncertainty' [128].It is relevant to point out that work on cyber domain of risks and security in the light of risk society's perspective is already in progress. Kook strongly argues that "the borderless nature of cyber security, including the lack of defined threat or actor, the total involvement of a society in the security process, and the reflexive nature of cyber opportunity are all characteristics which are descriptive of a risk society. The discourse which surrounds cyber security shows the awareness of these attributes, exemplifying the fact that society is aware of the risk which characterizes cyberspace. State's understanding and the nature of strategy and policy show that cyber security is best understood when observed from a lens of risk society' [129].No less important to say that taking Beck's risk society's approach to techno-scientific risks, as a point of departure, clarifies and illuminates in novel way to appreciate risks of Cloud computing technology in its global ramifications and implications. 'It was Ulrich Beck who first showed that risk is a fundamental category for social theory'. It was by means of his concepts of risk society and reflexive modernization that Beck 'fundamentally shifted the focus from technical and rational approaches to risk such as *risk assessment* and *risk communication* toa socio-theoretical perspective that positions risk in the context of fundamental social change'. The increasing number of' 'citations' of *Risk Society* and Beck's 'publications' speak for themselves for Beck's pre-eminence as a theorist risk and security in the Figure:17 given below [130].

Some Frequent Defects in Risk Governance Practice		
Pre-assessment		
	1	No effective system to anticipate forthcoming risks in certain sectors
	2	Underestimation of the public sensitivity of certain risk-issues
	3	Undue delay in recognising relevant risk-issues (“not-in-my-mandate”)
	4	Ignoring societal aspects of risk-issues
	5	Failing to identify and involve the relevant stakeholders
Appraisal		
	1	Appraisal limited to the scientific aspects
	2	Failure to identify and assess concerns
	3	Risk assessment launched without a preliminary assessment of all the relevant dimensions of risk, not addressing all the relevant questions
	4	Risk assessment process not transparently recognising and addressing value-laden aspects and assumptions, uncertainties and other limitations
	5	Failure to ensure transparency and consultation at the appraisal stage
	6	Unbalanced representation of interests and stakeholders
Management		
	1	Incomplete identification of policy options
	2	Option identification and assessment not comprehensively considering the diverse perspectives on, and dimensions of the issues at stake
	3	Biased, unbalanced or incomplete criteria for the assessment of policy options, not properly addressing relevant values and interests
	4	Application of simplistic models
	5	Evaluation of option not fairly reflecting the distribution of risks and benefits
Communication		
	1	One way communication aimed at “explaining” risk and “selling” to the public unilateral conclusions and decisions
	2	Lack of clarity on the aims of communication and dialogue processes
	3	Inadequate means and resources for the management of the communication process
	4	Lack of mutual trust and respect between the actors involved in the communication
Follow-up		
	1	Failure to establish mechanisms to support and monitor implementation of measures, building on stakeholders networks established in the preparatory phase
	2	Failure to monitor results achieved and problems encountered
	3	Failure to recognise problems and timely introduce additional or corrective measures, or reconsideration and revision/withdrawal of measures

Table 14: Some Frequent Defects in Risk Governance Practice

While Beck was hailed as forecaster par *excellence* by some, his magnum opus, ‘Risk Society: Towards a New Modernity’, originally published in German in 1986 but translated into English in 1992, has been translated into ‘ 35 languages and sold hundreds of thousands of copies worldwide. It remains one of the most cited social theory texts of the last four decades’. Giddens called him ‘the greatest sociologist of his generation’ [131].Beck’s *Risk Society* ‘triggered heated debates across nations and specialist fields – in sociology and political science, in law and history, in philosophy, anthropology, ecology and engineering’ [132].Beck is ‘without a doubt one of the most productive and innovative sociologists of our time’[133].The material contexts of risky events that strengthened his views on the rise of risk society have already been mentioned in the introduction. In particular, the accidents and disasters in Seveso (1976),Three Mile Island (1979), Bhopal (1984) and Chernobyl (1986) were incentivizing forces that led Beck to come to terms with reality of risk society [130], and prompted him to go move away from a particular kind of fruitless *zombie science* (or the ‘science of unreality’) in mainstream sociology to reinventing ‘a new sociological imagination’ embedding the concept of new society that has emerged as risk society [134]. It is scarcely a surprise that Beck received a Lifetime Achievement Award from the International Sociological Association. The concept of risk society became a touchstone in debates across many disciplines, having impact on risk management policy and regulation including climate, on shaping the thinking of European Commission officials on risk governance and on facilitating ‘the enactment of the precautionary principle in international agreements and the European Union’s 1992 Maastricht Treaty, which, in turn, exercised substantial influence on risk regulatory decision-making [135]’. No less important to mention here that numerous iconic events including the 9/11and 7/7 terrorist attacks ‘served to further embed risk into the media and political mainframe’ and risk became ‘ a ubiquitous topic of discussion in areas as diverse as healthcare, immigration, pensions and national security’[136].

Figure16: The qualitative importance of risk culture

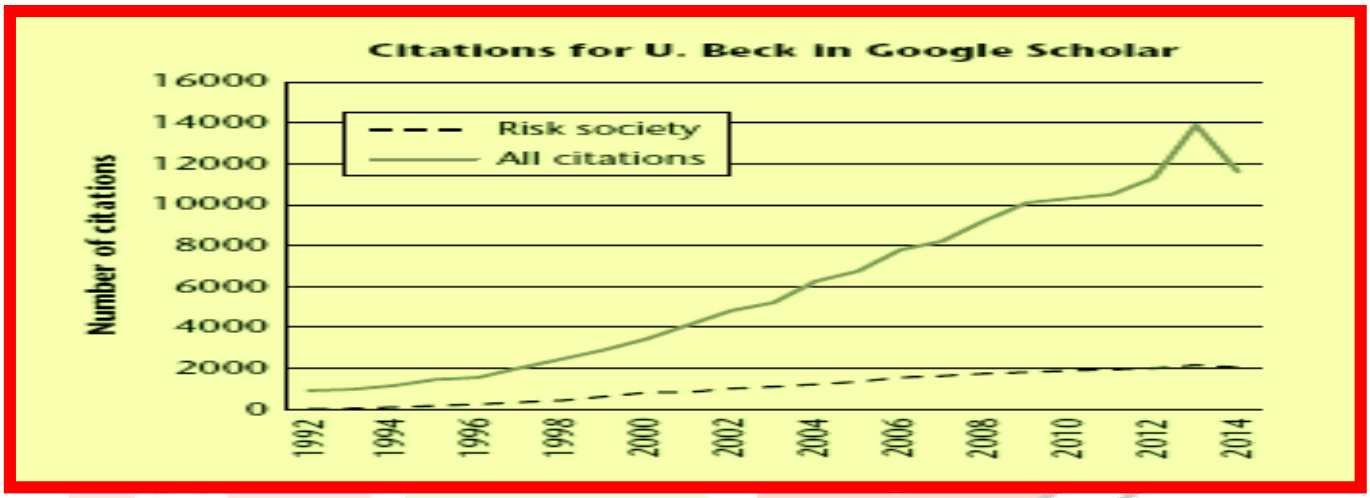


Figure17: Citations for U. Beck in Google Scholar

Having described the person and his achievements, it is necessary to contextualize briefly the emergence of risk society narrative within the historical and intellectual milieu of academic studies and research done earlier. Mythen informs that risk analysis arose in the 1950s with attempts made to understand and assess hazards and threats, eventually leading to the appearance of a culture of probabilistic risk analysis and also to the development of different forms of statistical modeling within engineering and mathematics by contributions within the decision science in the 1970s. It got further enriched by researches on risk perception and classification of risks within the psychometric paradigm along with contributions in decision science and psychology in the 1980s. These developments were further aided by contributions o from anthropology, sociology and media studies covering such issues as connections between processes of risk definition, perceptions of risk, and the reproduction of social order on the one hand and Social Amplification of Risk's modeling the interconnections between the processes of risk definition, representation, and reception, on the other hand. In the 1990s studies in the culture of fear and its threat in the society made their appearance [137].

At the same time, a few words need to be said in respect of material happenings on the ground that took place in connection with negative impacts of industrialization due to increasing environmental problems accompanied by popular movements and ideological battles ultimately leading to the acceptance of development model based on the paradigm of sustainable development for all societies. The forecasting of the planet rendered uninhabitable by expanding industrialization in the north, voiced by mounting popular distress in the North was compounded by grim realities, depicted by *Silent Spring* (1963), *The Population Bomb* (1970) and *The Limits to Growth* (1972), pointed to the resource base, spreading pollution, and ever growing population especially in the South , which demanded to catch with the standard of living and quality of life in the North. As a result, so Reed comments, 'the environmental agenda of the industrialized societies collided head-on with the political perspectives and priorities of the developing world. In contrast to industrialization problems of the North, the developing countries identified the issue of poverty alleviation as their most challenge to arresting environmental degradation'. The conflicting perspective for remedial measures for environmental problems was successively taken up foe arriving at a global consensus in successive world Conferences, viz., the Stockholm Conference (1972), the formation of the *World Commission on Environment and Development* (1984) whose Report was published as *Our Common Future*(1987), *The Rio Conference* (1992) also known as the Earth Summit in Rio de Janeiro , and lastly the *World Summit on Sustainable Development* (2002) in South Africa. In brief, while they provide a global backdrop in the light of which Beck's risk society concept can be viewed and understood , they also led to the principle of sustainable development - meaning improvement of 'the quality of human life while living within the carrying capacity of supporting ecosystems' [138].

IV. I. CONCEPTUALIZING RISK SOCIETY THESIS AND THE HISTORICAL EMERGENCE OF RISK SOCIETY

Beck, while theorizing risk society, started from the methodological standpoint that considers nether realism nor constructivism as an either or option. As he said: 'I am both a realist and constructivist, using realism *and* constructivism as far as those meta-narratives are useful for the purpose of understanding the complex and ambivalent 'nature' of risk in the world risk society we live in'[139]. With such methodological point of departure, supported by others [140],Beck captures the changing roles of some mainstream as well as new issues, which are both social and physical in nature, and they include such issues as the individual, the family and marriage, global warming, and climate change, health risks such as AIDS, biological warfare, BSE, worldwide automobility, nuclear accidents, terrorism and so on and so forth. These constitute what is known in academic parlance as risk society of which the current issues are neither purely social nor are they simply physical [141]. They provide 'a new and optimistic model for understanding our times' [139] for all developments that took place since the mid-twentieth century onward. Risk society thesis practically lays bare a concept of risk society encapsulating 'a theory of society' and 'the cultural diagnosis' that designates 'a stage of modernity in which the hazards produced in the growth of industrial society become predominant' [142]. Actually, Beck's risk society has undeniably become one of 'the foremost theoretical treatise on societal risk' elevating risk to centre stage as a prime analytical tool for understanding the dilemmas of late modernity' [143]. What is a risk society? The concept of risk society points up three dimensions of the epochal transformation of the industrial society. First, it highlights how, within the onward progressive movement of modernization, the modern industrial society is using up the resources of nature and culture, thus imperiling its own existence. Second, the concept of risk society illustrates how the industrial society's relationship to the hazards and problems that it has produced has indeed upset 'the bases of societal conception of security'. Third, it also attests to the erosion and disintegration of the cultural values meanings (viz. faith in progress, class consciousness, etc) of the industrial society, generating the social forces of what he calls the 'individualizing process [142]. For Beck, the risk society is a kind of society that systematically produces, defines and distributes 'techno-scientifically produced risks'. Accordingly, (risk) problems and conflicts in such a society arise 'from the production, definition and distribution of techno-scientifically produced risks' [144]. Elsewhere Beck argues that the term 'risk society' is used 'for those societies that are confronted by the challenges of the self-created possibility, hidden at first, then increasingly apparent, of the self-destruction of all life on this earth' [145].

Risk can be defined as "a *systematic way of dealing with hazards and insecurities induced and introduced by modernization itself*' [144]. In 1986, when he first published *Risk Society* in Germany, Beck was unaware of the distinction between risk and hazard. In 1988 he recognized the distinction and incorporated it in his work [133]. He redefined the concept of risk distinguishing it from hazard: ''Risks' are understood here (similarly in principle to the prevailing conception) to be determinable, calculable uncertainties; industrial modernity itself produced them in the form of foreseen or unforeseen secondary consequences, for which social responsibility is (or is not) taken through regulatory measures. They can be 'determined' by technical precautions, probability calculations, etc., but (and this is frequently not taken into account) also by social institutions for attribution, liability and by contingency plans. There is, accordingly, a consensus in international social-scientific literature that one should distinguish here between preindustrial hazards, not based on technological-economic decisions, and thus externalizable (onto nature, the gods), and industrial risks, products of social choice, which must be weighed against opportunities and acknowledged, dealt with, or simply foisted on individuals'[145]. Relevant here also is his distinction between risk and catastrophe, clarifying that 'risk is *not* synonymous with catastrophe. Risk means the *anticipation* of the catastrophe. Risks concern the possibility of future occurrences and developments; they make present a state of the world that does not (yet) exist. Whereas every catastrophe is spatially, temporally and socially determined, the anticipation of catastrophe lacks any spatio-temporal or social concreteness. ... Risks are always *future* events that *may* occur, that *threaten* us. But because this constant danger shapes our expectations, lodges in our heads and guides our actions, it becomes a political force that transforms the world' [142]. Risk, as a way of reducing indeterminacy or uncertainty, became indeed one of the key ideas which became an integral component of 'modernity' [146].The concept of modernity surfaced in the in the seventeenth-century Enlightenment and is linked to the idea that human progress and social order can be achieved with the instrumentality of scientific exploration and rational thinking. Modernity is thus based on the assumption 'that the social and natural worlds follow laws that may be measured, calculated and therefore predicted' [147]. By the beginning of the twenty-first century there emerged a consensus among concerned experts and publics on the fact that , as Beck reminds, modernity has already become 'a *technologically constituted* world, and one that will become even more so in the future' [148]. What is more, Beck came to regard 'modernity' as industrial society whose driving force is science and technology [149].

Against this backdrop of the emergence and continuity of modernity Beck situates the advent of the risk society in the light of changing threats within the modern (Western) society, causing its historical transformations in three distinct eras: preindustrial or traditional society, industrial society or first modernity, and risk society or second modernity. His classification is based on causative agents such as natural hazards for the traditional/pre-industrial society, industrial accidents for the industrial society/first modernity, and human manufactured risks for the risk society/second modernity. Table 15 provided by Beck points to the epochal transformations of the society [145]. In pre-industrial societies there were no risks as defined above. These societies were struck only by unforeseen natural hazards, threats or dangers such as earthquakes, famines, droughts or floods that were not the outcome of intentional human acts and decisions but whose causality was attributed to the external forces such acts of gods, demons or some other supernatural forces. Second, all this changes with the emergence of the classical industrial society since the middle of the eighteenth century. In this first phase of the industrial society risks or hazards, whether they emanate from factories or unemployment, result from decisions consciously taken by the individuals and society. However, because it is premised on the dominant public faith on such values as cumulative progress, increasing productivity and production, preservation of jobs and generation of wealth, the industrial society denies the existence of risks if they threaten those values, on the one hand, or if they cannot be defined in terms of probabilities and hence cannot be calculated, on the other. Finally, in the second phase of modernity, the industrial society involuntarily mutes 'into risk society through its own systematically produced hazards' [142]. By the time this happens, risks become historically specific and unique in several respects, warranting redefining industrial society as risk

society in the late modernity, especially since the 1970s [150]. In this phase of emergent risk society, 'the suspicion has become almost universalized that industry *is* emitting products that can harm us, and is making claims of safety they can't back up. We start to suspect the worst even when they are boasting. The consciousness of risk begins to surround progress like a shadow encircling the light' [151].In the changed situation risks as manufactured uncertainties become unpredictable, global, invisible, incalculable and beyond insurance. Thus the third type of historical development appears in the reality of risk society. The industrial society transforms it into a risk society that has become '*an uninsured society*, with protection paradoxically diminishing as the danger grows' [142]. Put otherwise more concretely, the key dissimilarity between industrial society and risk society is that 'whereas in the former, institutions and technological systems such as the welfare state, provided a relatively stable framework in which these risks could be assessed and managed, in the latter, such institutions persistently fail to transform risks into securities. Risk containment itself has become contaminated'[149].The development of Risk Society comes to full circle with its leading parameters, as put forth by Ekberg in Figure 18.These parameters provide a synoptic perspective on the risk society which extends the traditional concept of risk beyond the actuarial conceptualization of risk as the calculation of the probability of an adverse event and the magnitude of its consequences by including 'include the subjective perception of risk, the intersubjective communication of risk and the social experience of living in a risk environment'[134].Risk society, for Beck, is 'a developmental phase of modern society in which the social, political, economic and individual risks increasingly tend to escape the institutions for monitoring and protection in industrial society'[152]. Different contrasting dimensions of the industrial society and risk society, which are also their characteristics, are shown in Table 16 as provided by Sørensen and Christiansen [133].

TYPE OF SOCIETIES >	PRE-INDUSTRIAL HIGH CULTURES	CLASSICAL INDUSTRIAL SOCIETY	INDUSTRIAL RISK SOCIETY
Type and example	**Hazards, natural disasters, plague**	**Risk, accidents (occupational, Traffic)**	**Self-jeopardy, man-made disasters**
Contingent upon decisions?	**No: Projectable (gods, demons)**	**Yes: industrial development (economy, technology, organization)**	**Yes: nuclear, chemical, genetic industries and political safety guarantees**
Voluntary (individually avoidable?)	**No: assigned, pre-existing assigned destiny**	**Yes (e.g. smoking, driving, skiing, occupation) rule-governed attribution**	**No: collective decision, individually unavoidable hazards; yes and no (organized non-responsibility)**
Range: who affected	**Countries, peoples, cultures**	**Regionally, temporally, socially circumscribed events and destruction**	**Undelimitable 'accidents'**
Calculability (cause-effect, insurance against risks)	**Open insecurity; Politically neutral, because destined**	**Calculable insecurity (probability, compensation)**	**Politically explosive hazards, which render questionable the principles of calculation and precaution**

Table15: Beck's Three Phases of the development of Society and their Risks and Hazards

The transition from the first modernity (modern industrial society), emerging from the mid -1950s to the 1970s, culminated in the emergence of risk society in the second modernity of late modern industrial society in the 1980sonward was catalyzed by five social forces: (1) globalization; (2) individualization; (3) gender revolution; (4) underemployment; and (5) global risks (as ecological crisis and the crash of global financial markets) [142]. Sorensen and Christiansen relate underemployment as due to the impact of The Third Industrial Revolution based on the rise of Information and Communication Technologies (ICTs)m which reduced the demand for manual labor ' unintended side effects of the kind of rationalization drive which is inherent to global capitalism'[133]. Beck indeed was not oblivious of what was happening in the domain of the ICTs and referred to 'microelectronics'[144], 'global digitalization and networking' enabling the economy 'to operate as a unit in real time right across the planet' [153], 'information technology' making it 'possible to have digital capitalism'[151].In brief, the decline of the 'full-employment society' is one of side effects of the kind of rationalization inherent in global capitalism which is, in turn, now driven by the new technologies of the third industrial revolution [133]. The first industrial modernity was characterized by (1) nation-

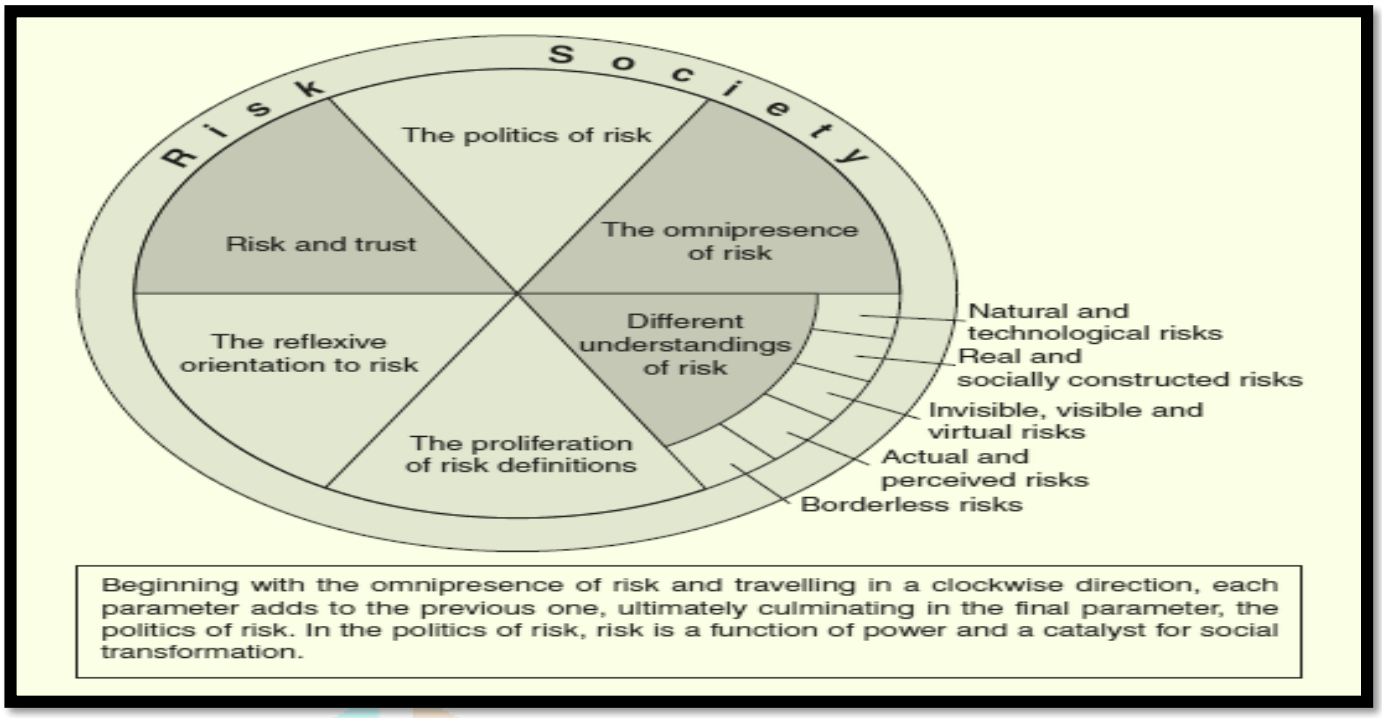


Figure 18: A Conceptual Map of the Six Interconnected Parameters of the Risk Society

state societies; (2)a programmatic individualization (institutionalized individualism); and (3) gainful employment societies with full employment. These were based (4) an instrumental view of nature; (5) a scientifically defined concept of rationality; and (6)the principle of functional differentiation. If these were the basis premises or foundation of the first modernity, they are eroded by the five catalytic social forces mentioned above and, eventually, gave rise to the second modernity [133]. In Beck's words, if the firsr industrial modernity was characterized by 'collective lifestyles, full employment, the national state and the welfare state, and an attitude of heedless exploitation of nature', then the second industrial modernity – pointing to the emergence of risk society – was characterized by 'ecological crises, the decline of paid employment, individualization, globalization and gender revolution'. [153]. Figure 19, provided by Sorensen and Christiansen, illustrate this transition from the first to the second modernity. The connecting link, as a motor of societal mega-change, is the process of reflexive modernization 'meaning the possibility of creative (self) destruction' for the entire epoch of industrial society [154].

Characteristics of Industrial Society and Risk Society		
No	INDUSTRIAL SOCIETY	RISK SOCIETY
1	Production of wealth	Production of risks
2	Elimination of scarcity/need	Elimination of risks
3	Wealth distribution	Risk distribution
4	An aim to achieve	An aim to avoid
5	Combating reality	Combating possible futures
6	Positive focus on the possibilities of the future	Negative focus on the future's potential disasters
7	Being determines consciousness (materialism)	Consciousness determines Being (idealism)
8	Poverty	Anxiety
9	I am hungry	I am afraid
10	Us/them distinctions (rich/poor, American/Russian etc.)	Us/them distinctions are diluted And lose meaning
11	Need is hierarchic	Smog is democratic
12	The industrial process is apolitical	The industrial process is political (the sources of wealth are also the sources of pollution)

Table 16: Industrial Society versus Risk society

IV. II. REFLEXIVE MODERNIZATION

Reflexive modernization lies at the back of 'fundamental societal transformation within modernity'. It takes into account 'the whole breadth of the modernization process. The structural break is explained not as a result of exogenous factors but as a consequence of modernization itself. Once modernization has been radicalized, it affects all spheres of society' [155]. Reflexive modernization, in a word, can be called 'modernization of modernity itself' and reflexive modernity occurs 'when modernity

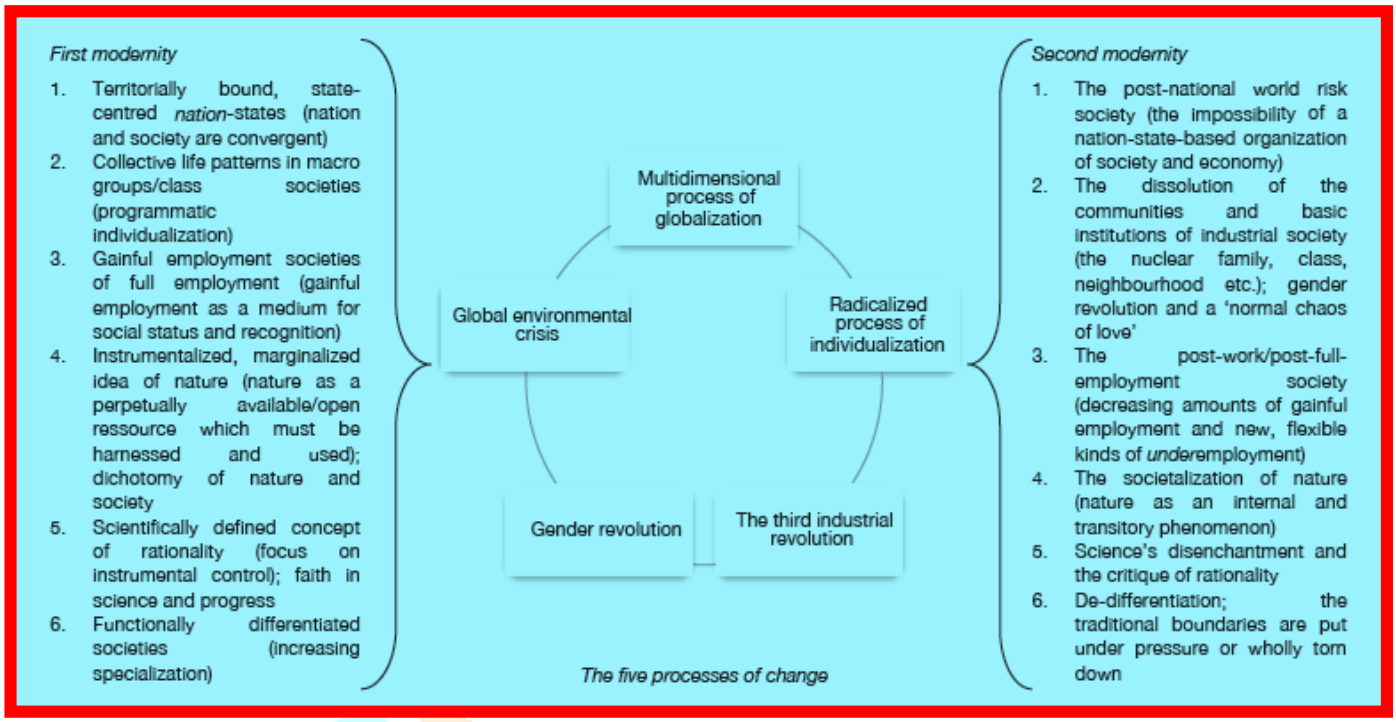


Figure 19: Transition from the First to Second Modernity

encounters itself, in the shape of the side effects and the unintended consequences of the first, simple-linear modernization' [133]. The concept of 'reflexivity' in reflexive modernization does mean '*reflection*' but 'self-confrontation' which emerges as an outcome of unintended side effects (of industrial society) which modernity itself criticizes [154]. Having distinguished the two concepts, it should now be stated that the transition from industrial society to risk society occurs in two distinct. In the first phase self endangerment of the industrial society takes place in terms of production of side effects which do not become the subject of public debate or political conflict. This phase is dominated by' the self-identity of industrial society, which simultaneously both intensifies and 'legitimates', as 'residual risks', hazards resulting from decisions made ('residual risk society')'. This changes dramatically in the next phase when hazards, produced and legitimated by industrial society, dominate public, political and private debates due to institutional inability to control those hazards. During this transition, 'industrial society sees and criticizes itself *as* risk society. On the one hand, the society *still* makes decisions and acts on the pattern of the old industrial society; on the other hand, debates and conflicts which originate in the dynamic of risk society are already being superimposed on interest organisations, the legal system and politics' [156].

The inherent dynamic of reflexive modernization forces the erstwhile industrial society 'to see itself as a risk society' [147].To quote Beck: 'The transition from the industrial to the risk epoch of modernity occurs intentionally, unseen, compulsively, in the course of a dynamic of modernization which has made itself autonomous, on the pattern of *latent side-effects.* One can almost say that the constellations of risk society are created because the self-evident truths of industrial society (the consensus on progress, the abstraction from ecological consequences and hazards) dominate the thinking and behaviour of human beings and institutions. Risk society is *not an option* which could be chosen or rejected in the course of political debate. It arises through the automatic operation of autonomous modernisation processes which are blind and deaf to consequences and dangers. In total, and latently, these produce hazards which call into question - indeed abolish-the basis of industrial society' [156].Figure 20 of the dynamics of reflexive modernization is provided by Bulkeley [157]. There are other important dimensions, other than **reflexive modernization,** that characterize risk society, viz., **world risk society, individualization**, **risk regime** (work society as risk society), **uncertainty**, and **risk management and assessment** Before these are briefly touched upon, the stark contrasts between the industrial and risk society, as updated by Rosa [158] in Table 17, may be perused.

IV. III. WORLD RISK SOCIETY

'Risk society, fully thought through, means world risk society. For its axial principle, its challenges are dangers produced by civilization which cannot be socially delimited in either space or time. In this way basic conditions and principles of the first, industrial modernity – class antagonism, national statehood as well as the images of linear, technical-economic rationality and control – are circumvented and annulled' [142]. In other words, the concept of world risk society exhibits limited controllability of the dangers the risk society itself has created. The issue is therefore 'how to take decisions under conditions of manufactured uncertainty, where not only the knowledgebase is incomplete, but more and better knowledge often means more uncertainty' [142]. Elsewhere, Beck defines world risk society in this way: 'The very power and characteristics that are supposed to create a new quality of security and certainty simultaneously determine the extent of *absolute uncontrollability* that exists. The more efficiently and comprehensively the anticipation of consequences is integrated into technical systems, the more evidently and conclusively we lose control. All attempts at minimizing or eliminating risk technologically simply multiply the uncertainty into which we are plunging the world'[148].Take for instance, the omnipresent accumulation of ecological, terrorist, military, financial, biomedical and informational risks today [159]. Risks have an inherent tendency towards globalization. Thus industrial production of hazards becomes universalized such as food chains connecting everyone regardless of territorial boundaries. Again, The acid content of the air is not affecting the sculptures and artistic treasures, it has also brought about the disintegration of modern customs barriers [144] Global risks like climate change is an unique example, for it is more than simply a climate change;

'it is at once much more and something very different. It is a reformation of modes of thought, of lifestyles and consumer habits, of law, economy, science and politics. Whether presenting climate change as a transformation of human authority over nature; as an issue of climate (in)justice; as concerning the rights of future generations; or as a matter of international politics and international trade; or even as an indication of suicidal capitalism – all this is about the dramatic power of the unintended, unseen emancipator side effects of global risk, which already have altered our being in the world, seeing the world and imagining and doing politics'[160].

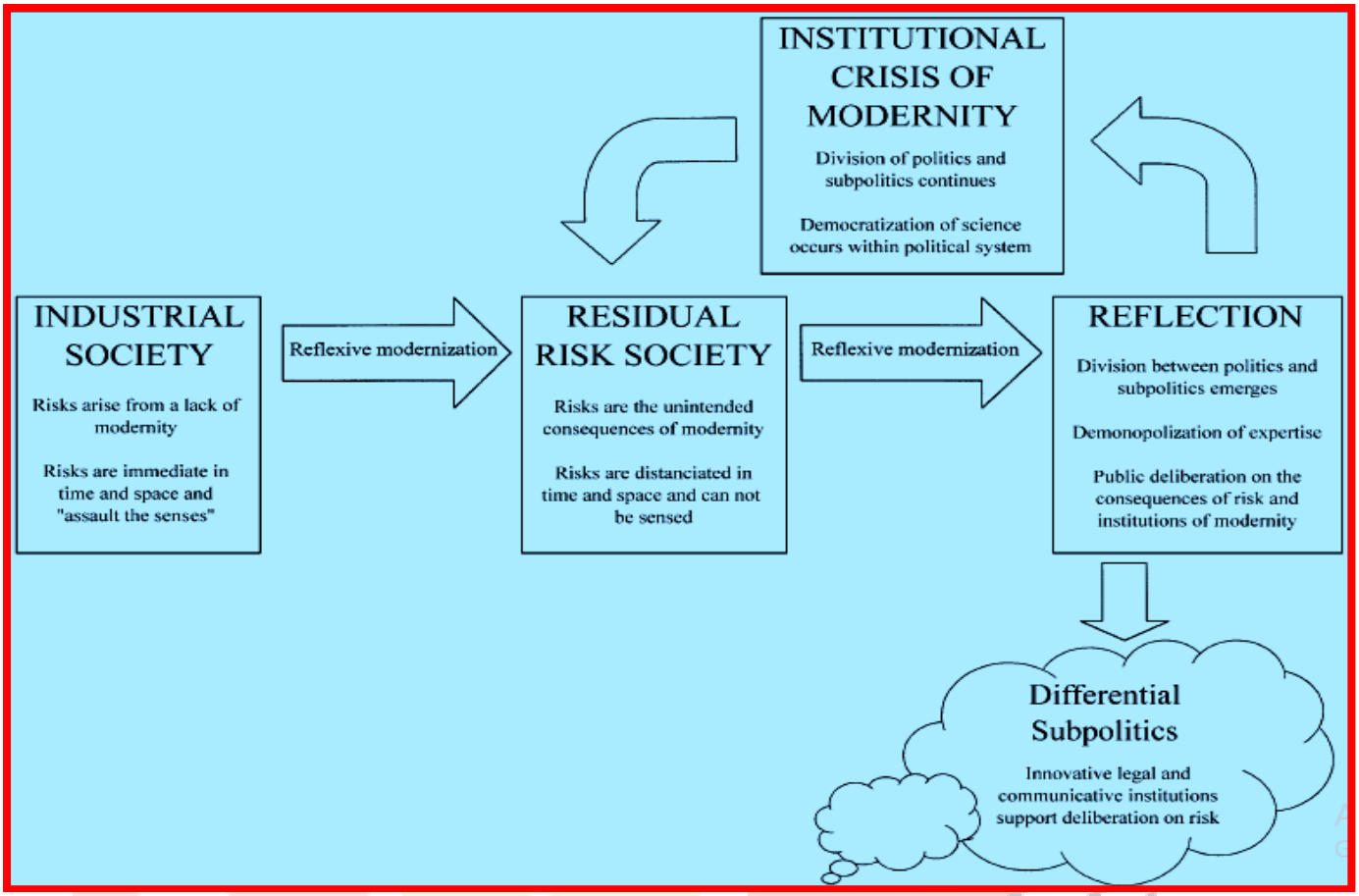


Figure 20: The dynamics of Reflexive Modernization

There are two variants of global risks. On the one hand there are unintended global catastrophes such as climate change or financial crisis, among others. On the other hand, there are intentional catastrophes, such as transnational suicidal terrorism, in which there is a lack of clear identifiable agent(s). [159]There are three features of world risk. The first is delocalization in the sense that there are certain risks which are omnipresent and their causes and consequences are not limited by geographical location or space. Second, there are global risks whose consequences are incalculable since they involve hypothetical or virtual risks which are basically based on 'science induced not-knowing and normative dissent. The third feature is their non-compensability. The new threats defy the logic of compensation and are substituted by the principle of '*precaution through prevention'*. In this case, 'not only is prevention taking precedence over compensation: we are also trying to anticipate and prevent risks whose existence has not been proved' [161]. The world risk society, which emerged since the 1960s [162], is not an egalitarian society, for the power structure in the world risk society is based on a division between those who produce and profit from risks while others are affected by the same [142].'The "proletariat" of the world society of risk live beneath the chimneys and alongside the refineries and chemical plants in the industrial centers of the third world' [163].This society remains basically capitalist, though it is 'a new kind of capitalism' [164]. And world risks become commoditized in the profitable risk industry with expanding markets. Thus Beck caustically remarks that 'the diffusion and commercialization of risks do not break with the logic of capitalist development completely, but instead they raise the latter to a new stage. There are always losers but also winners in risk definitions. The space between them varies in relation to different issues and power differentials. Modernization risks from the winners' points of view are *big business*. They are the insatiable demands long sought by economists. Hunger can be sated needs can be satisfied, but *civilization* risks are *a bottomless barrel of demands* unsatisfiable, infinite, self-producible' [144]. Risks represent not only 'dark side of opportunity' but also at the same time 'market opportunities' in the risk(capitalist) society. In the 'advanced capitalism', Beck argues, 'Demands , and thus markets, of a completely new type can be created by varying the definition of risk, especially demand for the avoidance of risk - open to interpretation, causally designable and infinitely reproducible'[144] . Following Beck, Krahman shows that risks have undergone further expansion and in turn, have promoted commodification of security and expansion of markets, eventually leading to intensification of the world risk society. 'Initially, businesses focussed on the provision of security as related to physical dangers such as robbery and burglary. In recent years, however, the search for new sales opportunities has encouraged firms across a widening range of economic sectors, from

	Modern Industrial Society	Risk Society
Origin of mega-risks	Earthquakes and floods are caused by nature or God	Climate change is caused by human decision making
Modernization process	Simple modernization from agrarian to industrial society (modernization of tradition)	Reflexive modernization from industrial to risk society (radicalization of modernization and rationalization of rationalization)
Prevailing type of differentiation	Class positions (rich versus poor) from distribution of goods	Risk positions (different grades of "affected") from distribution of bads
Transformation of human actors	Detraditionalization and early individualization	Heightened individualization
Human perception of risks	Retention of cognitive sovereignty	Loss of cognitive sovereignty (dependence on science to tell us how badly we are in trouble)
Emerging mode of science	Primary scientization	Reflexive scientization
Main line of conflict	Relations of production	Relations of definition
Preeminent political paradigm	Retention of national sovereignty	Emergence of cosmopolitanism
Management of risks	Attempts are appropriate to the magnitude and scope of risks	Magnitude and scope of risks outpace conventional attempts to manage them

Table 17: Contrasts between Industrial Society and Risk Society

healthcare and food to consumer goods, to indentify a wide variety of risks to the safety and wellbeing of peoples. This expansion of the private market in risks has contributed to the emergence of the world risk society through its discourse of unknown and unknown-unknown risks, and by offering to contain the uncontainable [165].

However, the numerous developments, including ones stated above, that are taking place within the womb of world risk society are also at the same time giving way to a cosmopolitan turn in the modern society. The so-called 'methodological nationalism' based on the 'container theory of society'–centering around omnipotent territorial national state – has become an obstacle to understand and analyze 'the dynamics , conflicts, ambiguities and new perspectives of world risk society'. The second modernity, while eroding 'methodological nationalism' along with the container theory of society, has unleashed new social processes embedded in the reflexive modernization which stresses 'the importance of the potentially transformative power of global risk conflicts and definitions' [159]. In addition, thus, it no surprise that nowadays people transcend national boundaries and 'shop internationally, work internationally, love internationally, marry internationally, research internationally, grow up and are educated internationally (that is, multi-lingually), live and think transnationally, that is, combine multiple loyalties and identities in their lives' [164].Technologically viewed, BSE(Bovine Spongiform Encephalopathy or mad cow disease) provides an 'explosive reminder of the inability of both nation-states and transnational decision-making bodies like the EU to manage risk in a chaotically interacting world risk society' [161]. Global risks are thus enforcing cosmopolitanism by tearing down national boundaries, making the distant other into inclusive other, and enabling people to make sense of their own life in exchange with life experiences of others in different parts of the world [166] [167]. Cosmopolitanism means 'global interrelationships and a transnational vocabulary of symbols, but it also means deep engagement in local activities, local consciousness, connection to local people. It means having wings and roots at the same time' [162]. Simply stated, the enforced cosmopolitanism, developing in the second industrial modernity, implies that global risks 'activate and connect' people across borders, people who would not have interacted otherwise [168].

IV. IV. INDIVIDUALIZATION

The concepts of risk society, reflexive modernization, and individualization are the interrelated central concepts of Beck [147]. As sar as individualization is concerned, it was based on affluence in the 1970s and 1980s. But since the early 1990s the process of individualization is based rather on the 'precarious conditions of life in capitalism *without work*'. Neither does it mean that people 'automatically want to live as individuals and relate to one another as individuals'. It is not the '*neoliberal idea of the free-market individual*'. It does not mean 'autarkic human self' or 'self-entrepreneur'. It does mean 'individualism' or 'individuation' which means 'the process of becoming an autonomous individual'. Neither does it refer to what Habermas calls 'emancipation' [169].

It does not stand for 'possessive and egoistic individualism' of Thatcher and Reagan or refer to contemporary 'global free-market liberalism'. Beck's concept is quite different from' even the ethical and altruistic individualism of the Enlightenment' which is more about 'being individual' than 'becoming-individual at all' [170]. Moreover, Individualization is not equivalent to 'mere management of self-image anymore than it can be equated with mass self-authenticity' [171].

The concept of individualization is thus, needless to say, not 'a celebratory ideology' but, rather, 'a concept which describes a structural transformation of society's institutions. It describes a change in the relation of the individual to society'. What individualization means in a 'constellation is *disembedding without re-embedding*'. In the second modernity 'the individual becomes, for the first time in history, the basic unit of social reproduction'. In the first modern industrial society roles and role sets were defined and prescribed for the individual actions and lives. One could not change the role or role sets without wrecking them and thus jeopardizing the order and stability of the society. All this changes with the advent of second modernity, i.e., risk society in view of the institutional developments in the domains of the educational system, the labor market, in the career patterns that followed from their interaction, and in the family structure will link them all. Now, instead of the role-sets, the individuals have the institutionalized have the freedom to choose from a variety of options through negotiation with no certainty that the options they choose are necessarily compatible. Accordingly, individual agency comes into being as a central dimension of the life experience, and his action is not longer an outcome collective pressure or an product of social attributes [171]. In the second modernity, the individual's normal biography turns into 'the 'elective biography', the 'reflexive biography', and the 'do-it-yourself biography'. The do-it-yourself biography is, however, always a 'risk biography', actually a 'tightrope biography', a kind of enduring '(partly overt, partly concealed) endangerment'. In any case, as Beck says, 'if they are not to fail, individuals must be able to plan for the long term and adapt to change; they must organize and improvise, set goals, recognize obstacles, accept defeats and attempt new starts. They need initiative, tenacity, flexibility and tolerance of frustration. Opportunities, dangers, biographical uncertainties that were earlier predefined within the family association, the village community, or by recourse to the rules of social estates or classes, must now be perceived, interpreted, decided and processed by individuals themselves. The consequences – opportunities and burdens alike – are shifted onto individuals who, naturally, in face of the complexity of social interconnections, are often unable to take the necessary decisions in a properly founded way, by considering interests, morality and consequences' [169]. In other words, the individual in the individualized society becomes 'the reproduction unit for the social in the life-world' and what the 'social' is or does has to with the decision of the individual who is at the center of action like 'the planning office with respect to his /her own biography, abilities, orientations, relationships and so on'[144]. One very serious implication of thisis that individualization process rests on the reality of 'I am I', rather than 'I think, therefore, I am' [170].The 'life of one's own is a reflexive life' and thus biography becomes basically a self-reflexive process requiring active management for conducting 'one's own life' amid diverse and contradictory identities, demands, uncertainties and risks [169].Reflexivity is a sort enabler to take on therisk society 'more positively in pursuit of an alternative modernity' and is also 'an effective concept in a critique of instrumental rationality'[149] Even then, individualization is not based on 'free decision of individuals' who are rather 'condemned to individualization' and thus it becomes 'compulsion' for them [154].

This phenomenon generates what is called 'tragic individualization' in the sense that the individual 'must cope with the uncertainty of the global world by himself or herself. Here individualization is a default outcome of a *failure* of expert systems to manage risks. Neither science nor the politics in power, nor the mass media, nor business, nor the law or even the military are in a position to define or control risks rationally. The individual is forced to distrust the promises of rationality of these key institutions. As a consequence, people are thrown back on to themselves, they are alienated from expert systems but have nothing else instead. *Disembedding without embedding* – this is the ironic–tragic formula for this dimension of individualization in world risk society' [172]. For instance, one as a responsible consumer is forced to decide whether to eat genetically modified foods which may have their unforeseeable or unknowable long-term consequences, to wear a seatbelt, touch a stranger, to eat or to have or not to have a pre-emptive mastectomy which may lead to breast cancer. Therefore the choices the individual makes are not free choices which are forced on to him/her but which are often untrustworthy sources [149]. Table 18 illustrates a synoptic view of the transformation of the individualization process from first modernity to second modernity [133].

Simple individualization versus reflexive, radicalized individualization

First wave of individualization⟶Second wave of individualization	
Industrial society/first modernity⟶ Risk society/second modernity	
Individualization in relation to the social structures and communities of feudal society	**Individualization in relation to the social structures and communities of industrial society** **Institutionalized individualization (the labour market, educational system and rights of the welfare state are all directed towards the individual)**
Replacement communities: class, status, family, nation	**Replacement communities are subjected to fundamental changes l loss of significance**
Born into a certain status and class	**Born into the framework of second modernity: institutionalized individualism**
The life trajectory of the individual is (largely) predetermined	**The life trajectory of the individual must be created/chosen** **Autobiographies of choice**

	Do It Yourself (DIY) biographies **Reflexive autobiographies** **Tightrope walkers' biographies** **Risk biographies** **Hazard biographies** **We are condemned to individualization** **(Sartre: condemned to freedom)**
Fixed connections, forced connections, predetermined connections (work, education, love, family etc.)	**The 'for now' prevails (Zygmunt Bauman)**
Nature and tradition will decide: religion, gender, identity. marriage, parenthood	**Must be chosen/created/invented by the individual: 'Who and what would you like to be?'**

Table18: Transformation of Individualization from First Modernity to Second Modernity

IV. V. CLASS *VIS*-À-*VIS*INDIVIDUALIZATION

An obverse of individualized society is class society, which does not have any significance in Beck's risks society. Marx advanced the conception that 'capital is the all-dominating economic power in the bourgeois society' [173]. In contrast, for Beck, risks, ecological, nuclear and other threats, are all-pervasive concerns of the modern (industrial capitalist) risk society in the second modernity since risks affect everybody –'property, capital, jobs, trade union power, the economic foundation of the whole sectors and regions, and the structure of nation-states and global markets' [142]. In the risk society 'the logic of risk production—bads—dominates the logic of wealth production–goods. 'The risk society is thus not a revolutionary society, but more than that, a *catastrophic society.* In it the *state oj emergency* threatens *to become the normal* state'. In Marxian class society the focus is on achieving 'equality', while the basis and motive force in the risk society is security or 'safety'. If in class society 'being' determines 'consciousness', in the risk society 'consciousness' or knowledge determines 'being'. The driving force in class society is '*I am hungry*', whereas in the risk society it is 'I am afraid' [144]. Class categories, if conceptualized on the basis of households or families, income or structures of work and employment, are of little use in the changed societal circumstances in the emergent risk society [169].In the wake of dissolution by reflexive modernization of the parameters of industrial society – class culture and consciousness, gender and family roles –there has occurred '*a social surge of individualization'* and consequently 'we increasingly confront the phenomenon of a capitalism *without* classes , but with individualized social inequality and all the related social and political problems'[144].

Individualization, rather than class, has thus become the essence of the societal structure of the late modern, i.e., risk society. To quote Beck: 'Individualization no longer only affects the superstructure of ideology and false consciousness, but also the economic substructure of "real classes." *For the first time in history, the individual rather than the class is becoming the basic unit of social reproduc*tion. ... Instead of individualism being placed in context and relativized by class analysis, in order to understand class we now need to place it in the new context of individualization. This is true of every social collectivity. They all have to be reinterpreted in the context of disembedded individualization. They are all being transformed. Individualization is the social structure of the second modernity [171].The concept class has become 'a zombie category' [169]. In the context of the new risks emerging from recent events (viz. Chernobyl, 9/11, climate change, the financial crisis, Fukushima, Euro crisis) Beck points out, in reply Curran's defence of the usefulness of class category[174], that epistemological monopoly of the category of class over social inequality needs to be overcome; and that historical classes require to be detached or uncoupled from social inequality. He strongly argues that 'the social structuring of the distribution of bads' from risks will be shaped 'not only by class, but also by other forms of social structuration of disadvantage, such as gender and race'. Thus he concludes by saying that class is '*too soft* a category to capture the explosiveness of social inequality in world risk society' and that 'risk, and not class or war, is the determining factor of power, identity and the future [175].

IV. VI. GLOBALIZATION

Globalization and individualization are at bottom two sides of the same coin, i.e., two sides of the same process of reflexive modernization in Beck's risk society thesis [154]. They are 'the constitutive features of the second modernity' [170].Risks are inherently globalizing, which equalize both the perpetrators and the victims of risk defying the territorial limits of the nation state. Reduced to a formula risks imply that 'poverty *is hierarchic, smog is democratic'* in the process of their distribution: 'They possess an *inherent tendency towards globalization.* A universalization of hazards accompanies industrial production, independent of the place where they are produced: food chains connect practically everyone on earth to everyone else. They dip under borders. The acid content of the air is not only nibbling at sculptures and artistic treasures, it also long ago brought about the disintegration of modern customs barriers. ... Sooner or later the risks also catch up with those who produce or profit from them. Risks display a social *boomerang effect* in their diffusion: even the rich and powerful are not safe from them' [144]. The hazards of technologically advanced civilization cannot be restricted anymore 'spatially, temporally, or socially' and they include nation-states, military alliances and all social classes' [145]. All people-rich and poor people and all countries-- rich and poor—were victims of the nuclear radiation from the Chernobyl nuclear disaster. Such radiation does not stop at national borders nor at the homes of the rich, although there are big inequalities in the distribution of expert resources to remedy the unintended consequences of such risks' [141].Globalization is one of the five challenges of the second modernity, the other four being ecological crises, the decline of paid employment, individualization, and gender revolution. It is also one of the constituents of what Beck calls 'risk regime'-- the political economy of insecurity, uncertainty and loss of boundaries –the others being ecologization, digitalization, individualization and politicization of work [153].

The concept of globalization is hard to define. It is a sneaky and plastic concept. Pinning it down is like, in Beck's words, 'trying to nail a blancmange to the wall'. It does not have one common denominator, though it is true that *people 'do not live and act any longer in the self-enclosed spaces of national states and their respective national societies'*, as they did in the first modernity. Given this, Beck gives a comprehensive definition: 'Globalization means that borders become markedly less relevant to everyday behaviour in the various dimensions of economics, information, ecology, technology, cross-cultural conflict and civil society. It points to something not understood and hard to understand yet at the same time familiar, which is changing everyday life with considerable force and compelling everyone to adapt and respond in various ways. Money, technologies, commodities, information and toxins 'cross' frontiers as if they did not exist. Even things, people and ideas that governments would like to keep out (for example, drugs, illegal immigrants or criticisms of human rights abuses) find their way into new territories. So does globalization conjures away distance. It means that people are thrown into transnational lifestyles that they often neither want nor understand – or, following Anthony Giddens's definition, it means *acting and living(together) over distances, across the apparently separate worlds of national states, religions, regions and continents*' [176]. He also cites quite a number of reasons why new globality has become irreversible, as many as eight reasons: (1) tremendous expansion of international trade, global networking of finance markets along with growing power of transnational corporations; (2) the ongoing revolution of information and communications technology; (3) the universal demands for human rights and democracy;(4) the stream of images from the global cultural industries; (5)the emergence of a postnational, polycentric world politics, in which transnational actors (viz., corporations, non-governmental organizations, United Nations) are growing in power and number alongside governments; (6) the question of world poverty; (7) the issue of global environmental destruction; and (8) transcultural conflicts in one and the same place [176]. What is paradoxical is that globalization, regardless of how it originated, is not a choice. It is nobody's rule. No one is in charge, no one started it, no one can stop it.It is a kind of organized irresponsibility. You keep looking for someone who is responsible, to whom you can complain. But there is nobody at the other end of the line, no e-mail address. The more the globalization discourse dominates all areas of life, the more powerful capital strategies become' [159]. In any case in the globalized world people engage in transboundary acts which further the globalizing processes. This occurs when 'people shop internationally, work internationally, love internationally, marry internationally, research internationally, grow up and are educated internationally (that is, multi-lingually), live and think transnationally, that is, combine multiple loyalties and identities in their lives' [164].More than this, 'the maelstrom of globalized modernization, has contributed to the production numerous global problems of everyday reality. 'Climate change, environmental destruction, food risks, global financial risks, migration, the anticipated consequences of innovations in genetics, human genetics, nanotechnology, and so forth, all serve to call into question in a quite tangible way the very foundations of social life'[148].

A few aspects or impacts of globalization, among others, can be noted here. The first concerns the role of information and communication technologies (ICTs) in bringing about societal changes including the shaping of both economy and society especially in view of the capability of the transnational corporation 'to withdraw the material resources (capital, taxes, jobs) from the society' and also to the domain of capital and labor relations [176] [177]. In global capitalism, capital is global whereas work becomes localized. The result is increased competition between businesses for capital investment, on the one hand, and intensification of capital-labour relations in the sense that capital becomes globally coordinated while labour is individualized. 'In the 'distanceless' space of computer technology, every location in the world now potentially competes with all others for scarce capital investment and cheap supplies of labour. The power relations between labour and capital become sharper as they are thus relocated within the structure of space and time'[153]. Second, the work society becomes risk society in which the role digitalization in particularly impactful. In the risk regime–'that is, the political economy of insecurity, uncertainty and loss of boundaries'–digitalization compels, and indeed facilitates the processes of globalization in several dimensions. **'**Global digitalization and networking are aimed at an economy that will have the capacity to operate as a unit in real time right across the planet. Digitalization should really be seen as the spread of a new kind of literacy: those who do not master computer language will be excluded from the circle of social communication. The 'grammar' of digital technology is not, however, the only element shaping people's view of the world; others are the scale and objectives of the flexibilization, virtualization and rationalization of work. A new type of 'high-tech' nomadic worker is appearing on the scene – or perhaps it would be more correct to speak of networked nomadic workers, capable, as it were, of being both here and there at the same time, of overcoming the gravity of space. They are no longer subject to an Either-Or, but to Both-And. They are simultaneously at work and at home, isolated yet working with and for others – in the distanceless space beyond frontiers and continents, but also concretely networked in the here and now' [153]. Third, the ICTs enable distribution and production of goods and services through division of labour in different parts of the world in such a manner that the distinctions between 'national and corporate labels inevitably become illusory'. Fourth, ICTs –the virtual forms of computer assisted communication—have potential 'political momentum' in as much as it 'can mobilize people' in the world risk society[176].

Fifth, following the collapse of uncontrollability, uncertainty and security in the second industrial modernity and the concomitant advent of globalization, 'a new kind of capitalism, a new kind of economy, a new kind of global order, a new kind of society and a new kind of personal life are coming into being, all of which differ from earlier phases of development'. This capitalism, which has produced 'second modernity', has brought about 'the increasing speed, intensity and significance of the processes of transnational interdependence' in the context of economic, cultural, political and societal globalization [162] [142]. Furthermore, 'capitalism is changing fundamentally because if doesn't have a nation-state base anymore, or at least has it less than before. There is a new force of de-territorialized capitalism now, which means a new power game between state, big businesses and the economy is being institutionalized. If international, transnational, global involvement in the distribution of risk is not matched by mechanisms for anticipation of and reflection on risk, even-mega corporations may be hurt very badly, especially if they are not secured by a nation-state which enforces special agreement and enacts conditions of limited liability into law' [162]. This capitalism, by creating more and more fields of production and profits can exploit less and less workers who are losing bargaining power and more so because of the decline of trade unions. More people are being excluded from the labour market as well as from opportunities for material and social securities and hence social integration. 'Consequently, not only are inequalities on the rise, but the *character* of social inequalities is dramatically changing as ever larger circles of people are excluded as in

principle 'economically in active'' [176]. Sixth, this new kind of capitalism has brought along with it new global market risks (viz, man-made financial risk) which are a new form of 'organized irresponsibility' for the institutional system is so informal that no one has accountability'. Enabled by the information revolution, the global market risk allows the near-instant flow of funds to determine who, if any one, will prosper and, and who will suffer. Like the competitive terms of economic theory, no one component is large enough to shift the overall; no body controls the global market risk. The components follow their own self-interest, and the results resemble those predicted by theory. Because there is no global government, the global market risk cannot be regulated like the national markets' [142]. Thus, the new kind of capitalism that has emerged and is spreading is a 'globally *disorganized* capitalism' with 'no hegemonic power and no international regime' to manage and regulate it [176]. In the global capitalist economy –'the risk society's laboratory'—the increase in global risks contributes to the global fragility of markets. 'The more fragile and unpredictable world markets become, the greater the threat to investment capital, the more frequently shareholders jump ship, and the more urgent the issue of power – that is, the question of 'relations of definition' – becomes for all those involved' [148]. Moreover, systemic loss of trust increases consumers' perception that risk is everywhere. If the trust is less, it then results in the creation of more risks. Consequently, 'the greater the awareness of risk, the more unstable global markets becomes. The more unstable global markets become, the greater the boomerang risks are for everyone – including corporations and governments' [148].

Finally, globalization poses a serious threat or challenge to transformation of first industrial modernity, i.e. to the 'simple, linear, industrial modernization based on the national state', leading eventually to the collapse of 'the nation-state' [142]. As Jarvis explains: 'the advent of globalization challenges the territoriality and sovereignty of the state, reduces the authority of the state and its citizens to act unilaterally or independently, and compromises economic autonomy by forcing states to act in ways and adopt policies broadly commensurate with the whims of highly mobile capital. Further, it de-nationalizes markets, creates international patterns of competition for foreign investment and forces the state to respond to an international rather than purely domestic constituency' [178]. To put it otherwise, the dialectic of modernity in the developing world risk society delivers 'the hardest blow to insular national thought, to political and methodological nationalism' that is implicit in the contents of the nation state whose erstwhile autonomy ceases to exist any longer [179]. The nation- state or nation- state societies are becoming 'zombie category' or 'zombie' societies. They are dead even though they are still alive but cannot handle the 'cosmopolitanization' – processes of transformation involving 'deep engagement in local activities, local consciousness, connections to local people' that are taking place within the nation state or nation-state societies [162]. That the nation state cannot handle transboundary scientific and technological problems has been cited, for instance, by Beck when he says that the BSE (*Bovine* spongiform encephalopathy) or 'Mad Cow Disease' is 'an explosive reminder of the inability of both nation-states and transnational decision-making bodies like the EU to manage risk in a chaotically interacting world risk society. But this is only the beginning. In developing the technologies of the future--genetic technology, nanotechnology and robotics--we are opening up a Pandora's Box. Genetic modification, communications technology and artificial intelligence, now also being combined with one another, undermine the state's monopoly of the use of force and leave the door wide open to an individualization of war--unless effective measures are taken soon at global level to bolt it shut' [180]. Understanding this requires an evaluative analysis of Beck's position concerning the role of science and technology in the risk society.

IV. VII. RISK SOCIETY AND THE ROLE OF SCIENCE AND TECHNOLOGY

The importance of science and technology in the production and reproduction of risk society lies in the fact that they play an integral role in the generating different types of risks and their associated social; problems in the late modern industrial society [149]. The transition from industrial to risk society germinates '*un*intentionally, *un*seen, compulsively', in the course of the dynamics of inexorably 'automatic operation of autonomous modernization processes which are blind and deaf to consequences and dangers' undermining and/or cancelling the established safety systems of the erstwhile industrial society [142]. Before more can be said of the role of science and technology in this mutation of the industrial society into risk society, let me define both terms. '*Technology differs from science in that science is about discovering and explaining and technology is about designing and making*. So technology encompasses design and method, though modern technology borrows heavily for its knowledge base from modern science. Science, for example, may investigate the properties of steel and plastics and build a body of knowledge about these materials whereas technology uses that knowledge, plus practical knowledge acquired in practice, to mould steel and plastic to practical ends like providing strong joists for buildings or tools for the kitchen' [181]. However, the distinction between science and technology should not be absolutized (viz. biotechnology etc.) for they are opposite ends of a continuum [182].Beck's analysis and elaboration of the nature character of modern science and technology is primarily a critique of what has been called 'the standard view of science'. This view considers that scientific knowledge has a privileged status and is independent of both the society and those who pursue scientific activity because scientific knowledge is based on empirical evidence [183].

To begin with, while comparing modern with postmodern theories of society, Beck points out the function, nature and position of science respectively in simple or first modern society on the hand, and reflexive or second modern society , on the other. The characteristics for the former are**:** 1. the ending of the debate through the discourse of scientific consensus; 2.the minimization of side effects and ineradicable residual uncertainty; and 3. the monopoly of legitimate knowledge. In contrast the following were the function, nature and position of science in the late industrial society: 1 the growth of contradictory scientific camps; 2. the recognition of extra-scientific justifications; 3. the increased account taken of unexpected side- effects; and 4.the ending of the debate through ad hoc institutional means of reaching a decision [155]. Initially "an unbroken faith in reason and progress" characterized science in the nascent industrial society and this prevailed until the 1950s.It was applied to "a 'given' world of nature, people and society" [144]. If science was then a source of risks, it was also then a source of solution. That is not the case in the risk society, as changes in the transformation of the character of science are illustrated by Sorensen and Christiansen in Table 19 [133]. Beck argues that, in the final instance, 'scientific civilization has entered a. stage in which it no longer merely nature,

Nos.	Industrial society	Risk society
1	The dangers/risks can be detected bythe individual using his or her senses (unemployment, industrial injuries etc.)	The new dangers and risks can be detected only by means of the senses of science: theories, experiments, measuring instruments etc. (e.g. CFC gases, global warming)
2	Experience of risk and danger is immediate, direct	Risk awareness is second-hand non-experience
3	Science demystifies the world (Weber)	Science is demystified
4	Belief in science	Belief in science crumbles, while we simultaneously grow increasingly dependent on it
5	Science as problem solver	Non-knowledge as an existential precondition

Table 19: Contrasting Roles of Science in Industrial and Risk Societies

people and society, but increasingly itself, its own products, effects and, mistakes. Science is no longer concerned with 'liberation' from *pre-existing* dependencies but with the definition and distribution of errors and risks which are *produced by itself'* [144]. In the reflexive phase of complete scientization of the second industrial modernity, scientific scepticism extends to the 'inherent foundations and external consequences of science itself' and this demystifies 'both its *claim to truth* and *its claim to enlightenment'* .However, it is an irony that as its success grows, so it seems that 'the risks of scientific development increase disproportionately faster; when put into practice, solutions and promises of liberation have emphatically revealed their negative sides as well, and these have in turn become the objects of scientific analysis' [144]. As it progresses, science expands and conducts its own critique and the practices of experts. Differentiation of science leads to overspecialization, hyper- complexity and uncertainty of scientific knowledge as well as interdisciplinary antagonisms. These developments are accompanied by the emergence of public risk consciousness and public protest movements subjecting science to public criticism. As the number of risks and shortcomings of first modernization increase and unfold, reflexive scientization – science evaluating science – erodes Enlightenment faith in the progress of scientific and technological rationality [144]. As its aftermath, the monopoly of science over its knowledge claims is broken. The more the science becomes necessary the more it becomes '*less and less sufficient* for the socially binding definition of truth'. This transformation of science is 'a *product of the reflexivity* of techno-scientific development under the conditions of risk society'[144].From the mid-1950s science has changed 'from an activity *in the service* of truth to an activity *without* truth', has become 'indispensable to *and in*capable of truth' and is becoming human in terms of mistakes and errors that one proverbially makes. The situation is such that '*if three scientists get together, fifteen opinions clash*'. In the late industrial society, risks are 'scientized' and hazards are 'technologized' [144] [145]. Moreover, the very purpose of science is being frustrated. 'The recourse to scientific results for the socially binding definition of truth is becoming *more and more necessary*, but at the same time *less and less sufficient*. This disparity between necessary and sufficient conditions and the resulting gray area reflect science's loss of functionality in its most central occupation, the representative determination of knowledge'. Under the circumstances it is no surprise that until the 1960s science could count on unsuspecting public for their faith in science. Since then, its activities 'are followed with mistrust. People suspect the unsaid, add in the side effects and expect the worst' [144]. Elsewhere Beck pointedly remarks that 'the natural science has thereby forfeited its exclusive right to judge what an experiment signifies. Research has, as it were, been implicitly socialized. Public opinion and governments, being components of the experiment, demand to have their say. Real-life experiments, such as the evaluation of nuclear, chemical and genetic hazards, have become fundamentally ambiguous and open to interpretation: the experience of the public breaks away from controlled scientific experience, and the two engage in a competitive struggle over interpretation of the results' [145]. As a matter of fact, nowadays science does not take took place any more 'in the laboratory as a spatially and temporally limited empirical science'. The world itself has become' a laboratory. The mobility of genetically modified plants shows how difficult it is to restrict and monitor the experimental location and the possible consequences and dangers' [132]. The notable aspect of recent scientific development is that the importance of the domain of risk diminishes as the standards of scientificity are raised constantly to a higher level. This virtually gives 'a scientific carte blanche for the potentiation of risks. To stretch the point: the insistence on the purity of scientific analysis leads to a pollution and contamination of the air, food water, and land, plants, animals, and human beings' [163].

The same crisis in the functionality and legitimacy that afflicted science, as said above, is also now overwhelming technology and technological practices. The world has become 'technologically constructed world' and is now also, says Beck, 'a test site for risky technologies' [145]. 'At a certain stage of social production, characterized by the development of the chemical industry, but also by reactor technology, microelectronics, and genetic technology, the predominance of the logic and conflicts of wealth production, and thus the social invisibility of the risk society, is no proof of its unreality; on the contrary, it is a motor for the origin of the risk society and thus a proof that it is becoming real' [144]. The practical developments within the techno-scientific domain leave much to be desired in coping with risks of industrial modernity. 'Today's recognized knowledge of the risks and threats of techno-scientific civilization has only been able to become established *against the massive denials*, against the often bitter resistance of a self-satisfied 'techno-scientific rationality' that was trapped m a narrow-minded belief in progress. The scientific investigation of risks everywhere is limping along behind the social critique of the industrial system from the perspectives of the environment, progress and culture. In this sense, there is always a good bit of the unavowed cultural *critical zeal of a convert* in the techno-scientific concern with risks, and *the engineering sciences' claim to a monopoly on rationality in risk perception is equivalent to the claim to infallibility of a Pope who has converted to Lutheranism*' [144]. Furthermore, 'techno-scientific development is beginning to be trapped more and more within a striking new contradiction: while the foundations of knowledge are being explored in the institutionalized self-skepticism of the sciences, the development of technology has been isolated against skepticism. Just as the risks and the pressure for action grow, absolutist claims to knowledge, infallibility and security, which have long since become untenable, are being renewed in technological development. *Dogma flourishes under the pressure on the engineering sciences to take action*. The unleashed and systematically fomented skepticism encounters the *anti-modernity* of scientific infallibility taboos in the development of technology. These harden as the risks increase' [144].

From this perspective, one can only apprehend that there is no reason to think that the powerful new technologies -- such as 'genetic technology, communication technology, and artificial intelligence' – of the twenty-first century will not produce equally powerful risks [151]. Beck goes on to state that, not without reason, that 'it is perfectly conceivable that a genetically engineered plague, one designed to have a long incubation period and to target specific populations, could be someday produced without its maker encountering much resistance. That would be as awesome a force as an atomic weapon. And it's only one example' [151]. Similarly, the information technology which drains the state power *vis `a vis* the economy, on the one hand, can well strengthen the state *vis `a vis* its own citizens, on the other, by being utilized as a very powerful surveillance tool of thoroughgoing control over the citizens [151]. The monopoly of the scientists and engineers in the matter of diagnosis and safety in regard to the large-scale industrial hazards is now increasingly being questioned. They can only predict probable safety, which is different from safety as such. Hence the contradiction between experimental logic and atomic hazard can hardly be resolved with the consequence that risks will continue to threaten life and society. 'The position of power which the relations of definition (i.e., 'the rules, institutions and capabilities which specify how risks are to be identified in particular contexts') accord the engineering sciences is based on a straightforward administrative decision. They are granted the authority – binding for law and politics – to decide using their own standards what the 'state of technology' requires. If one asks, for instance, what level of exposure to artificially produced radioactivity the population must tolerate – i.e. where the threshold of tolerance separating normality from dangerousness is situated – then the German Atomic Energy Act provides the general answer that the necessary precautions must correspond to 'the state of technology' (§7 II, No. 3). Anyone who wants to know precisely how large a daily ration of standardized pollution citizens are supposed to tolerate need only consult the 'Ordinance on Large Combustion Facilities' or the 'Technical Instructions: Air Quality' and the like to discover the (literally) 'irritating' details'[132].As Beck quips: 'Just as sociologists cannot force society into a test tube, engineers cannot let people's reactors blow up all around them in order to test their safety, unless they turn the world into a laboratory. Theories of nuclear reactor safety are testable only after they are built, not beforehand. The expedient of testing partial systems amplifies the contingencies of their interaction, and thus contains sources of error which cannot themselves be controlled experimentally' [142]. In addition, Beck rightly points out that the logic of research, a component of standard view of science and technology has undergone reversal in late modernity. In today's techno-scientific practices 'we no longer find progression, first laboratory then application. Instead, testing comes after application and production precedes research. The dilemma into which the mega-hazards have plunged scientific logic applies across the board; that is, for nuclear, chemical and genetic experiments science hovers blindly above the boundary of threats. Test tube babies must first be produced, genetically engineered artificial creatures released and reactors are built, in order that their properties and safety can be studied. The question of safety then must be answered affirmatively before it can even be raised. *The authority of the engineers is undermined by this 'safety circle'*" [142].

The risk society is basically characterized by a range of new risks which are in essence manufactured uncertainties, i.e., unintended side effects of technological and economic development under the framework of capitalist modernization, And these, in brief, 'manufactured uncertainties result from scientific and technological progress, which supposedly should solve, not create problems' [132]. It is no surprise that Beck incisively thus critiques the role of science and technology by saying that 'Technology and natural science have become one economic enterprise on a large industrial scale, without truth or enlightenment, comparable to the secular power of the medieval Church without God. Just as the Church of the Inquisition failed to prove the existence of God, so the reigning science still owes us proof of its truth. Moreover, it has involuntarily and indirectly furnished the proof of its contrary, across the length and breadth of its victory parade' [145] .

At this point it needs to be reminded that the role of science and technology in generating risk society cannot be absolutized or treated in isolation, for 'the calculus of risk connects the physical, the engineering and the social sciences' embodying intricate inter-linkages among them. The reason is that it can be applied to 'completely disparate phenomena', not only health risks but also to a host of other risks such as economic risks, risks of unemployment, risks of old age and so on [142]. The reigning scientization or technological 'fatalism' can only be overcome, so argues Beck, by 'more democracy – the production of accountability, redistribution of the burdens of proof, division of powers between the producers and evaluators of hazards, public disputes on technological alternatives. This in turn requires different organizational forms for science and business, science and public sphere, science and politics, technology and law, and so forth' [142]. Whether it is dangers, hazards or risks, they are unintended consequences of ongoing modernization in the late industrial society. Beck was no 'pessimist' [184]. Those unintended consequences are not something 'external' to the society and, accordingly, critique and resistance to the contemporary science and technology and their practitioners can only' improve everyone's chances of survival' [145].

IV. VIII. UNCERTAINTY AND NON-KNOWLEDGE

Caused by Tōhoku earthquake and tsunami, the Fukushima Daiichi nuclear accident occurred on 11 March 2011 at the Fukushima Daiichi Nuclear Power Plant in Ōkuma, Fukushima Prefecture, Japan. This nuclear disaster was preceded by the*Chernobyl nuclear disaster* on *26* April 1986 near the city of Pripyat in Ukraine in the Soviet Union. Interestingly, Beck was proofreading the first edition of his *Risk Society* in April 1986 when the Chernobyl disaster occurred. Ironically, Beck was also writing in 2011 a last minute preface to his Japanese publication of the lectures that he delivered in Japan 2010. When the Japanese government announced in December 2011 that 'complete decommissioning of the Fukushima Daiichi reactors would take forty years, it became clear that even in the most optimistic scenario the world would be living with this disaster for a long time to come' [185]. The classic example of manufactured risk in contemporary times was the intentional terrorist attack of 9/11 by Wahhabi terrorist group Al-Qaeda against the United States. It was anthropogenic and catastrophic in character with global reach implications [186]. Terrorist activities intentionally 'exploit the manifest vulnerability of modern civil society and replace the principle of chance and accident' in which case the prior 'the calculation of the probability of cases of loss' cannot be applied [179].All these calamities boil down to the irrefutable truth that we are now, to borrow the phrase from Beck, 'living in the world risk society' in the sense that 'it is increasingly occupied with debating, preventing and managing risks that it itself has produced'. Risks remain virtual and they cease to be risks as such when they become catastrophes. So risks are anticipation of catastrophes.

And then they move to other greener pastures: 'to the anticipation of further attacks, inflation, new markets, wars or the reduction of civil liberties. Risks are always events that are threatening'. At the same time, risk, argues Beck, 'is *not reducible to the product of probability of occurrence multiplied with the intensity and scope of potential har*m' [168]. The contradiction consists in the fact that action is needed to avert risks-- nuclear, ecological, financial, military, terrorist, biochemical and informational-- that contain in threatening future events, but such action can hardly be effective for the simple reason that the future is in many ways not knowable –unknowable –and hence uncertainty turns out to be 'a basic condition of human knowledge and existence. Uncertainty is 'a state of indeterminacy between cause and effect' [158]. This creates a paradox: '*How to provide certainty and security through knowledge of the future in the face of uncertainty as a basic condition of human knowledge*' [187]. Loon is not wide of the mark when he says that 'the more we know about the world, the more we know about risk, but the more we know about risk, the less we know about the world' [188].

Thus Beck expounds his arguments about the non-knowledge dominating the content and contours of the late modern risk society. 'Living in world risk society means living with ineradicable non-knowing [*Nichtwissen*] or, to be more precise, with the simultaneity of threats and non-knowing and the resulting political, social and moral paradoxes sand dilemmas. Because of the global character of the threat, the need and burden of having to make life-and-death decisions increase with non knowing. Talk of the 'knowledge society' is a euphemism of the first modernity. *World risk society is a non-knowledge society in a very precise sense. In contrast to the premodern era, it cannot be overcome by more and better knowledge, more and better science; rather precisely the opposite holds: it is the product* of more and better science. *Non-knowledge rules in the world risk society*. Hence, living in the milieu of manufactured non-knowing means seeking unknown answers to questions that nobody can clearly formulate'[132]. Non-knowing is pervasive affecting all spheres of human conditions and institutions including expert and control

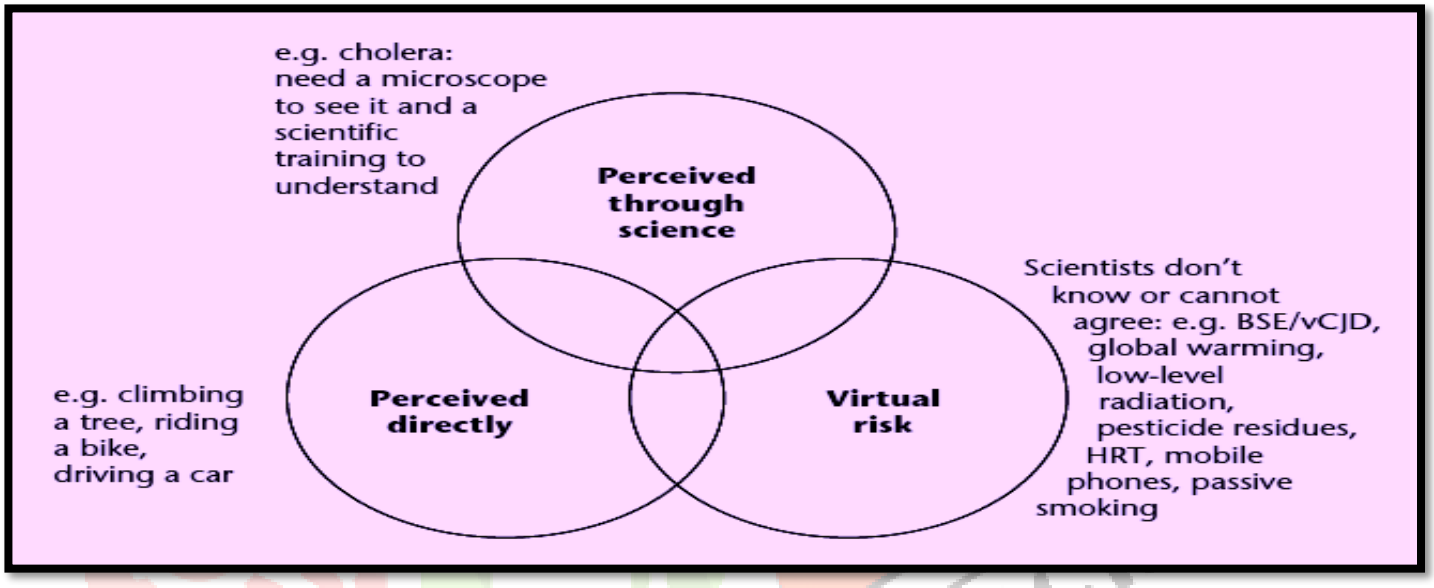


Figure 21: Types of Risks

systems. 'The medium of reflexive modernization is not knowledge, by–more or less reflexive—non-knowledge'. Non-knowing, along with the overlap and magnifications of different forms of knowledge and non-knowing, opens up a whole new area of questions, interpretations, meanings and misunderstandings. Non-knowing can thus be 'conscious or unconscious, concrete or theoretical, it can signify willful ignorance or an inability-to-know and so on'132]. Figure 21, provided by Adams, points to some concrete examples of virtual risks in this domain [189]. Beck provides a typology of forms of knowledge in his work, *World at Risk* (2009). First, 'the epistemic agenda through conflicts concerning *selective assumptions* that scale the ladder of credibility from non-knowing to knowledge'; second, wilful ignorance; third, reflected *non-knowing*; fourth, the *conscious inability*-to-know; fifth,' repressed or *unconscious non-knowing* which points to the 'limited horizon of a form of knowledge that does not reflect on its own limits. One does not know what one does not know. This is encountered among experts and counter-experts and in new (and old) religious and social movements'; finally, sixth, 'the *unknown inability-to-know*, i.e. those 'unknown unknowns' in which there lurks the ineradicable element of surprise' [132] [187]. In his *World Risk Society* (1999), Beck talks in terms of 'unawareness', i.e. ignorance or gaps in knowledge. 'Unawareness can be known or not known, concrete or theoretical, unwillingness to know or inability to know, and so on' [142] [134].

Risk society or, for that matter, the new risks, is characterized by '*manufactured uncertainties'*–viz. environmental problems—which are unintended side effects of and result from scientific and technological progress, which are supposedly should 'solve, not create problems'. The new risks or manufactured or 'fabricated uncertainties' are intangible to human senses and can be known only by scientific tests. They have often latency which means they are 'not fully scientifically determinable' [179].In the second or reflexive modernity risks that arise are characterized by 'radical uncertainty. Unclarity is inherently part of their nature, concerning both the population they affect and the time span in which they operate. In many cases, the time span alone is so long that prediction is impossible. In the face of risks, which by their nature can't be determined precisely, the whole institutional workings of the first modernity seem to get thrown into reverse' [151]. Beck gives the example of the industrial production of chlorofluorocarbons (CFCs) in 1930 as a new risk to illustrate that '*the greater the threat, the greater the gap in knowledge, the more urgent and more impossible is the decision (decision paradox)*'. It took more than 40 years to recognize the negative side effects of CFCs. In the 1970 and 1980s it became clear that that their uses as coolants in refrigerators and as a propellant in spray bottles were harming the ozone layer are posing 'a threat to life instead of its source'. The deleterious effects of the CFCs were

not known for more than forty years. Thus science 'did not even know what it did not know' – a paradigmatic example of the uncertainty of the type of 'unknown unknkowns'. It exemplifies 'a case of *un*intended inability-to-know, at any rate at the moment of decision' [142]. Sorensen explains: 'examples like this cast light on how the boundary between knowledge and non-knowledge has become blurred and how at any given time at which we have to make decisions on the application of a new technology, there will be knowledge of which we are unaware – and might not ever become aware. Beck and Wehling... see indication of this recognition spreading. They distinguish between a classic, modern understanding of non-knowledge as *not-yet-knowing* – like a territory that has yet to be explored and mapped (Bauman) – and a new, more complex understanding of non-knowledge that is able to encompass both not-yet-knowing (i.e. the knowledge that we are aware we lack) and the so-called 'unknown unknowns' (the knowledge we *don't* know that we lack)...Thus, 'unknown unknowns' were in play when we began using CFCs in the1930s. But the importance of these 'unknown unknowns' first became apparent 40 years later, when the link between CFCs and the holes in the ozone layer was discovered'[190].There are other examples of how science and technology generate uncertainty transforming the industrial society into a risk society. Take for instance the case of conflict over the risks associated with genetically modified foods that offer 'a prime example of why, in conditions of incalculable uncertainty'. 'In this case 'neither the technology's proponents nor its critics know for sure what its consequences will be. The victory of genetic technology forces everybody into making impossible decisions that may influence our very survival, while being *completely unable* to ground these decisions in knowledge. In fact, what we are dealing with here is not (calculable) risk but (incalculable) uncertainty. We are dealing with a dynamic in which more scientific knowledge, rather than leading to greater certainty, leads instead to an increase in cognitive uncertainty and normative insecurity'[148] **.**

Manufactured uncertainties, in which 'knowledge and non-knowledge of risks are undissolvable', arise out of the 'relations of definition' – rules, institutions and capabilities that specify how risks are indentified and assessed – which are outcomes of debates and controversies among those including scientists and experts. The ***relations of definition*** involves 'legal, epistemological and cultural power matrix in which risk politics is conducted' [179] [145]' The debates and controversies, in the context of issues such risk determination, accountability and so one, are quite crucial. Let me quote Beck in *extenso* to clarify the importance of issues concerned: '1.Who determines the hazardousness of products, dangers and risks? Where does the responsibility lie? With those who produce the risks, with those who benefit from them or those who are potentially or actually affected by the dangers in their lives and their social relations? What role do the different publics and their actors play in this context? And how can these questions be answered within national spaces, between national spaces and globally? 2. What kind of knowledge or non-knowledge of the causes, dimensions, actors, and so on, is involved? Who lays down the causal norms (or nomological correlations) which decide when a cause-effect relation is to be recognized? And who has the right to demand and get what information, and from whom? 3. What counts as 'proof' in a world where knowledge and non-knowledge of risks are inextricably fused and all knowledge is contested and probabilistic? 4. Who is to decide on compensation for the afflicted — within one or several nation-states? How is the call for 'precaution' put into effect? To what extent should those most seriously affected by the 'latent side effects' be involved in working out corresponding regulations?' [179]. The recently manufactured risk or manufactured uncertainties are not 'determinable with actuarial precision in terms of a probability calculus backed up by insurance and monetary compensation', and they are they are 'incalculable, uncontrollable and in the final analysis no longer (privately) insurable (climate change)' [159]. An instance illustrating the 'definition of relations' can be cited with reference to bovine spongiform encephalopathy (BSE) or mad cow disease, which is illustrative of 'a textbook example of risk society'. [142]. On the one hand , it concerns a radical separation, in the second modernity, between the producers of risk and those affected y the risk and bear the consequences. In this case the gap is apparently covered by causal analysis which is very complex. Under the circumstances, the affected person must prove exactly who it is that has harmed him/her before (s)/he can collect compensation and usually this is an impossible task for the affected persons. On the other hand, this was the case with BSE in which also problem was to locate and establish the chain of the causality which is very complex. The chain of causality–whether there was a link between BSE/mad cow disease and human version of mad cow disease (i..e., the variant Creutzfeldt-Jakob Disease)-for which there were competing definitions and rival theories about the consequences on the affected persons could not be corroborated. The result is that those who were looking for the chain of causality found themselves dealing with what is called by Beck as '*known* or *regressive* uncertainty, where the more facts we know, the more the uncertainty grows'[151].There was indeed no simple or straightforward answers to the concerned issues of mechanisms of causations, or the methods of control and so on [191]. While Beck, emphasizing the differences of opinion among the scientific experts, goes on to say that in the cases of BSE, SARS or avian flu 'the schema – the link between non knowledge and threat – is everywhere similar. Here the lack of knowledge extends, among other things, to the source of the illness, to the paths of transmission and to the latency period following an infection' [132]. Put simply, in BSE the indeterminacy was due to the lack of sufficient evidence to establish causal relationships between the mad cow disease and human illness. 'Mad cow disease was a certainty, but its complex connection to Creutzfeldt-Jakob disease was uncertain, creating an ambiguous context for decision making' [158].Another issue, the threats implicit in climate change are an outcome of technological-industrial development and cannot be calculated or controlled by existing institutional mechanisms. 'It requires crass ignorance or decidedly selective vision to overlook the link between an ominously rising temperature curve and increasing greenhouse gas emissions, notwithstanding the uncertainty of the correlation. That the uncertainty established national institutions have no answer to this is also in the mean time a truism' [132].

A recent example of pandemic, referred to in the previous section, is the new coronavirus (SARS-CoV-2) that causes acute respiratory syndrome (COVID-19). Between January and April 2020 it became a global pandemic killing over 126,000 people as of April 14th, 2020 [192]. It was previously 'unkown' to science and can be called an ingredient of how modern industrial society is turned into a risk society, as Beck analyzed. The global pandemic has offered disaster capitalists to open up 'new markets and develop new commodities in the domains of preparedness, protection, policing and care' [193] [194]. But, at the same time, 'despite the pace of research, significant scientific uncertainties remain though 'the full genetic sequence of the virus' became globally available within the ten days since the first alert by WHO [195]. The Covid-19 pandemic attests to ecological and financial crises and is transforming extant values and belief systems. Much in Beckian terms, Kims clarifies that 'these ecological, economic, and ideological turns toward a new form of humanity and global society are closely interconnected and

mutually reinforce one another' [196]. There is little doubt Covid-19 is a 'monstrous global risk' in terms of Beck's risk society thesis [197]. Freudendal-Pedersen and Kesselring argue that, following Beck, 'the dynamics of post-industrial societies are increasingly challenged by man-made, self-produced risks such as nuclear power, genetic engineering, climate change, congestion, and – from today's perspective – the COVID-19 virus. In one way or another, they represent modern uncertainties, insecurities and unintended consequences of procedures, technologies, and political-economic decisions that have been successful to date' [198]. World Health Organization (WHO) declares that uncertainty is 'inevitable' during a pandemic like Covid-19 which 'has not been seen in a century, and much remains unknown and evolving about the situation and the virus that causes it' [199].

Last but by no means least, uncertainty is not only a feature of the social institutions of the risks society; it also affects the individual – the basic unit of the social structure of late the modern society- within the ongoing process of individualization. 'The individual must cope with the uncertainty of the global world by him- or herself. Here individualization is a default outcome of a failure of expert systems to manage risks. ... The individual is forced to mistrust the promises of rationality of these key institutions. As a consequence, people are thrown back onto themselves, they are alienated from expert systems but have nothing else instead' [168]. The individual is the 'ultimate addressee' of ontological insecurity. 'Whatever propels risk and makes it incalculable, whatever provokes the institutional crisis at the level of the governing regime and the markets shifts the ultimate decision-making responsibility onto the individuals who are ultimately left to their own devices with their partial and biased knowledge, with undecidability and multiple layers of uncertainty'[200] . Relevant here is the growth of 'self-culture' or 'own life culture' as an accompaniment of individualization process. Self culture involves two related conceptions. On the one hand, it implies the recognition of the self along with its indeterminacy and associated conflicts, crisis and developmental opportunities .On the other hand, it is binding or bonding, whether friendly or hostile, relationship of the 'self-oriented individual' to others. To state otherwise, it means 'the the compulsion and the pleasure of leading an insecure life of one's own and co-ordinating it with the distinctive lives of other people'. When this self-culture appears, the proletarian culture fades and disappears. What emerges is not the middle class culture but 'precisely a self-culture that is unpredictable both for oneself and for others, a cross between civil society, consumer society, therapy society and risk society'. In contrast to proletarian and bourgeois culture, where class categories count, the self-culture is characterized by 'a social and political dynamic of one's own life that puts its imprint on the individualized society. 'The lines of conflict are more diffuse but no less profound. New imaginaries of morality and responsibility take shape and develop; poverty, marriage, youth and political commitment assume new countenances. [169].The individualized society has its own system of values that cannot be equated with egoism or narcissism. Though based on commitment to the principle of 'duty to oneself', the individualized value orientations emphasize 'self-enlightenment and self-liberation as an active process to be accomplished in their own lives, including the search for new social ties in family, workplace and politics'. However, individualization, its self-culture of living 'a life of one's own', and the individualized society are not all without alarm and despondency. Do-it-yourself biography can transmute into breakdown biography too. Thus individual's 'self-culture means detraditionalization, release from pre-given certainties and supports. Your life becomes in principle a *risky venture*. A normal life story becomes a (seemingly) elective life, a *risk* biography, in the sense that everything (or nearly everything) is a matter for decision. And yet, faced with the opaque and contradictory character of modern society, the self-focused individual is hardly in a position to take the unavoidable decisions in a rational and responsible manner, that is, with reference to the possible consequences' [169].

To summarize, if the risk society is the outcome of different types of uncertainty such as provisional non-knowing, unacknowledged non-knowing wilful ignorance or conscious and unconscious inability to know, the risk society and its institutions are caught in a conundrum [132]. That is, the ultimate deadlock of the risk society is in the gap between knowledge and decision, for no one knows the outcome at 'the level of positive knowledge' even though one will have to take the decision. 'The risk epoch imposes on each of us the burden of making crucial decisions which affect our very survival without any proper foundation in knowledge. ... So risk society is provoking an obscene gamble, a kind of ironic reversal of predestination. I am held accountable for decisions which I was forced to make without proper knowledge of the situation. The freedom of decision enjoyed by the subject of risk society is the 'freedom' of someone who is compelled to make decisions without being aware of their consequences' [145].

IV. IX. BECK AND RISK MANAGEMENT

Risk society thesis of Beck does not deal with risk analysis, risk management or risk assessment, neither systematically nor indirectly as such. His views on this issue are raised only when he discusses now and then or when he deals with issues of his concern or relevance to shore up his risk society thesis. But is he careful to emphasize the point that the concept of risk is 'not merely of interest for actuarial science or risk studies' only. It is concept that is relevant to other fields including social sciences as well [190]. Beck's theoretical and methodological argument is that the 'risk calculus' links the natural, technical and social sciences. It can be applied as much to highly diverse phenomena in public health – from the risk of smoking to the risk posed by nuclear power stations – as to economic risks, risks of unemployment, of traffic accidents, of ageing, and so forth' [132]. Bosco and Giulio support the Beckian contention that the natural sciences and engineering, could not guarantee 'zero risk' [209]. It is quite reasonable to state that risk research is indeed multidisciplinary involving diverse disciplines including engineering, statistics, mathematics, decision theory, psychology, philosophy, sociology, political science and media studies [28]. It has been emphasized that 'the risk field is an inherently interdisciplinary activity, and in this role of the social sciences is is regarded as one of central importance [203]. Beck points, however, to the essence of risk analysis as a paradox: 'how to provide certainty and security through knowledge of the future in the face of uncertainty as a basic condition of human knowledge?' People have always tried to mitigate 'irrevocable uncertainty' by various means ranging from religious imaginaries to 'the sophisticated tools of probability and risk calculation (and of law, of planning, of futurology, methods of scenario construction, and finally of esoteric)' [159].

Indeed Jasanoff, having reviewed the relevant literature including Beck's perspective on risk and also environmental assessment, puts forward a strong plea that risk cannot be essentially determined on the basis of 'physical, biological or social causes'. Instead, it is more fitting to view risk as 'the embodiment of deeply held cultural values and beliefs' in respect of issues like 'agency, causation, and uncertainty'. She thus concludes by arguing that 'the social sciences have deeply altered our understanding of what 'risk' means - from something real and physical if hard to measure, and accessible only to experts, to something constructed out of history and experience by experts and laypeople alike. Risk in this sense is culturally embedded and has texture and meaning that vary from one social grouping to another. Trying to assess risk is therefore necessarily a social and political exercise, even when the methods employed are the seemingly technical routines of quantitative risk assessment. Judgments about the nature and severity of environmental risk inevitably incorporate tacit understandings concerning causality, agency, and uncertainty, and these are by no means universally shared even in similarly situated western societies' [206]. Rosa and others have extensively discussed the controversy between the rationalistic-bureaucratic approach of the scientists and experts on the one hand and the lay persons' perception concerning risk and risk assessment as put forward by social scientists, social psychologists and cognitive psychologists from the 1970s onward, on the other hand. 'The dual nature of risk as a potential for technological progress and improved well-being, on the one hand, and as a real threat to society and its members, on the other hand, demands a dual strategy for risk governance. Public values and social concerns may act as the driving agents for identifying those topics for which more refined assessments are judged necessary or desirable. As much as new scientific assessment methods are needed to broaden the scope of research targets, as well as to improve the handling of uncertainty, the expertise of social sciences will remain necessary to inform policymakers as well as the various attentive audiences in a plural society about new social trends and emerging public concerns' [158]. Be that as it may, by the 1990s risk management became a widespread 'grand narrative' of organizational and managerial practices indicating an explosion of risk management for numerous public and private organizations in different jurisdictions in the late 1990s. Thus Power quotes Ewald's statement the dual character of risk: 'Nothing is a risk in itself: there is no risk in reality. But on the other hand anything can be a risk; it all depends on how one analyses the danger, considers the event' [207].This closely parallels also the concept of risk for Beck. Risk is not real but may become a reality such as in a catastrophe like a terrorist attack [168].

What is stake is in the modern risk society are inherent manufactured uncertainties that are created by the society itself and dependent on human decisions. In addition, theses uncertainties are externalizable, collectively imposed, unavoidable for individuals. Their perceptions have not parallels in the past or previously experienced risks and institutionalized routines. And, above all, these manufactured uncertainties are 'are incalculable, uncontrollable and in the final analysis no longer (privately) insurable (climate change)'. As has been pointed out earlier, these new hypothetical or virtual manufactured uncertainties (e.g. climate change, financial crises, terrorism) (1) defy geographical space or territory, (2)are in principle incalculable but based on scientifically induced not-knowing and normative dissent, and (3) erode the logic of compensation which is replaced by the principle precaution by prevention [159]. Given this, Beck's analysis pores over the biases in the technical assessments and points up them. Rosa and others explain: 'Risk assessors in science and government systematically under-estimate the real threats to society. This is because they rely on a methodology that truncates the full range of risk elements to meet the demands of risk assessment formulas. The result is to legitimize the ubiquitous exposure of society to incalculable risks.... Beck argued that the expert's strategy is to legitimize political and economic interests by "relativizing" the incalculable and unlimited risk exposures, the multiple association between probability and the extent of potential damage is, according to Beck, a strategy of immunization on the part of the technology enthusiasts against rationally valid arguments for reasonable precautions against risk and, above all, against empirical evidence' [158]. It seems that, for Beck, the ultimate resolution of these manufactured uncertainties lie in the autonomous process of reflexive modernization operating within the risk society itself which is undergoing silently an epochal transformation- metamorphosis, as outlined in Beck's last publication, *The Metamorphosis of the World* (2015). This is why Wong goes on to say that 'the answer to better risk management for Beck, therefore, rests in large-scale societal metamorphosis. Global catastrophe, he posits, would result in social catharsis and the emancipatory impulses that would drive metamorphosis from a world risk society into reflexive modernization led by cosmopolitan communities around the world, united by risk and decline' [208]. The reason is that the new risks are intangible to the human senses and they are often latent. Latency is one reason why, says Beck, 'these new risks are not fully scientifically determinable, even though they are to a degree knowable through science. *This means that the traditional technologies of risk assessment, management and insurance are no longer fully functional*. The new risks are, in other words, manufactured uncertainties and dangers: modernity is faced with its own destructive potential of social and technological development without having adopted adequate answers [179]. Elsewhere, he says that 'specific calculable uncertainties'—risks—are 'not determinable with actuarial precision in terms of a probability calculus backed up by insurance and monetary compensation, such as were typical of first modern industrial society' 'and 'at the centre of attention today, by contrast, are 'manufactured uncertainties' But managing risks may find solution in the process of transfiguration or metamorphosis of the risk society since the 'incalculable uncertainty can also be acknowledged and become a source of creativity, the reason for permitting the unexpected and experimenting with the new'. Stated otherwise, 'manufactured uncertainties, global risks, are highly ambivalent, paradoxically also a moment of hope, of unbelievable opportunities—a cosmopolitan moment'[159]. Beck, on a broader canvas, looks toward a positive cosmopolitan future in which the institutions might be forced out of 'ingrained habits of organized irresponsibility' and would be compelled 'to open up to and involve those affected by the risks which others produce'[131]. It is important to note that Beck has not altogether ruled out risk management. For instance, in the *future the risk assessments of techno-scientific developments* 'will have to take into account, literally, intention as well as chance, the terrorist threats and the conceivable malicious uses as well as dangerous side effects' in spite of the fact that '*every modelling of uncertainty remains under the spell of the tradition of risk analysis and risk management* which has its roots in classical security research and is driven by the concern to achieve a socially acceptable and efficient 'managing' of uncertainty'. In the context of 'risk war' he also refers to the concept of *global risk management* with military means by states with 'the goal of minimizing and controlling a 'global risk' (transnational terrorism, the proliferation of atomic, chemical and biological weapons of mass destruction, etc.)'[132].

Beck uses and utilizes the concepts of threat, danger, risk, hazard, catastrophe, among other things. More importantly, he is cognizant of the quantitative dimension of risk and distinguishes it from danger. Risk refers to 'a future that is made knowable by measurement, even if this 'knowledge' remains speculative. This quantitative knowledge then forms a basis for rational decisions and calculations that are no longer determined by faith or the affective perception of danger. While danger is something we find ourselves (passively) exposed to, risk is something we (actively) take on'[159]. But Beck, from social scientific perspective, adds more flesh to definitional concept of risk, while considering the concept holistically and realistic. 'When it comes to determining what should be regarded as a 'risk' and what should not – and who should be made liable for it – *cultural values and stereotypes play a much more decisive role in relation to non-quantifiable uncertainties than to predictable risks....Risks are not things*. They are social constructions in which expert knowledge as well as cultural values and symbols play a key role. In order to unravel the power conflicts that lie behind conflicts over risk, it is necessary to raise the issue of '**relations *of definition'***. The power relations embedded in the relations of definition concerning revelation of the content and nature of risk, which has not only an objective or realist content but also a subjective –socially constructed dimension. And both dimensions, in the last instance, enforce responsibilities in the risk production. As Beck puts it: 'A whole series of questions points to this substructure of risk-defining power: who has what to prove? In other words, who bears the burden of proof in any given situation? What qualifies as causal evidence and as 'proof' under conditions of cognitive uncertainty? Which norms of accountability apply? Who is responsible? Who must carry the costs? As we begin to examine these cognitive power bases of the relations of definition, we gain a deeper insight into the connection between risk and power; we also get some indication of how changes in the power relations of definition – such as a redistribution of the burden of proof, or product liability regulations – can influence the political dynamic of risk conflicts. *Transformation of the power relations of definition may not only improve the chances of opposition movements but may also make global companies take social responsibility for the unknown consequences they trigger*' [148]. Managing risk has thus very important bearing on the definition of relations concerning management of risk. In addition, rational control of the risk, which has it its own rationality, appears to defy the logic risk management: 'Risk, by its inner logic, means uncertainty and accentuates uncertainty, and not only negatively in the shape of catastrophes (collapse of the global economy, etc.), but also positively: the experience of the everyday 'real world' is beyond the horizon of this risk model science... The controlling rationality of risk *cannot* be applied to the uncertainty of the effects, the side effects and the side effects of the side effects. The uncertainty of risk *cannot* be tamed by means of uncertain risk. Rather, the converse holds: all attempts at rational control give rise to new 'irrational', incalculable, unpredictable consequences. This is shown by the history of 'side effects' – for example, of climate change and the globalization of financial risks…--and the associated research. Control of the control of control can become a source of threats and side effects of threats without end [132]. In Beckian terms, the repercussions of complex technologies can hardly be predicted or managed by risk experts who can only make them seem apparently, not realistically manageable, and they thereby provide not the solution but rather become part of the problem. 'Since they base their calculations and recommendations only on demonstrable chain of causal inferences that are, if Beck is correct, inherently unavailable in advance, they inevitably contribute to a process of 'risk denial''. The example of this are such failures are Chernobyl, BSE and Foot and Mouth Disease which are stated to have no or minimal risk or risks that 'can be managed or contained' [329]. The uncertainty, experienced in the past and present, continues to remain without any organized solutions for the problems that uncertainty breeds. As a consequence, says Beck, 'key institutions of modernity such as science, business and politics, which are supposed to guarantee rationality and security, find themselves confronted by situations in which their apparatus no longer has a purchase and the fundamental principles of modernity no longer automatically hold good. Indeed, the perception of their rating changes -- from trustee to suspect. *They are no longer seen only as instruments of risk management, but also as a source of risk*' [336]. I now pass on to a brief discussion of recent literature of risk and risk management in cloud computing, which will enable a profitable comparison between risks in the Beckian risk society thesis and risks in the cloud computing.

V.RISKS AND RISK MANAGEMENT IN CLOUD COMPUTING

V. I. CLOUD SECURITY, RISKS AND CYBER INCIDENTS

Against the backdrop of the foregoing brief elaboration and analysis of risk and, especially Beck's theorization of the development of world risk society in the late modern industrial society, it is only apparent that one has to look for remediation of risks as far as possible when unknown and unknown risks continue to emerge in the context of the persistence non-knowledge or unawareness. In the risk regime 'insecurities' and 'uncertainties, continue to be present in the second modernity [153]Thus, the search for security or safety accordingly continues to dominate in the domain of risk society and analysis. Although Beck would suggest a thoroughgoing transformation of the social institutions–-metamorphosis—for dealing with what he calls 'social vulnerability' or risks to ensure security, the plain point is that security, within capitalist modernization, has become 'a profitable public and private sector consumer good like water and electricity'[132]**.**While more will be said later, the point to be emphasized here is that, above all, security (i.e., maintenance of confidentiality, integrity, authentication, availability, and accountability) for protecting data has turned out to be the topmost for all stakeholders in respect of threats, attacks and risks, some new and some traditional, at all levels of Cloud computing including the cloud service and deployment models [210] [211] 'In today's computing world, security concerns follow us everywhere and as such should be paramount to all, not just corporations or government entities' [212].Security is indeed "a major challenge in cloud computing emerging systems" [213].

The birth and propagation of security risks has their origins in 'the loss of control of the systems, applications, data and other resources' of the Cloud computing [214]. Similarly, Razaque and others looks at security from a broad-based perspective, considering cloud computing security as 'a wide concept of strategies, techniques and control measures to protect the safety of data, applications and infrastructures related to cloud computing' and also as related to manifold dimensions such as 'disaster recovery, application security, identification and access management, privacy protection and so on' [215].Cloud computing enables , cheaply and with minimal management, the cloud consumer to obtain 'a large pool of computing resources such as networks, storage, applications, servers, and services remotely' from any place in the world through Internet [216]. While Jouini and Rabai argue that Cloud computing lacks 'absolute security of subscriber data and applications with respect to data integrity, confidentiality, and availability', Akshaya and Padmavati conclude that there is no 'general or universal taxonomy' of cloud

attacks although proper mitigation of threats and attacks are needed to be developed[213] [217]. Samarati and di Vimercati go on to say, in a similar fashion, that 'there is not a one-size-fits-all solution (or even a one-size-fits-all problem definition). There are instead different aspects, with related issues, challenges, and security controls that need to be considered and that can find application in different scenarios' [218]. De Decker remarks that 'there is no system that is 100% safe, except one that is switched off and kept in a bunker' [219]. Roberts is more explicit: 'There will always be some degree of mismatch between the countermeasures on offer and the risks identified in the particular environment of the system. A matrix of risks perceived in the system against risks addressed by the selected countermeasures will show where there is overlap (and, perhaps, overkill) and where there are gaps. The gaps left by the countermeasures are collectively known as residual risk. It is important to understand that in any system there is an element of residual risk which must be accepted by the organization. A little thought will show that the security of a system can never be 100%. There will always be some small risk that information will leak (if only via subverted staff) or be corrupted (if only through mistakes made by careless staff)' [220].Trust, which may depend on many factors (viz., management, processes, policies etc.), among all the concerned stakeholders could be conducive to the establishment of successful Cloud computing environment [221]. In this context it is vital to negotiate and have cloud computing policy concerning the organization 'may reap the benefits of using a cloud service while limiting the threats such as reputation loss and liabilities'[222]. Liu rightly suggests that 'a cloud security policy is a document that states in writing how a company plans to protect the company's cloud solutions and information assets. A security policy is often considered to be a "living document," meaning that the document is never finalized but is continuously updated as technology and business requirements change. Building cloud security policies is a crucial step to take before diving into the cloud, to ensure maximum benefits are achieved and data is secure' [214]. Even then the security solution may not be found. Antonucci draws attention to the primary risks of Cloud computing: 'internet dependency, concentration of data, and poorly executed contracts'. For instance, cloud-computing sites can go down due to outages from Internet service providers. If the cloud providers rely on a third party to safeguard their centralized data, then the client might suffer loss of data when cloud provider's network is compromised. Similarly, weak service contracts could bean hindrance to resolve any problems that may arise later for the client organization [222]. Mithunzi and others, while proposing a holistic cloud computing security taxonomy which will be cited below, aptly notes further that ' considering other cloud-driven technologies such as IoT and cloud converged systems where interconnected objects introduce a host of potential risks, unresolved security challenges could have catastrophic consequences' [223].the complexity and dynamic nature of the Information and Communication Technologies (ICTs) are such as to prompt Huth and others to take a rather summary view of the problems of security. As he says: 'The risk domains of security, privacy, safety, reliability, resilience, and the influence of regulatory environments all combine to determine the risks of security or privacy breach, system failure, or safety issues. Moreover, different operational contexts, such as cryptocurrency, organizational use of IT, or driving a connected car, further complicates the analysis of these risks, especially since a system could be used in a variety of operational contexts over its lifetime. For example, the use of a smart phone as a GPS device in a moving connected car could provide information about the location of individual, a potential breach of privacy, thus altering the risk picture'[224].

The indefatigable exploration for security valve makes sense continual, if not continuous, attacks which have been alluded to in the first section of this paper. Some more may be added in this appropriate context. Cyberspace is intensely saturated with cyber harms that result from cyber attacks. Cyberspace--'a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers' [225] – has become a global information commons which has become a object of cyber attacks. Cyber attacks are targets at individuals' or enterprises' use of cyberspace for 'the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information'[226]. The issue of cyber securitization has become important in view of in view of cyberattacks, viz. Snowden's 2013 leaks of secret and classified NSA surveillance programmes, the alleged Russian hacking of the 2016 US national elections, 2017's Equifax beach , and worldwide WannaCry ransomware attack in May 201 [227]. Recently, these attacks due to Covid-19 pandemic are affecting individuals, business enterprises, and even CC. It is no surprise that *Check Point Cyber Security Report (2020),* which detailed various types of cyber incidents occurring in 2019, states that 'if there's one clear takeaway from 2019, it's that no organization, big or small, is immune from a devastating cyber attack. Cyber exploits are more sophisticated, illusive, and targeted than ever before... Attacks from unknown threats pose critical risks to businesses, and unfortunately, they're also the hardest to prevent'. One of the key findings of the 2019 Cloud Security Report mentions that the top four public cloud vulnerabilities cited by the respondents were the unauthorized cloud access (42%), insecure interfaces (42%), misconfiguration of the cloud platform (40%), and account hijacking (39%).The leading operational cloud security headaches are lack of visibility into cloud infrastructure security and compliance (67% in total), setting consistent security policies across cloud and on premise environments and a lack of qualified security staff (31% each) [228]. Deloitte (2020) reports 'a spike in phishing attacks, Malspams and ransomware attacks as attackers are using COVID-19 as bait to impersonate brands thereby misleading employees and customers. This will likely result in more infected personal computers and phones. Not only are businesses being targeted, end users who download COVID-19 related applications are also being tricked into downloading ransomware disguised as legitimate applications' [229]. Coronavirus-themed cyberattacks were worldwide. The countries targeted by largest share of global malicious spam emails with 'coronavirus' in the subject from January 1 to March 27, 2020 are, for example,, the UK (20.8%), France (11.5%), the US (8.2%), Italy (5.9%),Belgium (8.2%), Germany (8.1%), India (4.9%), and Netherlands (3.5%). [230]. Khan et al. mention specifically ten (10) deadly cyber security threats closely on the heels of the global outbreak of Covid-19 pandemic since 30th January 2020,when the World Health Organization (WHO) confirmed it as an international health emergency. These are: (1) DDOS Attack, (2) Malicious Domains, (3) Malicious Websites (4) Malware (5) Ransomware (6) Spam Emails, (7) Malicious Social Media Messaging, (8) Business Email Compromise, (9) Mobile Threats, and (10) Browsing Apps. For reasons of financial gains and other motives, the hackers and cyber criminals attacked individuals, government officials, and even medical and health care systems, online workers, and there also has been an increased 'registration of malicious domains, websites, and spam emails' [231]. ISACA, CMMI Institute and Infosecurity Group surveyed a global population of over 4,500 professionals involved in risk decisions for large and small enterprises, across six continents and The industries, surveyed include manufacturing to government and financial services, and every industry in

between in regard to enterprises' risk management programs. According to them, cybersecurity risks have now become an emerging computing domain and, accordingly, their challenges have become difficult, among other things, due to security budget constraints (39%), lack of adequate number of security personnel (52%), missing skills in the existing cybersecurity team(51%), changes/advances in technology (64%), increased threats and their frequency of occurrence(45%), legal and/or regulatory challenges (29%). This illustrates that the problems in mitigating cybersecurity risks have also increased ranging from very difficult to very easy. To cite a few instances, mitigating information/cyber security has become (1) very difficult (10%), (2) difficult (39%), (3) medium (43%),(4) easy (8%), and (5) very easy (1%). The corresponding figures for compliance/legal mitigation difficulties are 4%, 24%, 51%, 18%, and 3%. For reputation risks the figures are 12%, 38%, 39%, 9%, and 1%. The same for operation risks are 3%, 24%, 55%, 16% and 2%. .As far as cloud computing is concerned, the report says that "Cloud, as one would expect, is a significant pain point for many enterprises and a key source of potential new risk. Although cloud is no longer an emerging technology because most enterprises have adopted it extensively, the trajectory of cloud—both adoption dynamics and risk introduced—can serve as a bellwether for other, newer technologies. ... When asked about the impact of new technologies on the enterprise risk profile, respondents most often cite cloud as increasing threats and vulnerabilities (70 percent). There is a good reason why the cloud percentage is so high— practitioners are intimately familiar with the challenges of cloud, including compliance and regulatory challenges, data sovereignty, lack of direct operational control over service provider environments, shadow adoption, and numerous other pain points. However, and perhaps unexpectedly, respondents cite other technologies—Internet of Things (IoT) (34 percent), machine learning and artificial intelligence (AI) (25 percent), and blockchain (13 percent)—significantly less as sources of potential new vulnerabilities and threats' [232].

This brief review of threats, vulnerabilities, attacks and risks is very much reminiscent of Beck's analysis of the uncertainty and incalculability of the manufactured risks immanent in the risk society, and it indeed points to the domain of not-knowing or non-knowledge persisting in both Cloud technology and risk theoretical perspective, in both science and technology, on the one hand, and social sciences, on the other. Thus Beck could say that 'the very power and characteristics that are supposed to create a new quality of security and certainty simultaneously determine the extent of *absolute uncontrollability* that exists. The more efficiently and comprehensively the anticipation of consequences is integrated into technical systems, the more evidently and conclusively we lose control. All attempts at minimizing or eliminating risk technologically simply multiply the uncertainty into which we are plunging the world' [148]. Today's 'manufactured uncertainties', not perceived previously and breaking with the institutionalized routines, are 'incalculable, uncontrollable and in the final analysis no longer (privately) insurable (climate change)' [159]. In any case, risk researchers and analysts in the cloud domain strive always to achieve, as one should, the effective cloud computing security by synchronizing 'people, process and technology, each of which is integral to successful security. Security teams must continually develop their knowledge by collaboration with the broader security community; organizational policies, protocols and procedures must adapt to evolving threats; and finally, security platforms and analytics must effectively be applied. The strength of the alignment among these three components determines the success of an organization's overall security program' [233]. One important requirement in this regard is, among other things, framing and enforcement of a clear security policy. As Antonucci suggests: 'Clarify the purpose of your cloud computing policy as to how your organization may reap the benefits of using a cloud service while limiting the threats such as reputation loss and liabilities (should the service not perform as expected). It is vital that organizations both procure cloud provider services effectively and understand the contract language and negotiate key terms'[222]. For detecting, preventing or recovering from security attacks, Alani suggests the use of security mechanisms as process or a device ((viz., .encryption, hashing etc) and needed security service such as a processing or communication service to enhance data security and data transmission [211]. In any case, as previously shown in Section III, concept of risk, its definition and relations of definition along with different usages in different disciplines has already been discussed. The particular point to note is that Cloud computing researchers and analysts more or less define the concept in specific ways. Put otherwise, experts do not necessarily accept any one definition unanimously [147]. The following three Tables 20, 21 and 22, and Figure 22, taken from Wani and others (2019) [234], Kumar and Goyal (2019) [235], and Mithunzi and others (2020) [223], Buyya and others (2018) [236] illustrate how they differ in framing the discourse of cloud security assurances, thus sustaining Beckian perspective on relations of definition. Chandrasekaran aptly concludes that even though security issues have been addressed, still there is 'no standard development procedure is defined for the development of the cloud model' [237]. The divergence of cloud security recommendations are not confined to the above-mentioned analysts; there are others too who also differ in this respect, bolstering the analysis of Beck [218] [238] [239] [240] [241] [242] [243] [244] [245] among themselves depending the Cloud computing dimensions of security emphasized. Maroc and Zhang, who analyzed Cloud security Classifications, Taxonomies, and Ontologies had this to say: 'Although several classification schemes have been proposed, there is still no established taxonomy or ontology in general use. There is a need for a holistic approach that integrates efficiently the multifaceted nature of the cloud. We believe that a common framework of these classifications can further aid in the understanding of the security issues in the cloud context'[246]. Table 23, taken from Maurer and Hinck, illustrates recent cloud security incidents [247].

Cloud Computing Security Issue and Classifications		
1	Security standards	1. Deficiency of security measures.2.Compliance dangers. 3. Deficiency of looking into 4. Lack of lawful components (service-level understanding). 5.Trust
2	Network	1. Appropriate establishment of system firewalls. 2 Security setups. 3. Internet protocol shortcomings. 4. Internet Requirements.
3	Access Control	1. Accounts. 2. Malicious insiders. 3. Validation. 4. Private client access. 5. Browser Safety.
4	Data	1. Redundancy of information and data.2.Loss and data and information. 3. Location of data and information.4.Privacy of data and information. 5. Protection of information. 6. Data Availability.
5	Cloud Infrastructure	1. Uncertain interface of API. 2. Quality of administration. 3. Allocation of technical defects. 4. Dependability of Suppliers. 5. Security misconfiguration. 6. Multi-occupancy. 7. Server Site and Backup.

Table 20: Cloud computing security issues and classifications

At the end of the day it is only in the fitness of things to say that 'securitzation in cloud computing' has progressed as a component of what Schuilenburg calls the 'securitization of society'— a concept that implies 'mobilization of a range of actors— health, education, spatial planning, welfare, the retail sector, energy utilities— whose aim is to make our lives safer and more secure' [266]. The goal of securitization in cloud computing can only be seen as part a of the entire process of ordering, or rather making safer and secure, the cloud computing processes and technologies as a whole. According to *Cloud Standards Customer Council* (2017), cloud customers should ask themselves and their cloud providers relevant critical questions and seek answers during each of the 10 (ten) steps of *Security Assessment* process concerning these issues: 1. Ensuring effective governance, risk and compliance processes exist; 2. Provision for audit and ensuring reporting of operational and business processes; 3. Managing people, roles and identities; 4. Ensuring proper detection of data and information; 5. Enforcement of privacy policies; 6. Assessing the security provisions for cloud applications; 7.Ensuring cloud networks and connections secure; 8.Evaluating security controls on the physical infrastructure and facilities; 9. Managing security in the cloud service agreement; and 10. Understanding the security requirements of the exit process [306]. In this regard it is of importance to note that, according to Cloud Security Alliance Definition, cloud computing security refers to' the set of control-based technologies and policies designed to follow to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use'. However, as per ISO27001 definition, the security is 'preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved' [307].

Cloud Computing Security	
Requirements	**1. Confidentiality. 2. Integrity. 3. Availability. 4. Authentication. 5. Authorization. 6. Accountability. 7. Privacy.**
Threats	**1. Data Breaches. 2. Weak Identity, Credential and Access Management. 3. Insecure APs. 4. System and Application Vulnerabilities. 5. Account Hijacking. 6. Malicious Insider. 7. Advanced Persistent Threats (APTs). 8. Data Loss. 9. Insufficient Due Diligence. 10. Abuse and Nefarious use of Cloud Services. 11. Denial of Service. 12. Shared Technology Vulnerabilities.**
Vulnerabilities	**1. Application and Interface Layer. 2. Platform Layer. 3. Infrastructure Layer—Virtualization and Hypervisor. 4. Infrastructure Layer—Network. 5. Infrastructure Layer –Storage. 6. Infrastructure Layer—Hardware. 7. Infrastructure Layer—Facilities. 8. Assurance and Compliance Vertical**
Countermeasures	**1. Identity and Access Management. 2. Encryption and Key Management. 3. Digital Signature and Message Digest. 4. Intrusion Detection and Prevention System. 5. Web Application, Services and Interface security Measures. 6. Software Development environment security Measures. 7. Virtual Environment Security Measures. 8. Network Communication Security Measures. 9. Data Storage Security Measures. 10. Hardware Security Measures. 11. Physical Security Measures. 12. Assurance and Compliance Measures.**

Table 21: Cloud computing security taxonomy

V. II. THREATS, VULNERABILITIES, RISK AND CYBER-HARMS IN CLOUD COMPUTING

Table 23 points to the threats, vulnerabilities, and risks that are always evolving with the appearance of new technologies along with complexities there in, affecting functionalities and services of Cloud computing. The concepts of threat, vulnerability and risk are often used interchangeably although they are distinct in their definitions [248]. Generally speaking from the perspective of Cloud computing, *threat*is an event that causes harm to a system in different forms (viz. damaging the system's reliability or demoting the CIA*triad* (i.e., confidentiality, availability or integrity of information) in the system. *Vulnerability* stands for

A General View of Cloud Security Challenges		
1	**Software security**	**1. Platform and Framework. 2. User-fronted issue**
2	**Storage Security**	**1. Malware. 2. Sanitization. 3. Cryptography. 4. Availability.5. Unreliable Computing. 6.Data Storage**
3	**Virtualization Security**	**1. Availability. 2. Malware. 3. Mobility. 4. Virtualized Networking. 5. VM Monitoring. 6. Managing Images**
4	**Internet Service Security**	**1. Availability. 2. Web Services. 3. Protocols and Standards. 4. Persistent Threats.**
5	**Access Security**	**1. Anonymization. 2. Identity Management. 3. Authorization.4. Authentication. 5. Credentials. 6. Physical Access.**
6	**Trust**	**1. Anonymization. 2. Audidability. 3. Reputation. 4. Human Issues. 5. Adoption Issues.**
7	**Compliance and Legal**	**1. Governance. 2. Accountability. 3. Legal Issues. 4. Forensics.**
8	**Network Security**	**1. Mobile Security. 2. Perimeter Security.**

Table 22: A general view of cloud security challenges

weaknesses or flaws in the hardware, software or process. Threats might exploit them to damage the system. Bhowmik defines *risk* is 'the ability of a threat to exploit vulnerabilities and thereby causing harm to the system. Risk occurs when threat and vulnerability overlap. It is the prospect of a threat to materialize '[249]. For Dahbur, risk is equal to *Vulnerability x Threat x Impact x Likelihood* [250].Generally vulnerabilities emanate from bug. These arise out of 'flaws in the code logic, poor software design, or implementation choices' and bugs may affect the information system, i.e. the CIA *triad* [251]. Impact refers to 'the

amount of harm' that results when risk is materialized, i.e. when the threats exploits a vulnerability [252].The inter-relationship between the three in Cloud computing in shown by Hakak et al. in the following Figure 23 [27].

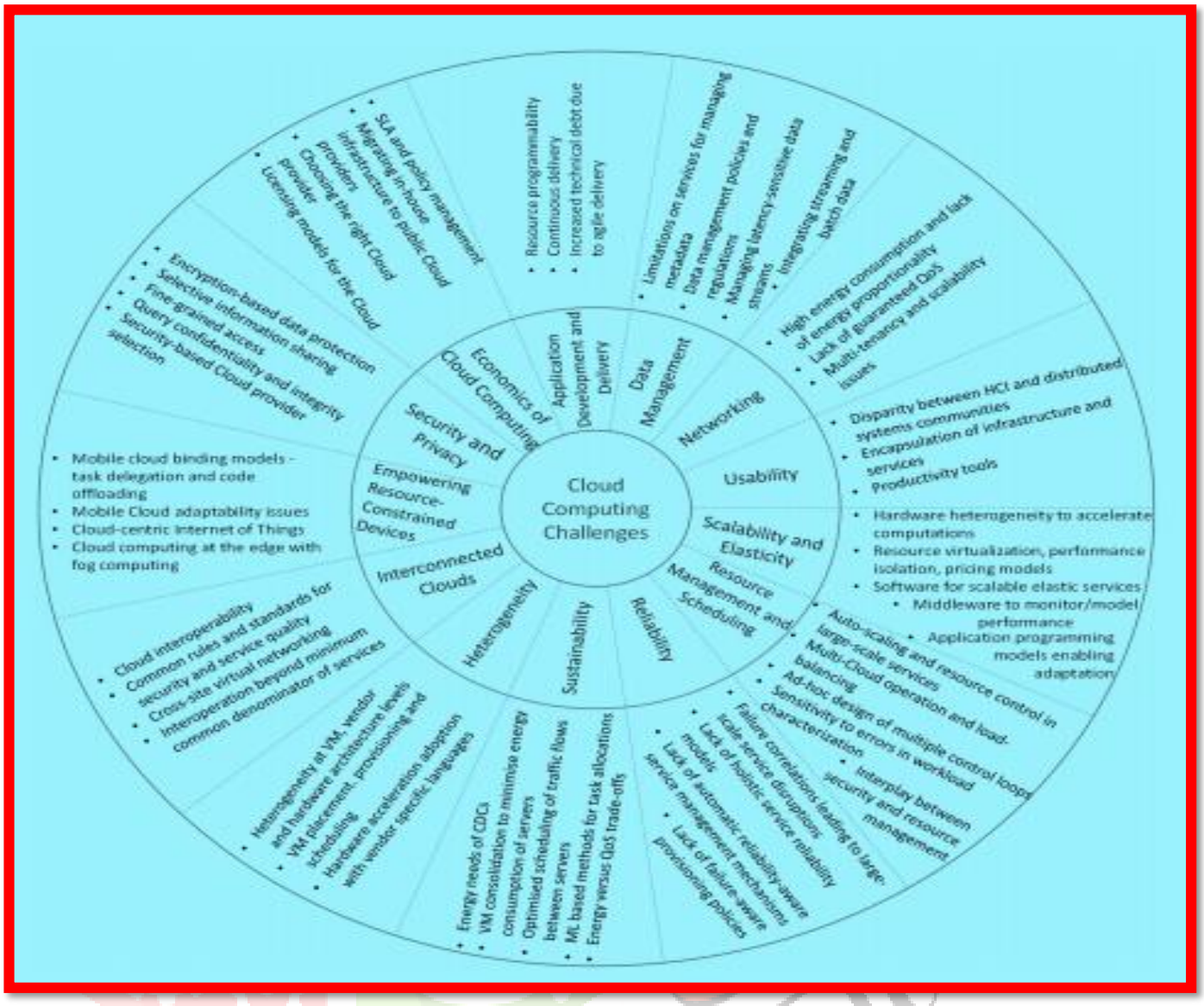


Figure 22: Cloud computing challenges, state of the art, and open issue

Since threats, vulnerabilities and risks are all interrelated, it is useful to look at the current situation in those domains. *Cloud Security Alliance* lists top Egregious Eleven (ranked in order of significance) threats of 2019 that are 'inherent with cloud security': 1. Data Breaches. 2. Misconfiguration and inadequate change control. 3. Lack of cloud security architecture and strategy.4.Insufficient identity credential, access and key management. 5. Account hijacking. 6. Insider threat.7.Insecure interfaces and APIs 8. Weak control plane.9.Metastructure and applistructure failures. 10. Limited cloud usage visibility. 11.Abuse and nefarious use of cloud services [253].Cloud analysts often list cloud threats that they deem from their viewpoints based on different considerations such as levels, likelihood, importance etc, and more often they differ than when they agree. To give an instance, Tabrizchi and Rafsanjani recently (2020) list such threats and risks as 1. Data breaches. 2. Hacked interface and application program interfaces. 3. Account hijacking. 4. Malicious insiders. 5. Distributed denial of service attacks. They also mention specifically 12 types of cloud attacks (viz., 1.Abuse of functionality. 2. Data structure attack. 3. Embedded malicious code. 4. Exploitation of authentication. 5. Injection. 6. Path traversal attack. 7. Probabilistic techniques, 8Protocol manipulation. 9. Resource depletion. 10. Resource manipulation. 11. Sniffing attacks. 12. Spoofing) [254]. In contrast, Ahmed and Litchfield (2018) provided taxonomy of Cloud computing threats, dividing it into two types. First, they take due note of human factors (Trust, Compliance, Regulations, Competence/Specialization, SLA Misinterpretation and Social context). The second category is technology which he divides further in two types: (A) Software (viz., Local Platform, Network Protocols, Virtualization, Software Tools, Web Services Security Mechanisms, and Mobile Computing); and (B) Hardware, which is further divided into three types such as Computing Services, Internal Infrastructure, and External Networks (viz. Mobile/Wireless Networks, and Fixed Networks). Having suggested that the proposed taxonomy is applicable to a wide range of issues, they contend that 'to better understand the genre and nature of any newly introduced threat, the taxonomy may be applied by categorizing them or by considering how threats are related to other categories' [255].The implications of the threats can be understood, also actually mainly, in the light of Cloud computing risks, vulnerabilities and assets which were listed by The European Network and Information Security Agency (ENISA) in 2009. It included seven(7) policy and organization risks, thirteen (13) technical risks, and four (4) legal risks, and eleven (11) non-cloud specific risks, totaling altogether thirty five(35) risks. The number of cloud specific vulnerabilities was fifty three (53). It also listed twenty three (23) cloud assets. The Table 24 depicts the overall listing [256].It is important to note that this list was revised and updated in 2012 publication which listed twenty three (23) risks, as well

as their probability rating, their impact and levels. Taken together, it is needless to state that they convey quite a comprehensive view of the risks that afflict cloud computing. It concludes that 'ENISA will continue to monitor the developments related to risks of Cloud computing and update the Risk Assessment as necessary' [257].

Key Cloud Security Incidents (2014–2019)		
1	Sept. 2014	Responding to a vulnerability in the Xen hypervisor, AWS and Rackspace initiated reboots of their computing instances around the globe to implement security patches.
2	Nov. 2014	A system update rolled out globally for Microsoft Azure's storage services caused failures in its virtual machines. Some customers experienced disruptions for up to eleven hours.
3	Aug. 2015	Lighting strikes that hit the power grid in Belgium caused a failure in Google Compute Engine services for the local region. Some customers lost data because storage systems experienced repeated power drain.
4	Sept. 2015	A failure in AWS's internal metadata service caused a cascading set of disruptions that triggered outages for many customers relying on AWS services in the US-EAST-1 region, including Airbnb, IMDb, and Netflix.
5	Jan. 2016	faulty update prevented Microsoft Office 365 users from accessing some email messages, a delay lasting up to five days for some users.
6	May 2016	A Salesforce U.S. data center went down for about one day, tracing its cause to a failed circuit breaker in another data center that caused a flood of traffic leading to disruptions for many customers.
7	Feb. 2017	Fn AWS outage in US-EAST-1 region caused failures in many online platforms and organizations, including Airbnb, Signal, Slack, and the U.S. Securities and Exchange Commission over a five-hour period. One firm later estimated that the downtime caused a loss of $150 million for the S&P 500 companies affected.
8	Mar. 2017	A power failure leading to software errors caused issues with Azure's storage service, especially for customers in its U.S. East region. Azure restored full service in eight hours.
9	Jun. 2017	Security researchers warned chip manufacturer Intel and others about the Spectre/Meltdown speculative exploitation vulnerabilities. They were kept secret for six months with the chip manufacturers working with major tech companies to implement a solution.
10	Jan. 2018	The Spectre and Meltdown vulnerabilities became public, with CSPs working to implement software and hardware fixes.
11	Jun. 2018	Azure customers in Northern Europe experienced a five-hour outage due to hot summer temperatures in a data center, leading to automated infrastructure shutdowns
12	Sept. 2018	Lightning strikes caused failure at an Azure data center in Texas, affecting customers using storage in the local region as well as some Azure services globally. The local region was offline for about four hours.
13	Nov. 2018	The misconfiguration of an internet routing protocol by a Nigerian internet service provider caused failures for traffic to Google Cloud after traffic was mistakenly sent through China.
14	Jan. 2019	Issues with an external domain name service provider caused errors in internal Microsoft Azure systems that lead to the accidental dropping of customer databases, which were later recovered.

Table 23: Examples of Cloud Security Incidents (2014-2019)

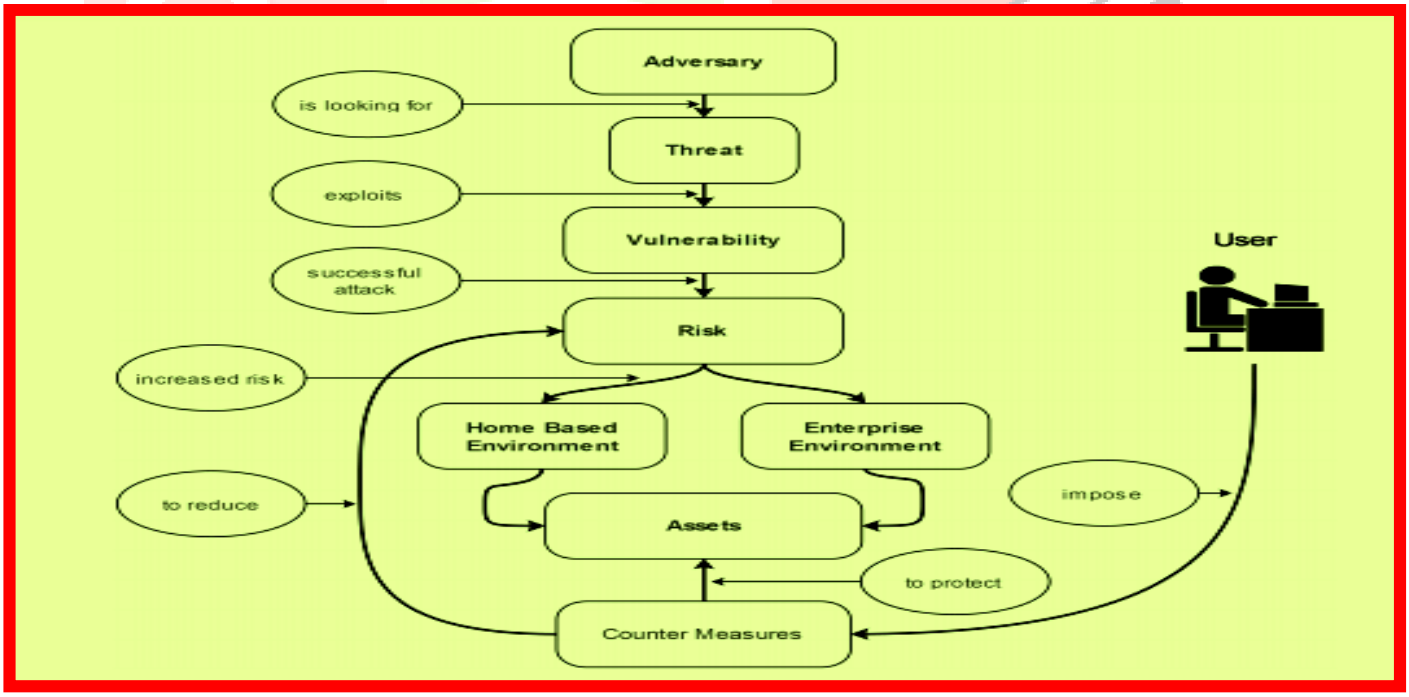


Figure 23: Relationship among threat, vulnerability, and risk

ENISA, 2009: RISKS, VULNERABILITIES, AND ASSETS			
Nos.	Risks-Probability-impact	Cloud Specific Vulnerabilities	Assets
Policy and Organizational			
1	Lock-In- High- Medium	Authentication Authorization Accounting (AAA) vulnerabilities	Company reputation

2	Loss Of Governance- Very High - Very High	User provisioning vulnerabilities	Customer trust
3	Compliance Challenges-Very High -High	User de-provisioning vulnerabilities	Employee loyalty and experience
4	Loss Of Business Reputation Due To Co-Tenant Activities-Low -High	Remote access to management interface	Intellectual property
5	Cloud Service Termination Or Failure- N/A - Very High	Hypervisor vulnerabilities	Personal sensitive data
6	Cloud Provider Acquisition--N/A -Medium	Lack of resource isolation	Personal data
7	Supply Chain Failure-Low - Medium	Lack of reputational isolation	Personal data - critical
	Technical Risks		
8	Resource Exhaustion (Under Or Over Provisioning)-Medium/Low or Low/Medium - Low/Medium or High Depending On Capacity to provide to the customer	Communication encryption vulnerabilities	HR data
9	Isolation Failure-Low (Private Cloud)/ Medium (Public Cloud)- Very High	Lack of or weak encryption of archives and data in transit	Service delivery - real time services
10	Cloud Provider Malicious Insider - Or Abuse Of High Privilege Roles-Medium (Lower Than Traditional) -Very High (Higher Than Traditional)	Impossibility of processing data in encrypted form	Service delivery
11	Management Interface Compromise (Manipulation, Availability Of Infrastructure)-Medium- Very High	Poor key management procedures	Access control / authentication / authorization (root/admin v others)
12	Intercepting Data In Transit- Medium - High	Key generation: low entropy for random number generation	Credentials
13	Data Leakage On Up/Download, Intra-Cloud-Medium (N/A)-High	Lack of standard technologies and solutions	User directory (data)
14	Insecure Or Ineffective Deletion Of Data-Medium - Very High	No source escrow agreement	Cloud service management interface
15	Distributed Denial Of Service (Ddos)- Customer: Medium/ Provider: Low- Customer: High /Provider: Very High	Inaccurate modelling of resource	Management interface APIs
16	Economic Denial Of Service (Edos)-Low-High	No control on vulnerability assessment process	Network (connections, etc.)
17	Loss of Encryption Keys-Low-High	Possibility that internal (cloud) network probing will occur	Physical hardware
18	Undertaking Malicious Probes Or Scans-Medium-Medium	Possibility that co-residence checks will be performed	Physical buildings
19	Compromise Service Engine- Low -Very High	Lack of forensic readiness	Cloud Provider Application (source code)
20	Conflicts Between Customer Hardening Procedures And Cloud Environment- Low - Medium	Sensitive media sanitization	Certification
	Legal Risks		
21	Subpoena And E-Discovery- High-Medium	Synchronizing responsibilities or contractual obligations external to cloud	Operational logs (customer and cloud provider)
22	Risk From Changes Of Jurisdiction-Very High-High	Cross-cloud applications creating hidden dependency	Security logs
23	Data Protection Risks-High-High	SLA clauses with conflicting promises to different stakeholders	Backup or archive data
24	Licensing Risks-Medium-Medium	SLA clauses containing excessive business risk	
	Risks not Specific to the Cloud	**Cloud Specific Vulnerabilities**	
25	Network Breaks- Low - Very High	Audit or certification not available to customers	
26	Network Management (Ie, Network Congestion / Mis-Connection / Non-Optimal Use)-Medium -Very High	Certification schemes not adapted to cloud infrastructures	
27	Modifying Network Traffic-Low-High	Inadequate resource provisioning and investments ininfrastructure	
28	Privilege Escalation-Low-High	No policies for resource capping	
29	Social Engineering Attacks (Ie, Impersonation)-Medium-High	Storage of data in multiple jurisdictions and lack of transparency about this	
30	Loss or Compromise of Operational Logs -Low-Medium	Lack of information on jurisdictions	
31	Loss or Compromise Of Security Logs (Manipulation Of Forensic Investigation)- Low- Medium	Lack of completeness and transparency in terms of use	
		Vulnerabilities not specific to the cloud	
32	Backups Lost, Stolen-Low—High	Lack of security awareness	
33	Unauthorized Access To Premises (Including Physical Access To Machines And Other Facilities)- Very Low-High	Lack of vetting processes	
34	Theft of Computer Equipment-Very Low - High	Unclear roles and responsibilities	
35	Natural Disasters-Very Low - High	Poor enforcement of role definitions	
36		Need-to-know principle not applied	
37		Inadequate physical security procedures	

38		**Misconfiguration**
39		**System or OS vulnerabilities**
40		**Untrusted software**
41		**Lack of, or a poor and untested, business continuity and disaster recovery plan**
42		**Lack of, or incomplete or inaccurate, asset inventory**
43		**Lack of, or poor or inadequate, asset classification**
44		**Unclear asset ownership**
45		**Poor identification of project requirements**
46		**Poor provider selection**
47		**Lack of supplier redundancy**
48		**Application vulnerabilities or poor patch management**
49		**Resource consumption vulnerabilities**
50		**Breach of NDA by provider**
51		**Liability from data loss**
52		**Lack of policy or poor procedures for logs collection and retention**
53		**Inadequate or misconfigured filtering resources**

Table 24 Cloud Computing Risks, Vulnerabilities and Assets

There are numerous researchers who have concentrated on the risks in Cloud computing. But the point remains that all of them have their own viewpoints in including what are and what are not risks, in spite of the fact that there are more often than not common risks in their respective listings. For instance, Malik and Singh (2019) list the following 16 risks in Cloud computing (2019): 1. Insecure Interfaces developed for cloud application. 2. Sensitive credentials access control and authentication. 3 Less control over computing environments. 4. Insecure data flow over network. 5. Untrained software professionals. 6. Data leakage and privacy problems due to data sharing. 7. Improper database design. 8. Service unavailability. 9. Natural Disasters. 10. Improper data locations.11.Data virtualization issue.12.Noncompliance with regulations.13.Service provider mismanagement. 14. Improper transaction management. 15. Poor service Level agreement. 16. Reputational loss due to inaccurate resources estimates [258]. Belbergui and others (2019) have proposed, reviewing of the concerned literature, identification of users' risks by type in the general context of Cloud computing and have classified them as follows: A. ***Generic Risks*** (*Risks related to data Security*, Risk of data loss, Risk of data modification, Non-recovery of data, Loss of controlled destruction of data); *2) Usurpation of Identity and Unauthorized Access* (Usurpation of identity, Unauthorized access); 3.*Technical Risk Deficiencies in Interfaces and APIs*; 4.*Risks Related to the Choice of the Service Provider* (The use of data except perimeter, Management of Cloud by incompetent or malicious people, Non-compliance with security requirements); 5. *Legal Risk*; 6. *Risks Related to the Break of Service* (Risk of moving to another supplier, Cessation of service, Risk of the end of contract); **B. *Classification of the Risks Corresponding to the Service Models*** *1) Risks in IaaS* (Infrastructure management by incompetent or malicious personnel of consumer organization; Bad use of virtual machines); *2) Risks in PaaS* (Loss of control of its applications, The use of Service Oriented Architecture (SOA), Loss of control of the application development cycle); *3) Risks in SaaS* (Risk of loss of data ownership); **C. *Classification of the Risks Corresponding to the Deployment Models***:*1) Risks in a Public Cloud* (Collateral risks, Manipulation of resources by parties using the same Cloud); *2) Risks in a Private Cloud* (Risk of insufficient resources); *3) Risks in a Hybrid Cloud* (Interdependence); ***D. Classification of the Risks Corresponding to the Types of Hosting*** (*1) Risks in External Cloud* (Reallocation of resources, Non-isolation of environments and data, Loss of control and governance); *2) Risks in Internal Cloud*, i.e., common risks which the cloud consumers face in all cloud types [259].Three specific risks relate to the principles of confidentiality, integrity, and availability, as mentioned in the NIST (National Institute of Standards and Technology) document, are most relevant to the cloud computing security. Confidentiality means that only authorized persons or systems can access protected data. Integrity means that cloud user's data, software and hardware are not modified or deleted by anyone in an unauthorized manner. Availability means that data will only be available, when needed, to the authorized cloud entities, whether a cloud user, proves or device [260] [261] [41]. Table 25 below shows the well-known cybersecurity triad of confidentiality, integrity, and availability to a variety of risk vectors and they include 'rough guesstimates of the probabilities that various incidents will occur, ranging from more common incidents to potential black swan'. These risk vectors are only a starting point for discussing how different risks could be improved with opinions from other experts over a period of time. Maurer and Hinck thus cautiously remark that 'cloud security is not an all-or-nothing affair. It is simply less well conceptualized than existing cybersecurity. Potential risks range from the cascading effects of temporary disruptions to the exploitation of vulnerabilities in the underlying hardware and software that run the cloud. And, of course, while the cloud can be seen as "someone else's computer," the basics of cybersecurity still apply, and customers may expose themselves by not fulfilling their end of the shared responsibility for security. Understanding the new potential risks associated with the cloud and what their impacts might be is a crucial task for

CONFIDENTIALITY				
	Effects on	**Type**	**Vectors**	**Probability**
1	**External: Unintentional Data Leakage**	Accidental	Customer misconfigure or does not enable security keys for stored data	Very High
2		Accidental	CSP misconfigures or does not enable security keys for stored data	Medium
3		Structural	Vulnerability discovered in security protocols making data accessible to third parties or the public internet	Low

4	External: Malicious data theft	Adversarial	Malicious actor steals credentials from customer to steal data hosted in the cloud	Medium
5		Adversarial	Threat actor compromises CSP to steal security keysto access customer accounts	Low
6		Adversarial	Insider threat at customer or CSP permits theft of data	Low
7		Adversarial	Manipulated domain name system (DNS) or Border Gateway Protocol (BGP) routing information allowsmalicious actors to redirect cloud-customer traffic	Medium
8		Adversarial	Installation of fake hypervisor through server compromise to exfiltrate data	Very Low
9	Internal: From one customer to another	Accidental	Misconfiguration of hypervisor or containers permits customers to access data of other customers	Low
10		Adversarial	Exploitation of hypervisor or container vulnerability permits virtual machine escape	Low
11		Structural	Chip or hardware vulnerability allows virtual machine/container escape	Low
INTEGRITY				
	Effects on	**Type**	**Vectors**	**Probability**
12	Data Deletion	Accidental	Misconfiguration of automated process leads todeletion of virtual machines and stored data	Medium
13		Accidental	Automated process deletes datasets because of internal errors or unavailability	Medium
14		Accidental	Automated process or human error causes overwritingof datasets, losing information	Medium
15		Adversarial	Adversary compromises CSP system managers anddeletes large swaths of customer data	Low
16		Adversarial	CSP internal systems infected with wiper malware or ransomware	Low
17	Data Manipulation	Accidental	Error in automated process or human error causesalterations to replicated data	Medium
18		Adversarial	Malicious insider within enterprise customer alters data for personal gain	Low
19		Adversarial	Malicious insider at CSP alters data of single or many customers	Low
20		Adversarial	Hacker steals credentials from user, gains access to data in the cloud, and alters it	Medium
21		Adversarial	Compromise of CSP permits hackers to alter data across many customer accounts	Medium
22		Adversarial	Man-in-the-middle threat between CSP and customer substitutes altered data to be stored in the cloud	Low
23	Data asynchrony	Accidental	Failures in availability lead to different copies of data indifferent CSP regions because of asynchronous geo-replication	Medium
AVAILABILITY				
	Effects on	**Type**	**Vectors**	**Probability**
24	Temporary Unavilability	Environmental	Lightning strike on data center	Very High
25		Environmental	Flooding of data center	High
26		Environmental	Earthquake near data center	High
27		Environmental	Damage to power lines leading to failures of backups (from natural disasters)	High
28		Accidental	Accidental cutting of undersea or local fiber-optic cables	Medium
29		Accidental	Unintentional rebooting of all servers within anAZ or availability region	Medium
30		Accidental	Accidental deletion of a large number of virtual machines	High
31		Accidental	Use of incorrect configuration settings during routine upgrades leads to loss of availability	Medium
32		Accidental	Insufficient capacity of backup servers during routine maintenance	Low
33		Accidental	Internal automated or human errors during routine maintenance lead to internal traffic flood, causing denial of service	Medium
34		Accidental	Expiration of HTTPS certificates leads to authentication unavailability	Medium
35		Accidental	Misconfiguration of BGP or DNS information by outside providers for CSPs leads external networks to drop traffic	Medium

36		Adversarial	Compromise of customer accounts to conduct cryptocurrency mining operations (cryptojacking)	Medium
37		Adversarial	Distributed denial of service attack on CSP	High
38		Adversarial	Intentional deletion of virtual machine or stoppage of services by insider	Low
37	**Permanent Unavailability**	Environmental	Nuclear meltdown or accident renders data center inoperable	Very Low
38		Adversarial	Bombing or other attack on data centers by terrorists or state actors	Very Low
39		Adversarial	Intentional destruction of power grids leads to data center failure	Low
40		Adversarial	Cutting of multiple undersea cables degradesinternational internet connectivity	Low
41	**Second-order effects of unavailability**	Structural	Automated failure detection systems mask errors, leading to catastrophic failure and large-scale downtime	Medium
42		Structural	Unavailability of core systems or other components delays efforts to restore system	Medium
43		Structural	Unavailability of core systems leads to unintentional activities by automated systems, resulting in either deletion of virtual machines, dropping of databases, or other services going offline	Medium
44		Structural	Unavailability in a key region leads to widespread downtime of key platforms that rely on services based in that region	Medium

Table 25: Mapping the Impact of Cloud Security Risk

policy makers to undertake now' [262]. The CIA paradigm is stands out as a means to select security capabilities 'to counter risk to the system from a number of forms of cyber attack'. Furthermore, it has been stated that role of standards or frameworks is to act as best practice guides in handling risks. Since the task of the security engineers is above all to minimize 'the publicized attacks' , one needs 'to respect issues such as scientific method, repeatability, ethical behavior and presentation of results, and ought to be as objective as possible -presenting facts and evidence that support any claim'[263]. Table 26, based on Goman's work, provides selected the standards that are examples of practices in risk analysis along with definitions of risk. However seen from Beck's point of view the frameworks are not beyond infallibilities. What is notable in this Table is the plurality of definitions of risks, which are conflictual or contradictory in nature. In Beckian terms it is, in the first instance, symbolic of the differences of opinion among the risk analysts—this aspect falling within the scope of Beck's relations of definitions in respect of the respective worldviews on security highlighting both conceptual and methodological approaches to risk, its nature and even security objectives within the same field and discipline, Goman, in critiquing this aspect, goes on to say that 'all of the frameworks are not perfect in reflection of the nature of risk. It is surprising, but the frameworks refer to each other for alignment and support in narrow areas like project management or IS. The ambiguity of the risk concept is also reflected in a notion of risk as 'a good thing" [264].

V. III. CLOUD RISK ANALYSIS: RISK MANAGEMENT AND RISK ASSESSMENT

Risks, when materialized as real events cause deleterious consequences, as Beck theorized in his risk society thesis. Likewise, risks in the cyber world also cause harms, as pointed out by Agrafiotis and others who drew an analogy fro Beck and Giddens who discussed risks immanent in nuclear, chemical and biomedical technologies. Agrafiotis and others classified cyber-harms into five main categories, shown in Figure 24: 'Physical or Digital harm' referring to a physical or digital negative effect on someone or something; 'Economic harm' relating to negative financial or economic consequences; 'Psychological harm' focusing on an individual and their mental well-being and psyche; 'Reputational harm' relating to the general estimation held about an entity; and ' Social and Societal harm' that may result from within a social context or society more broadly. Cyber-harm is initially define as the damage that arises as a direct result of an attack conducted wholly or partially via digital infrastructures, and the information, devices and software applications that these infrastructures are composed of'. In Figure 24 Agrafiotis and other provides a taxonomy of organizational cyber-harms –damages – that will help enterprises to engage in 'security risk management tasks intended to identify, assess, prioritize and treat the various risks that they face', thereby facilitating organizations in comprehending and realizing the desired cybersecurity [265].

The nature and scope of risk analysis in its general outline has already been provided earlier in section Section III of the present paper in the light of differential perspectives of the selected risks analysts. The broader definition of risk analysis has been provided by Aven who defines risk analysis as **'**risk understanding, risk assessment, risk characterization, risk communication, risk management, risk governance, and policy relating to risk, in the context of risks which are a concern for individuals, public and private sector organizations, and society at a local, regional, national or global level'[96]. Figure 11 reproduced ISO 3100: 18which enunciates Principles, framework and risk management process, and Figure 12 provided by Yoe who has listed five steps in the risk management process such as (1) risk identification; (2) risk estimation; (3) risk evaluation; 4) risk control; and (5) risk monitoring, along with explanatory requirements [105]. In this context the cloud security risk management and particularly cloud security risk assessment is necessary for all enterprises embracing cloud computing, regardless of their size because it reduces risks in any areas within a cloud computing and at the same time offers many benefits thus closing the doors open to cyber-crime. The reason is quite straight forward. 'A cloud security assessment teases apart, any areas within a cloud computing model that increase risk. In doing so, it also improves the visibility of the data life \cycle. In an era where cyber-crime is now

commonplace, having an analytical approach to security is vital. Cyber-threats are complex and multi-faceted. We need to use a cloud security assessment to counterbalance these gross threats' [267]. The ecosystem of the ICTs is becoming very dynamic and diverse with the incorporation of newly connected technologies in the system and thus in this dynamic environment no single domain strategy to evaluate and manage risks suffices. What is required is rather a holistic, more integrated risk models for managing and assessing multiple domains of risks that are emerging in the concerned technological environment. [224]. The same is true of Cloud computing domains of threats, vulnerabilities and especially risks. While research literature on risk management is growing [268] [40] [258][264][269] [270] [271] [272][273], Akande and other provide below in Figure 25 a conceptual a conceptual model of management issues with cloud computing. Similarly, research work on risk assessment in cloud computing is also in progress when accurate risk estimation sand predictions have to be made involving large uncertainties. As Aven, while reviewing the current trends, goes on to say this: 'Today risk assessments are well established in situations with considerable data and clearly defined boundaries for their use. Statistical and probabilistic tools have been developed and provide useful decisions support for many types of applications. However, risk decisions are, to an increasing extent, about situations characterized by large uncertainties and emergence. Such situations call for different types of approaches and methods, and it is a main challenge for the risk field to develop suitable frameworks and tools for this purpose' [268]. Table 27 is taken from Alosaimi and M. Alnuem [40] who reviewed the advantages and disadvantages risk management frameworks of several cloud computing analysts such as Saripalli and Walters [274], Tanimoto et al.[275], Fito et al. [276], Zhang et al.[277], Almosrsy et al. [278], Xie et al.[279], and Albakri et al. [280]. The Table 27 can be read with the following Table 28, provided by Akinrolabu and others

SUMMARY OF PRACTICES OF RISK ANALYSIS IN FRAMEWORKS				
Standard	**Concept of risk**	**Assessment method**	**Link to business risk**	**Risk management effectiveness measure**
Control Objectives for Information and related Technology (COBIT)	**1. "risk is the combination of the probability of an event and its consequence" 2. business risk is "a probable situation with uncertain frequency and magnitude of loss (or gain)" 3. IT risk is "a business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise"**	**heat map; scale for risk (low, medium, high, very high), scale for frequency (0 to 5), scale for impact (0 to 5)**	**Yes**	**maturity levels**
IT Infrastructure Library (ITIL)	**1. "risk is a possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred" 2. "risk can also be defined as uncertainty of outcome, and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes"**	**refers to other frameworks: MANAGEMENT OF RISK (M o R), ISO 31000, ISO/IEC 27000, RISK IT**	**Yes**	**refers to other frameworks: MANAGEMENT OF RISK (M o R), ISO 31000, ISO/IEC 27000, RISK IT**
Project Management Body of Knowledge(PMBOK)	**"project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost, and quality"**	**qualitative risk analysis, quantitative risk analysis**	**Yes**	**1. audit of risk methodology 2. lessons learned**
ISO 27005:2011 31000:2009	**1. risk is "an effect of uncertainty on objectives" 2. risk is "a combination of the probability of an event ... and its consequence" 3. information security risk is "potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization"**	**qualitative risk analysis, quantitative risk analysis**	**Yes**	**audit of risk methodology**

Table 26: Summary of Practices of Risk Analysis In Frameworks

in 2019. They conceptualized and proposed their own risk assessment model (CSCCRA) and compared it with these three other established approaches, while noting different aspects of each of the models [274] [280] [281].They argue that this comparison highlights each models' 'goal, risk assessment steps, decisions, the scope of assessment, and risk conceptualization, while also suggesting their applicability and reproducibility' along with a comparison of the respective model's 'strengths, weaknesses, applicability, and reproducibility' [282]. This review can further added to the work done by Mannane and others (2018), shown in Table 29, who also reviewed the risk assessment models framed by Albakri et al.[280] , Djemame et al.[281], Sendi et al. [283] ,Drissi et al. [286],Cayirci et al.,[284] [285], Mellon [287], and Mehari [288] in their own research[289]. What are the risk categories along with their sub-categories from both cloud providers and customer's perspectives in so far as the focus is on risk assessment? From their review of the selected literature Latif and others [290] point out the main risks shown in the next Figure 26. These risks are concerns of both the cloud provider and the cloud customer. Razaque and others, while pleading for their enhanced risk minimization in the cloud environment, argue that the advantage of their framework basically consists in both the cloud provider and cloud consumer becoming 'good partners of mutual trust based on the third-party auditor's review'[215]. The current approached do not meet 'all the specifics of the cloud' [289]. Relevant in this respect is the fact that cloud computing risks have now come into view as 'emerging risks' whose we potential for harm or loss is not yet fully known and they are therefore an area of significant concern. According to *RSA Digital Survey* (2020), the opinion of 1,050 qualified respondents were analyzed on the digital profile of risks. What is important in the context of this paper is that 2020 Report draws attention to the digital transformations by cloud computing. It notes that "Cloud initiatives, namely moving a significant number of workloads to the cloud, were cited as the most common type of digital transformation efforts. As organizations embrace more cloud

Figure 24: Taxonomy of organizational cyber-harms

architectures, public, private and hybrid, the ramifications ripple across the risk and security landscape. Visibility into these environments can become problematic as well as the challenge of the shift of operational management and responsibility'[291].In the latest Emerging Risks Report and Monitor of Gartner, the majority of risk executives cautioned these indicators: '(1) Rising proportion of data stored in the cloud; (2) Changes in product offerings or contract terms from cloud provider(s); (3) Growing percentage of non-cloud provider third parties with access to data in the cloud; and (4) Unauthorized employee usage of cloud services' [292]. The novel technologies which embed the emerging risks have been defined by Rotolo and others as a complex

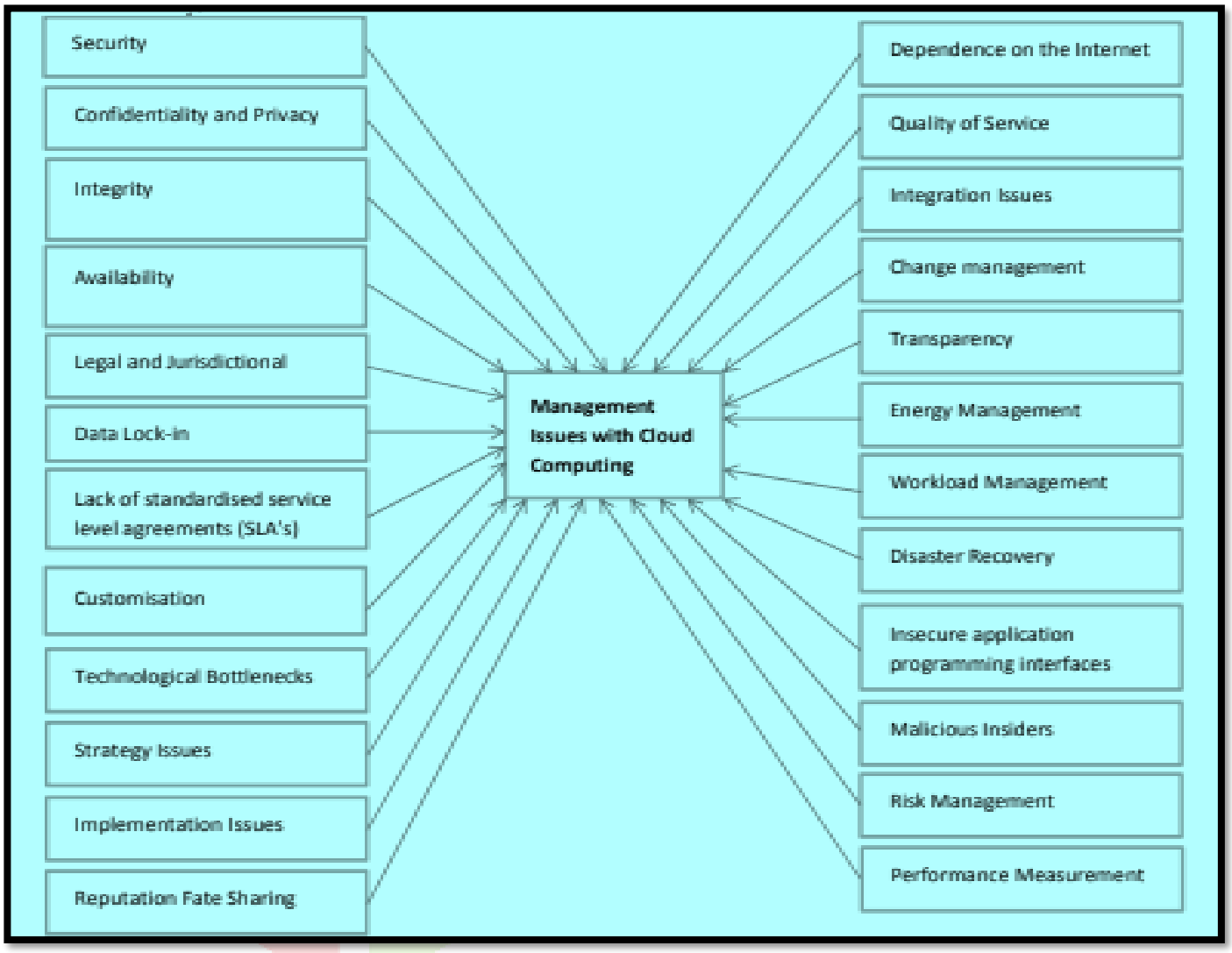


Figure25: Conceptual Model of Management Issues with Cloud Computing

of five attributes such as (i) radical novelty,(ii) relatively fast growth, (iii) coherence, (iv) prominent impact, and (v) uncertainty and ambiguity. They thus define emerging risks as '*a radically novel and relatively fast growing technology characterised by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domain(s) which is observed in terms of the composition of actors, institutions and patterns of interactions among those, along with the associated knowledge production processes. Its most prominent impact, however, lies in the future and so in the emergence phase is still somewhat uncertain and ambiguous*' [293]. Indeed, uncertainty is stated to be the 'main characteristic of emerging risk' that does exist in Cloud computing [294]. In any case, despite availability of multiple approaches to risk assessment in Cloud computing to address cloud risks, the efficacy of such approaches nevertheless remain limited. The is complicated because risk assessment practices are failing to keep pace with different risks particularly in the context of 'the dynamic and rapidly advancing nature of the cloud' and hence requires 'a more dynamic and inclusive approach to cloud risk assessment' [282]. This only reminds Beck's assessment, *inter alia*, of the role modern industrial technology in the risk society since 'most risks cannot be completely eliminated' [295]

V. IV: CLOUD UNCERTAINTY, GOVERNANCE,CULTURE AND HUMAN FACTORS

Cyber security including cloud security is fast becoming a distinct domain of associated emerging risks including cyber terrorism, hacker attacks, and cybercrimes. The attacks (viz. Denial of service (DOS) and distributed denial of service (DDoS), Spoofing, Sniffing, Man-in-the-middle (MITM), Cross-site scripting (XSS) and cross-site request forgery (CSRF), etc) in the realm of cloud computing are a familiar example of emerging risks. The reason is that in a fast changing era of technological innovations 'new capabilities and techniques are constantly being developed by very sophisticated and well-funded hackers that include insiders, organized crime, and others'. Emerging risks exhibit usually a high level of uncertainty, making it difficult to assess its

frequency and potential impact and hence to mitigate them. 'It is difficult to assess an emerging risk because it may be something that has never happened before or rarely occurs. A small, seemingly low risk could be a cascading failure where a small risk or event creates other problems until there is a major crisis [25]. As contemporary cloud analysts show, if risks are ridden with.

CLOUD COMPUTING: RISK MANAGEMENT FRAMEWORKS PROS AND CONS

Papers	Advantages	Disadvantages
P. Saripalli and B. Walters (2010)	1. The approach is fully iterative convergence and enables a comparative assessment of the relative robustness of different cloud vendor offerings in a defensible manner 2. It proposes three additional specific security objectives for a cloud environment to be appropriate for a cloud security risk assessment	1. It requires the careful and precise collection of input data for a probability calculation of threat events, which needs to be used to assess cloud computing risks. 2. It only focuses on risk assessment, which is only one step in the risk management process. The remaining steps are still required. 3. A quantitative risk assessment method has been used; thus, the results may be confusing and even imprecise. In addition, the method is expensive and requires solid experience with advanced tools.
S.Tanimoto, et al. (2011)	1. This approach analyses and ascertains the risk factors of cloud computing and gives detailed countermeasures. 2. It uses a combination of quantitative and qualitative methods for risk analysis and achieved the advantages of both. It has avoided bias and inaccuracy in the assessment results.	1. It lacks a risk identification process for the threats, vulnerabilities, and assets of a cloud computing environment. 2. The risk factors were ascertained only from the consumers' viewpoints and the approach overlooked that the cloud provider is the manager and owner of the cloud infrastructure.
J. Fito et al. (2010)	1. This approach evaluates the impact of cloud risks on the BLOs of a cloud organization, instead of considering the impacts on the whole cloud environment. It therefore has strong focus and precision. 2. It uses a combination of quantitative and qualitative methods for risk analysis and achieves the advantages of both. It has avoided bias and inaccuracy in the assessment results.	1. There is no explanation for the risk identification method, which is an important and critical process in the risk assessment of cloud environment. 2. The impact of risks has been evaluated based only on the BLOs of a cloud provider and has overlooked consumers' objectives and the fact that the cloud consumer is the real owner of the data assets.
X. Zhang et al. (2010)	The risk management was based on selecting critical areas in a cloud computing environment, which makes the risk assessment process strongly focused.	1. The risk management was semi-static because the list of critical areas was fixed. This may make the risk assessment of the cloud environment inflexible and some of the risks may be ignored. 2. A qualitative risk assessment method was followed. This makes the costs and benefits analysis during the selection of recommended controls difficult. 3. The risk management has focused only on the cloud provider and has overlooked that the cloud consumer is the real owner of the data assets.
M. Almorsy et al. (2011)	1. This approach tackles the loss of trust and security control problems by enabling cloud consumers to extend their SMP to include cloud hosted assets. 2. It mitigates the loss of control for cloud providers in terms of the hosted services developed by other parties. 3. The security management framework was undertaken separately for each of the provided services. This is where the problem of multi-tenancy lies.	1. Cloud consumers were involved in every step of the risk assessment processes. This complicates the risk assessment processes, particularly when the number of consumers increases. 2. A qualitative risk assessment method was followed. This makes the costs and benefits analysis during the selection of recommended controls difficult.
F. Xie et al. (2012)	1. This approach analyses the security status of cloud service providers by reviewing historical incidents. 2. It introduces third party assessment agency to ensure the effectiveness and safety of cloud computing applications.	1. Consumer involvement was not really considered to be active in the risk assessment process, which is only able to decide the security level in general and to select a cloud computing service and deployment model. 2. Consumers are only involved in determining the appropriate cloud providers based on their requirements. 3. A qualitative risk assessment method was followed. This makes the costs and benefits analysis during the selection of recommended controls difficult. 4. There is a lack of risk treatment or acceptance in terms of the appropriate action to be taken for each risk.
Albakri, et al.(2014)	1. This approach activates the involvement of consumers in the risk management process. 2. It tries to balance between the benefits of the participation of consumers and the complexity caused thereby.	1. The involvement of consumers involves notifying them at each phase that their participation is needed and completion of their responses must be awaited. Thiscould disrupt or delay the process. 2. The cloud computing consumer does not participate in risk treatment and acceptance. It is the consumer who experiences the risks to its own assets and, therefore, they should make the decision. 3. A qualitative risk assessment method has been followed. This makes the costs and benefits analysis during the selection of recommended controls difficult.

Table 27: Risk Management Frameworks Advantages and Disadvantages.

uncertainty, Cloud computing is no exception.

Having defined uncertainty as 'the difference between the available knowledge and the complete knowledge', and considering several types of uncertainties, Tchernykh and others investigate into the role of uncertainty in cloud computing service and

resource provisioning. They consider two types of uncertainties: parameter uncertainties that 'arise from the incomplete knowledge and variation of the parameters, for example, when data are inaccurate or not fully representative of the phenomenon of interest', and system uncertainties that 'arise from an incomplete understanding of the processes that control service provisioning, for example, when the conceptual model of the system used for service provisioning does not include all the relevant processes or relationships'. In the following Figure 27 they depict the sources of uncertainties in the efficient service provisioning. An example may be cited: 'In most existing solutions, it is assumed that behavior of VMs and services is predictable and stable in performance. On actual cloud infrastructures, these assumptions do not hold. While most providers guarantee a certain processor speed, memory capacity, and local storage for each provisioned VM, the actual performance is subject to the underlying physical hardware as well as the usage of shared resources by other VMs assigned to the same host machine. It is also true for communication infrastructure, where 'actual bandwidth is very dynamic and difficult to guarantee' [296]. There are other cloud analysts who have discusses the role of uncertainty, which in fact imping upon the advantages offered by Cloud computing. For instance, Trenz and others find sources of uncertainty due to several factors including the target environment (e.g., cloud federation, multi-cloud, mobile cloud, etc.), the service delivery model (e.g., SaaS, PaaS, IaaS, mashup, mobile applications), the

Systematic Evaluation of Cloud Risk Assessment Models					
Criterion / Models	Goal	Risk Assessment steps	Decisions supported by the model	The scope of risk assessment	Risk Conceptualisation
Quantitative risk and impact assessment framework (QUIRC) Saripalli and Walters (2010) [1]	Assessing cloud risks based on security objectives	The RA process is split into two phases: impact assessment using wide-band Delphi method, & probability assessment based on security reports	The model supports business-driven assessment of the security of cloud services	The CSP conducts the assessment with help from experts. The model is applicable to other IT systems beyond the cloud	Risk (score) = Impact * Probability
Cloud service provider risk assessment manager (CSPRAM) Albakri et al. (2014) [2]	Assessing the risk of cloud services, with inputs from cloud consumers (CC)	The model follows the steps defined in the ISO/IEC 27005 standard and is split into two aspects: CSP and CC	Supports the implementation of appropriate security controls based on changing customer requirements	The scope is reliant on the CSP and how much they choose to include customers in the assessment. The model also includes elements of risk management processes	Risk (score) = Impact* Likelihood
Service Provider Risk Assessment Tool (SPRAT) Djemame et al. (2011) [3]	To enable cloud providers analyse and address risk factors in a cloud ecosystem	The RA process follows a use-case scenario in determining the assets and actors required to conduct the assessment. It addresses two cloud stakeholder risks: SP & IP	The model supports the assessment of risks involved with the outsourcing of a cloud service to an external provider	The assessment involves both service provider and infrastructure provider. The model extends beyond RA to include risk mitigation and monitoring steps	Risk (score) = Impact* Likelihood
Cyber Supply Chain Cloud Risk Assessment (CSCCRA) Akinrolabu et al. (2019) [4]	To enable CSPs identify, analyse, and evaluate cloud risks from a dynamic supply chain perspective	The model builds on existing RA standards and involves the mapping of a cloud supply chain, supplier assessment, before the risk analysis phase	The presentation of cloud risks in dollar value promotes cost-effective risk mitigation and optimal risk prioritisation	The CSP conducts the assessment following the assessment of the security posture of their suppliers. The model is extensible to any composite IT service	Risk (cost) = Impact * Probability* Frequency

Table 28: Systematic evaluation of cloud risk assessment models

ADVANTAGES AND LIMITATIONS OF SELECTED RISK ASSESSMENT MODELS		
Paper	advantages	Limitations
S.H. Albakri et al. (2014)	Based on ISO 27005 Standard. Useful in Traditional Information System.	There is a lack of this approach implementation for risk analysis in cloud computing. This approach does not support cloud environment properties.
K. Djemame et al. (2016)	Based on an iterative and incremental approach. Use of a fuzzy multi-criteria decision making	This framework does not clarify roles of customers and CSP in this process and how It can be implemented in cloud environment.

	technique.	
A.S. Sendi et al. (2014)	This approach proposes a risk assessment model for selecting cloud service providers. Based on Cloud adoption risk assessment model (CARAM) framework and ENISA incident scenarios.	This approach of risk assessment for cloud computing is far from lights to be established after migrating to cloud service.
S. Drissi et al. (2014)	Depends on the accuracy of the input data and the appropriateness. Based on CARAM framework and ENISA incidents	The transition to cloud needs to define more details. There is a lack of implementation process in cloud environment.
E. Cayirci et al. (2016)	The framework can be used just to compare between cloud providers to select the best one basing on calculation of risk factor of each one by applying Analytic Hierarchy Process (AHP) model.	This approach does not give a model for implementation in cloud environment with no clarification about likelihood determination..
E, Cayirci et al. (2014)	This framework proposes a risk assessment lifecycle with the aims to respect internal threats to service execution based on analysis of historical and live data from the cloud infrastructure.	This framework does not clarify the implementation process and need to clarify the role of customers and CSP.
C.Mellon (1999) and Method Harmonized Risk Analysis (MEHARI) (2004)	Those standards and models (MEHARI ISO 27705) and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) can be used while migrating from traditional IT to cloud environment.	Cannot give a good result for risk assessment in cloud computing. Does not include the complexity and distributed character of cloud environment

Table 29: Selected Risk Assessment Models

service life-cycle phase (e.g., composition, deployment, selection, provisioning, etc.), the users profiles, etc. For them, uncertainty arises basically due to 'the lack of knowledge about cost, performance, reliability, privacy, security and availability levels of cloud services' and point to the new uncertainties in cloud that are there in addition to those which cloud has inherited from traditional IT. They mention several types of uncertainties in the cloud. But, more importantly, they argue that 'unlike non-cloud solutions in which resources are mostly manually provisioned with a fixed capacity and based on a prior knowledge on the available resources, cloud resources are *self-provisioned* in an *elastic* fashion. However, these two major characteristics of the cloud computing may become a part of the uncertainty problem. Uncertainty is also related to data storage and management in the cloud. For example, adopting non-effective data reduction strategies in cloud-based big data environments may affect the workload optimization and risks to increase the financial cost of data storage services.... Moreover, in case of big data, uncertainty sources on cloud in comparison to non-cloud systems are related to the data placement strategies and jobs performance, taking as example resource-intensive applications. In such context, network latency, file size and job failures are considered as uncertainty factors that may degrade performance... Besides the user and provider relationships, services and resources provisioning is also subject to uncertainty in the cloud environment. From the sources of uncertainty whose impact on the service provisioning is with an increased importance, we mention: fault tolerance, provisioning time, virtualization, elasticity, resource availability, scalability, etc.' [297]. In Table 30 they outline a number of the most discussed uncertainties and their impact on the basis of existing literature. Cloud computing thus does not come without a cost despite the advantages it offers to the individual consumers or business organizations. Risk carries with itself the fact of uncertainty in decision-making. Its nature has numerous diverse forms such as, as Goman (2019) points out recently, 'imprecise information about threats, competitors, unclear perspectives of a technology, absence of technological documentation, inaccurate estimations and underlying models, lack of internal control (acknowledged or not), immature organization structure, etc.'[264]

The generalized aspects of governance, along with risk culture, has already been analyzed in Section III of the present paper as ingredients of risk analysis. However, the present discourse remains incomplete unless they are discussed in relation to Cloud computing. While governance in general refers to the manner in which an organization ensures how it strategies will be set, monitored, and achieved [298], *Cloud governance* is 'a carefully designed set of rules and protocols put in place by businesses that operate in a cloud environment to enhance data security, manage risks, and keep things running smoothly... Cloud governance ensures that everything from asset deployment to systems interactions to data security is properly considered, examined, and managed. The shift from on-premise IT infrastructures to a cloud environment adds layers of complexity to ... system architecture. It also means that more people across your organization have the potential to impact that architecture'[299]. Price looks at, cloud

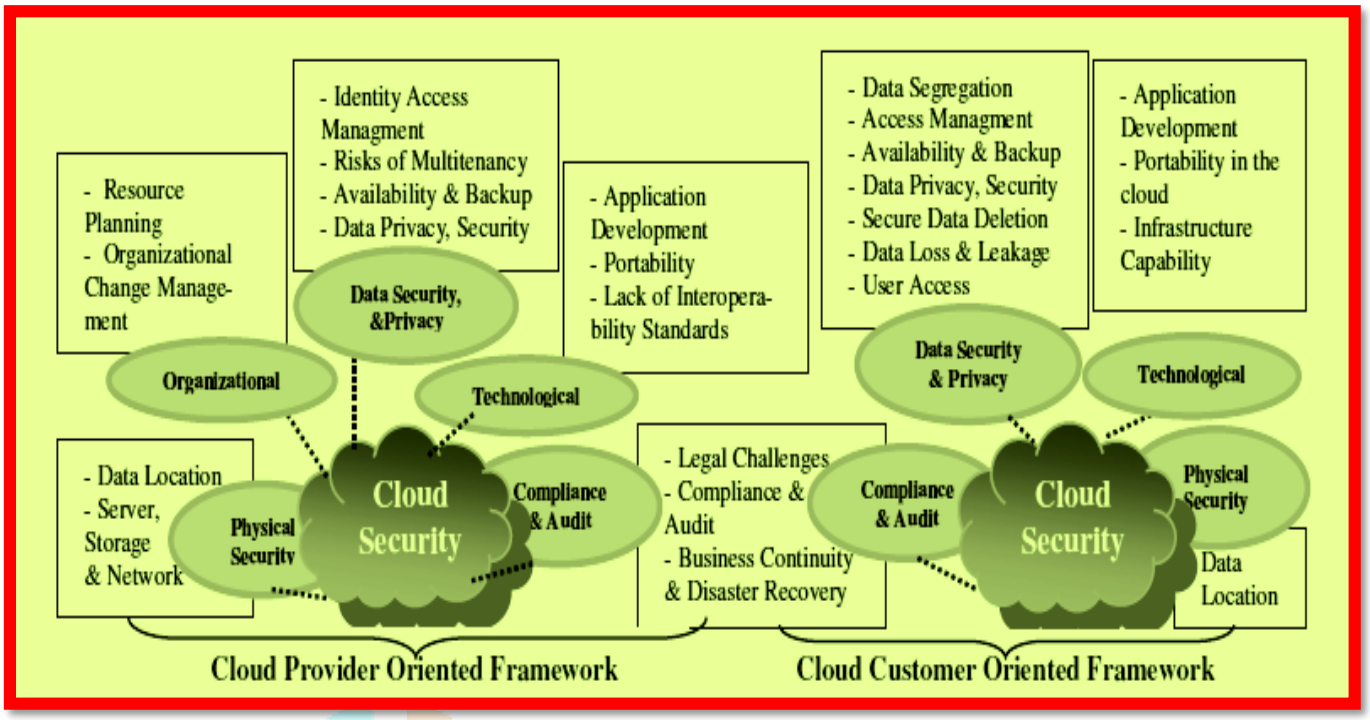


Figure. 26: Cloud Security Risk Categories and Sub-Categories

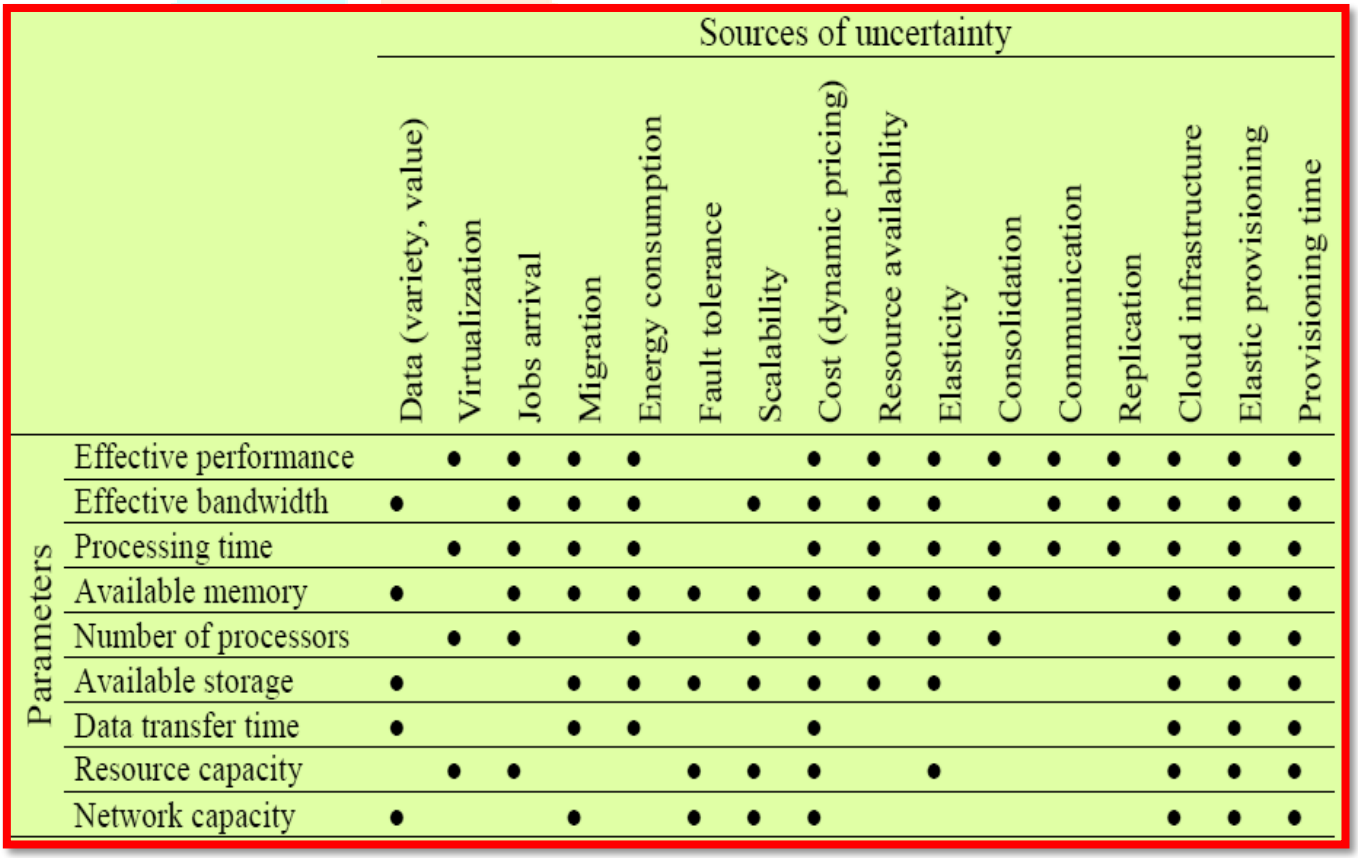


Figure 27: Cloud computing parameters and main sources of their uncertainty

governance in another way, referring to the development and implementation of 'controls to manage access, budget, and compliance' across the workloads in the cloud platform [300].Cloud governance is distinct concept which should not be confused with its other kindred terms such as corporate governance, Information governance, IT governance, and Cloud computing governance. The relation among them is clarified by Al-Ruithe et al. in the following Figure 28. While information governance, according to Gartner, is 'the specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information, cloud governance, according toMicrosoft cloud governance is conceptualized as 'defining policies around managing the factors: availability, security, privacy, location of cloud services and compliance and tracking for enforcing the policies at run time when the applications are running'[301]. More importantly, cloud data governance is the essence of cloud governance and Ruithe et al. visualizes the key dimensions of cloud data governance in Figure 29 [302]. The importance of (Cloud) data governance can simply be understood in terms of the volume and complexity of the growth of digital data. Data governance has taken on new dimensions in what is nowadays known as Big Data. It was projected that by 2020 the amount accumulated digital data would be around 44 zettabytes (or 44 trillion gigabytes)

and is likely grow to 180 trillion gigabytes by 2025 [303]. This explosion of data, mostly due to the expanding businesses, along with other factors (viz. governmental institutions etc.), is creating 'new demands that require different ways to combine, manipulate, store, and present information' and hence the importance [301]. Data governance enables implementation of data

Sources and impact of uncertainty on cloud computing				
Nos.	**Cloud computing operations**	**Source of uncertainty**	**Uncertainty parameters**	**Impact of uncertainty**
1	**data/service interoperability and integration**	**data variety, data value, data semantics, data provenance**	**data representation, data metering, communication protocols**	**data quality**
2	**service selection and recommendation**	**user preferences, users ratings, QoS levels**	**users profiles, QoS dimensions and metrics, preference weighting**	**QoS level, recommendation accuracy**
3	**service integration and composition**	**service descriptions, data provenance, security and privacy policies**	**providers policies, execution context, security level**	**infeasible composition, service failure**
4	**service placement and management**	**Resources availability, deployment cost, hosting zones infrastructure, security and privacy policies, replication, consolidation**	**memory, storage capacity, bandwidth, connectivity, processing time, data transfer time, Security breaches**	**resource usage, SLA violation**
5	**resource provisioning and orchestration**	**Virtualization, resources availability, Elasticity, replication, provisioning time, dynamic pricing**	**memory, storage capacity, performance**	**cost, resource consumption**
6	**Scheduling**	**tasks arrivals, tasks execution times, workload**	**workload and performance changes, processing time**	**tasks termination, resource consumption**
7	**Data management and analytics**	**data representation, volume, variety**	**patterns, frequency**	**inaccurate decision-making, inappropriate data visualization**

Table 30: Sources and impact of uncertainty on cloud computing

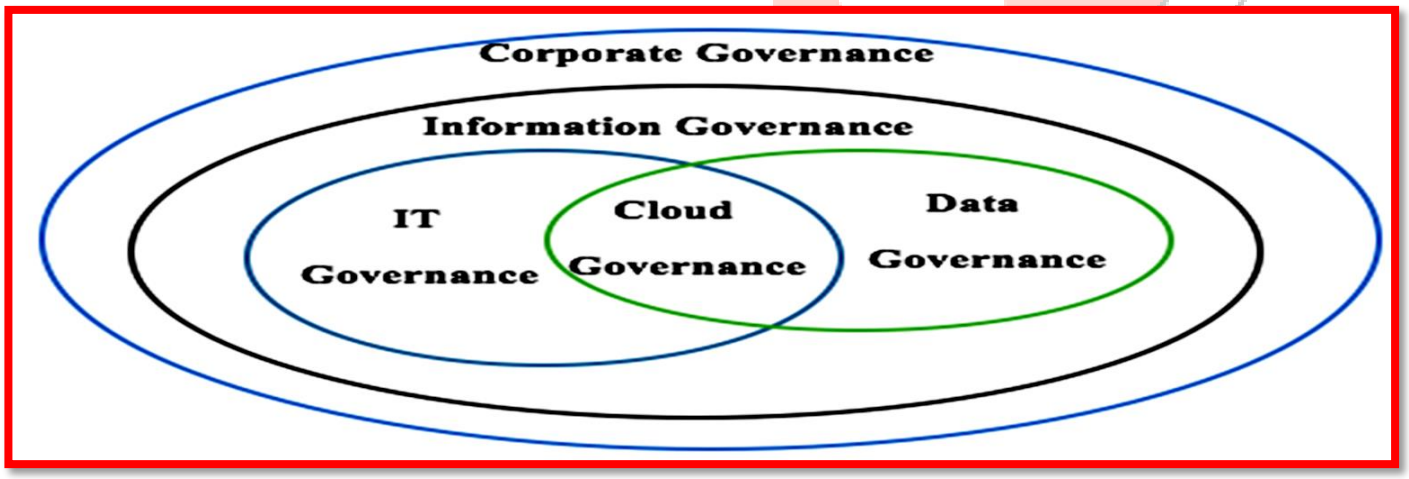


Figure 28: The interrelations between governance domains

agenda of the business corporations, maximizes the value of data assets in the organizations and helps to manage data-related risks [304]. Cloud computing, being an innovative and disruptive technology, which generates not only advantages but also risks, as has been stated earlier, requires cloud ***risk governance*** for managing of cloud risks view such risks as related to loss of control of data, security and privacy of data, data quality and assurance, data stewardship, data lock-in and so on [301]. Ladley (2020) has thus enunciated, as in Figure 30 the general principles concerning especially business data and information, which directly or indirectly bear on risk management. That is why he argues that 'besides privacy breaches, errors, reputation, we have entered an age where organizations need to be aware of enormous ramifications of mistreating data' [305].More specifically further, Ruithe has provided in Table 31 the leading differences between traditional IT and particularly Cloud computing along six commonly defined dimensions in the light of governance [298].

Figure 29: Key dimensions for cloud Data governance

In Section III the concept of ***culture and risk culture*** and the relevance in risk assessment has already been amply discussed. The role of human factors and culture has been an ingredient of ISO 31000: 2018, as mentioned in Figure 11 cited in the same section. They are valuable in themselves in of risk assessment, they can be also adopted and indeed also in cloud computing risk assessment process for purposes of prevention and mitigation of risks in Cloud computing. While advocating the need for a risk management approach that balances economic value against risks in order to protect information in the Cloud, Kaplan et al. urges the IT professionals to include the component of risk culture for updating risk management approach. Risk culture should considered in terms of 'clear metrics and targeted interventions that foster a strong risk-management mind-set' [308]. Alassaffi and others look into the governance, risks and vulnerabilities in moving to the cloud in the context of security issues in organization. While discussing different security risks and their mitigation, the mention that information security governance (ISG), a subset of corporate governance (CG) is one of the important success factors for an organization in adopting and using the cloud effectively. They do not specifically speak of developing a coherent information security (IS) risk culture or the role of human factors as conducive elements to ensure cloud security from cloud risks. Rather they argue that organizations need to have a proactive strategic management leadership 'in order to ensure that the activities of information security are supported and understood at all organizational levels, and aligned with organizational objectives. In addition to that, when staff members see the management concern and attention to security, they understand the necessity and importance of security, therefore, its benefit the creation of security culture'. Further, 'adopting ISG framework is an important action in assisting organizations with integrating ISG into their CG practices, securing information, improving the efficiency of organizational processes, complying with regulations, and cultivating an acceptable IS culture'[307]. Further, Lim and others show how the relationship between organization culture (OC) –'a set of shared values, beliefs, assumptions and practices that shape and direct members' attitude and behaviour in the organizations'- and information security culture (ISC) - - 'the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds'-- can generate varying degrees of risk. Risk vulnerability is low when ISC is embedded into the OC and where ISC is separated from OC, risk vulnerability becomes high. The Table 32 captures the scenarios of low, medium, and high risk vulnerability in the different relationships between OC and ISC [309]. *Sultan and de Bunt-Kokhuis, while analyzing the disruptive role of innovation on cloud computing and creation of new opportunities, argues that cultures is a double-edged sword in the context of security risks (viz.* loss of control, vendor lock-in, security, privacy and reliability etc in view of scale, complexity and novelty), argue that 'organizations develop their own cultural identity as they grow. This cultural identity of organizations is their own way of conducting their business, epitomized in the values exhibited by their employees when they decide which orders are more important, what type of customers should have priority, and whether an idea of a product is attractive. As well as defining what an organization can do, it also defines what an organization cannot do. Culture is therefore a double-edged sword. When great changes such as disruptive innovation occur, cases studies have shown that organizational culture generates cultural inertia, which is so difficult to overcome directly. It is often a key reason why

GAIP™ - Generally Accepted Information Principles	
Principle	**Description**
Content as Asset	Data and content of all types are assets with all the characteristics of any other asset. Therefore, they should be managed, secured, and accounted for as other material or financial assets.
Real Value	There is value in all data and content, based on their contribution to an organization's business/operational objectives, their intrinsic marketability, and/or their contribution to the organization's Goodwill (balance sheet) valuation.
Going Concern	Data and content are not viewed as temporary means to achieve results (or merely as a business by-product), but are critical to successful, ongoing business operations and management.
Risk	There is risk associated with data and content. This risk must be formally recognized, either as a liability or through incurring costs to manage and reduce the inherent risk.
Due Diligence	If a risk is known, it must be reported. If a risk is possible, it must be confirmed.
Quality	The relevance, meaning, accuracy, and life cycle of data and content can affect the financial status of an organization.
Audit	The accuracy of data and content is subject to periodic audit by an independent body.
Account-ability	An organization must identify parties which are ultimately responsible for data and content assets.
Liability	The risks in information means there is a financial liability inherent in all data or content that is based on regulatory and ethical misuse or mismanagement.

Figure 30: Generally Accepted Information Principles of Data Governance

managers fail to introduce timely and substantial change, even when they know that it is needed'. They also state that 'consumers of cloud computing should also be prepared to implement cultural changes in the way they view their IT resources and infrastructures' [310]. Glaspie and Karwowski forcefully contend that technology by itself, regardless of any amount invest, cannot eliminate many security challenges. Glaspie and Karwowski, in their review of 50 pertinent publications in concerned literature, advocate promoting 'a positive information security culture within the organization' for reasons of increasing security policy compliance, strengthening the overall information security posture, and reducing the financial loss due to security breaches for combating human errors like negligence, accident, or deliberate action. Humans beings are the weakest links in the information security culture (ISC), or in the cyber security culture (CSC) or, if it can be added, in the cloud security culture [311]. Corradini and Nardelli carried out a two-stage survey of risk perception of 815 employers working in a multinational company in the financial sector. They assert that in ensure in an effective security approach to cybersecurity one cannot 'neglect the role of human beings. It is fundamental to build a strong cyber security culture in every organization so that employees in their daily life are constantly aware of the possible outcomes of their actions and perform accordingly'. In this they took note of the the concept of risk culture as 'the values, beliefs, knowledge and understanding about risk, shared by a group of people with a common intended purpose, in particular the leadership and employees of an organization' and the construction of a cyber security culture can only start with 'an investigation of the organization culture and of employees' risks knowledge' [312]. In the final instance it is the human factor that counts. It is also they, being fallible and prone of committing mistakes, who stand to lose instead of being beneficiaries when the systems fail to ensure security from the risks involved. 'One of the roles of security engineers is to recognize this fallibility and to be up front about what can and cannot be done with respect to countering threats that limits the damage of such fallibility. In doing this it is essential to also recognize that humans are adaptable and resourceful in both designing systems and correcting them when they go wrong. These characteristics mean that humans can be both the strongest and the weakest link in system security. It also means that there is an incentive to manage the human element in systems such that those systems work well (functionality matches the requirement), efficiently (don't overuse resources), safely and securely. Thus human centric design, even for mostly machine based systems, is essential [263].

Dimensions	Traditional IT	Cloud Computing
Data governance function	**All data governance policies are handled in-house.**	**Data policies are put in place, however, it is up to the third party to ensure that guidelines are followed.**

Data governance structure	**The infrastructure is on-site, and all aspects of data governance are left to the local administrators.**	**The infrastructure is multi-site, hence new entities become involved in data governance structure, such as the Cloud manager, Cloud provider and Cloud broker.**
Organisational	**1. No extra cost. 2. Internal training. 3 .Local employees involved in data governance structure.**	**1. Extra cost and training. 2. Change management. 3. New skills and experience are required 4. New roles and responsibilities are required. 5. External members involved in data governance structure.**
Technical	**1. The infrastructure is set-up and maintained by local administrators in IT department. 2. Runs programs and services on servers by local administrators. 3. Data governance policies implemented by local administrators. 4. No loss of control and governance. 5. Local administrators have responsibilities to protect data.**	**1.The infrastructure is set up and maintained by a third party. 2. Runs programs and services on servers by a third party. 3. Data governance policies implemented by a third party. 4. Loss control and governance. 5. A third party has responsibilities to protect data.**
Environmental	**No Cloud regulation.**	**Cloud regulation alignment will be considered in data governance policies.**
Measuring and monitoring tool.	**Data governance policies are controlled and monitored by local management inhouse.**	**1. Checking the data governance policies of a cloud provider's data centers. 2. A third party should have a document that shows what measures they will take to examine data governance policies. 3. A third party reports data governance situation to Cloud consumer.**

Table 31: Differences between the Traditional IT and Cloud Paradigm Along Six Common Dimensions

VI: CONCLUDING REMARKS

At this point it needs to be reminded that the role of science and technology in generating risk society cannot be absolutized or treated in isolation, for 'the calculus of risk connects the physical, the engineering and the social sciences' embodying intricate interlinkages among them. The reason is that it can be applied to 'completely disparate phenomena', not only health risks but also to a host of other risks such as economic risks, risks of unemployment, risks of old age and so on [142]. The reigning scientization or technological 'fatalism' can only be overcome, so argues Beck, by 'more democracy – the production of accountability, redistribution of the burdens of proof, division of powers between the producers and evaluators of hazards, public disputes on technological alternatives. This in turn requires different organizational forms for science and business, science and public sphere, science and politics, technology and law, and so forth'[142]. Whether it is dangers, hazards or risks, they are unintended consequences of ongoing modernization in the late industrial society. Beck was no 'pessimist' [184]. Those unintended consequences are not something 'external' to the society and, accordingly, critique and resistance to the contemporary science and technology and their practitioners can only' improve everyone's chances of survival' [145]. The failure of techno-scientific rationality accompanied by the growing threats and risks in the society does not mean the failure of the scientists, technologists or their disciplines but, in the last instance, is grounded 'in the institutional and methodological approach of the sciences to risks' [144]. This can happen when the disciplines undertakes self-criticism: 'Only when medicine opposes medicine, nuclear physics opposes nuclear physics, human genetics opposes human genetics or information technology opposes information technology can the future that is being brewed up in the test-tube become intelligible and evaluable for the outside world. Enabling self-criticism in all its forms is not some sort of danger, but probably the *only way* that the mistakes that would sooner or later destroy our world can be detected in advance'[144].

There is more to Beck's optimism and this relates to efforts and strategies for action and remediation which go a long way to challenge the neo-liberal capital-state coalition and its power and bring about new empowerments in the emergent cosmopolitan society. Global risks 'empower states and civil society movements, because they reveal new sources of legitimation and options for action for these groups of actors; they disempower globalized capital on the other hand, because the consequences of investment decisions contribute to creating global risks, destabilizing markets and activating the power of that sleeping giant the

Relationship between Organizational Culture and Information Security Culture			
Nature of Relationship	**Organizational Culture (OC)**	**Employees Beliefs, Actions and Behaviours (ISC)**	**Probable Consequences**
Type 3 relationship: where ISC is embedded	**Management Involvement:** Management bring security matters and strategy into board meeting. Updates are made on a periodic basis to the company board of directors.	**Responsibility:** Always adhere to the security procedures and guides/ **Participation:** Employees undergo periodic security	**Risk Vulnerability: Low.** **Awareness:** Employees are highly aware and concern

into OC. **High**	**Locus of Responsibility:** Management involves every member of organizations. **Information Security Policy**: Created in holistic manners. In addition, there are regular updates on security policy. **Education/Training:** Management make the awareness program compulsory for all the employees. **Budget Practice:** Management allocates budget for security activities annually.	training, awareness programme. C**ommitment:** Employees feel responsible and ownership of information. **Motivation:** Motivated and committed towards security matters. **Awareness/Know how:** Knowhow and who to deal with when facing security problems.	about security matters in organization. **Responsibility:** Security is every employee's business. **Security Practices:** Holistic manners. Unconsciously become daily routine activities. **Investment for security practices:** High cost in implementing security activities.
Type 2 relationship: where ISC is a subculture of OC **Moderate**	**Management Involvement:** Management typically delegates understanding of information security matters to CIO. **Locus of Responsibility**: Management starts to empower security matters to head of dept. **Information Security Policy**: Created within IT department and may not have widespread support or knowledge of where they are located. **Education/Training:** Management starts to pay attention to awareness. People receive some training of information security. **Budget Practice:** Management acts promptly towards expenses pertaining security activities.	**Responsibility:** Adhere to security matters as a requirement of management **Participation:** Employees are involved insecurity matters in own dept. Less interdepartmental coordination. **Commitment: Responsible** and committed in security matters for own dept. **Motivation:** Employees are motivated in security matters in own dept. **Awareness/Know how:** Knowhow and who to deal with when facing security problems within dept.	**Risk Vulnerability: Medium.** **Awareness:** Employees are aware of security matters within their own dept. **Responsibility:** Employees are responsible for security matters within own dept. **Security Practices:** Security is employees 'routine activities within own dept. **Investment for security activities:** Medium cost in implementing security activities.
Type 1 relationship: where ISC is separated from OC **Low**	**Management Involvement:** Management intuitively knows that information security is important, but it assigns the same level of importance as ensuring that computer is up. **Locus of Responsibility:** Management assigns all the security responsibility to IT department. **Information Security Policy**: Created by copying without the means to enforce them. Usually issued by a memo. **Education/training** Low awareness. Management does not emphasize on security training. **Budget Practice:** Usually part of a budget for IT support.	**Responsibility:** Do not care and not responsible towards security matters. **Participation:** Employees are not involved in security matters. **Commitment:** Employees leave it to IT dept. Always bypass security procedures. **Motivation:** Employees are not motivated in dealing with security matters. **Awareness/Know how:** Do not know what to do when facing with security problems.	**Risk Vulnerability: High** **Awareness**: No awareness insecurity matters **Responsibility:** Only IT dept is responsible for security matters **Security Practices:** Not a routine activity of employees **Investment for security activities :**Low cost in implementing security activities

Table 32: Types of Relationships between ISC and OC

consumer. Conversely, the goal of global civil society and its actors is to achieve a connection between civil society and the state, that is, to bring about what I call a *cosmopolitan form of statehood'* [168].The burden of evidence in Beck's contributions points clearly that Beck was not a prophet of doom and dystopian in his overall writings on risk society and issues related to it. He was not a 'professional Cassandra'; his *weltanschauung* was rather 'optimistic, positive, and progressive'. He warned about the threats and harms of capitalist modernization, wanted to confront dangers of environmental and other societal problems inherent in them, andwas 'sanguine about the possibilities of public engagement and the opportunity to chart alternative political futures' [131]. Beck was quite confident that 'the uncertainty produced by industrial society does not result ineluctably in chaos or in catastrophe. Rather, incalculable uncertainty can also be acknowledged and become a source of creativity, the reason for permitting the unexpected and experimenting with the new' [159]. Table 5 and Figure 2 corroborate this. Anyway, in his last publication, *The Metamorphosis of the World* (2016), Beck argues that the risk society is the agent of the 'metamorphosis of the world' for one can hardly 'understand or deal with the world and one's own position in it without analysing risk society'. Here, Beck moves beyond world risk society to enunciate what is hidden in metamorphosis of the risk society and then point to the 'goods' immanent in emancipatory catastrophism. The risk society is undergoing a thoroughgoing but silent transformation or, more appropriately, 'transfiguration'. 'Metamorphosis implies a much more radical transformation in which the old certainties of modern society are falling away and something quite new is emerging' [201]. Take, for instance, the issue of climate change, among others (viz., the financial crisis, the transformative role of IVF treatment etc.). Global climate change risk is not plainly an issue of measuring carbon dioxide and the production of pollution only. It is more than this, creating 'new ways of being, looking, hearing and acting in the world' as an outcome of 'the dramatic power of the unintended, unseen emancipator side effects of global risk'. Global climate change may result in the 'rebirth of modernity' [160]. To explain in a little more detail in the word of Beck: 'Seen as a global risk to all civilization, climate change could be made into an antidote to war. It induces the necessity to overcome neoliberalism, to perceive and to practise new forms of transnational responsibility; it puts the problem of cosmopolitan justice on the agenda of international politics; it creates informal and formal cooperation patterns between countries and governments that otherwise ignore each other or even consider each other enemies. It makes economic and public actors accountable and responsible – even those who do not want to be accountable and responsible. It opens up new world markets, new innovation patterns, and the consequence is that deniers are losers. It changes lifestyles and consumption patterns; it reveals a strong source of future-oriented meanings, in everyday life and for legitimation of political action (reforms or even revolutions). Finally, it induces new forms of understanding and caring for nature. All of this happens under the surface of the mantra of disappointments and disillusionments at the *travelling circus* of one climate conference after the other. From this perspective, climate change

means first the metamorphosis of politics and society that has to be discovered and closely analyzed through the social science of methodological cosmopolitanism. This is not to say that there is an easy solution to climate change' [201].

Beck provides many other examples of the 'goods' that can be derived from the global risk society. For instance, global risks, crises and threats are a sort of motors of a growing awareness of globality, and generate risk communities which are based neither on descent nor spatial presence but which can also 'generate a kind of 'compulsory cosmopolitanism', a 'glue' for diversity and plurality in a world whose boundaries are as porous' in terms of communication and economics [132]. Global risks are 'capable of awakening the energies, the consensus, the legitimation necessary for creating a global community of fate, one that will demolish the walls of nation-state borders and egotisms—at least for a global moment in time and beyond democracy. ...Global risks tear down national boundaries and jumble together the native with the foreign. The distant other is becoming the inclusive other—not through mobility but through risk. The global other is here in our midst. Everyday life is becoming cosmopolitan: human beings must find the meaning of life in the exchange with others and no longer in the encounter with like. We are all trapped in a shared global space of threats-without exit' [159]. At the same time *digital communication* provides 'structural dynamic' that enables global risks to create novel forms of communities. Since global risks (e.g., climate change, financial risk, etc.), which can change society and politics, can only do so through the medium of public communication. 'It is only through mediated images that they acquire the power to break through this invisibility. Large-scale disasters are occurring everywhere, but they unfold their emancipatory potential only with the power of the public images that create a global public sphere, a categorically different kind of public than the one trapped in the national view. What we can observe is an interaction: global risks create globalized publics, and globalized publics make global risks visible and political'. In this regard, the empirical investigation of the role of a transnational networked public sphere of air pollution can be mentioned. Chen draws on digitaltrace data, government documents, and journalistic reports to integrates Beck's risk society theory with digital media theories for examining the mediated process of risk definition and assessment of PM2.5 (particulate matters with a diameter less than 2.5 micrometers) in 'a networked public sphere' and found out that, by using network and content analysis of a PM2.5 Twitter network, 'political and professional elite remained the most powerful producers of risk definition'[202]. In any case, communication is no longer nation state-oriented but operates beyond national boundary and becomes representative of the 'humanity as a whole' indicating a cosmopolitan turn. Furthermore, as Beck contends, data in the digital communication are 'reflexive data' which produce 'a kind of organized reflexivity'. 'What we have with digital communication are data which *constitute the reality* of cosmopolitization. They *produce* cosmopolitization; they do *not* simply *represent* it. They are socially and politically meaningful'. To instance, the internet is not only 'a space of action or a tool to organize, communicate and exchange' but it is 'a process of becoming a cosmopolitanized world' [201]. In addition, Beck extends the concept metamorphosis to the digital space and talks of digital metamorphosis as the non-intentional, often unseen side effects, which create metamorphosed subjects (i.e., *digital humans)* on the one hand, and can be understood, on the other, as 'the essential enmeshment of the online and the offline'. The digital realm offer a novel opportunity: 'The emancipatory side effect of global risk, which is produced here, is the expectation of *digital humanism, at the heart of which is the demand that the right of data protection and digital freedom is a global human right, which must prevail like any other human right'* [201].

How 'goods, can germinate and flourish shaping numerous spheres of society and economy from the health risk -- the global pandemic named Covid -19–appeared suddenly since Beck's death in 2015, has already been mentioned in the earlier section of this paper. Though previously 'unlown to science', this new risk has thrown the challenge of developing and adopting 'actionable and feasible emergency preparedness and resilience plans' to cope with the crisis [204]. The pandemic has brought forth new opportunities such as, for example, 'shifting digital transformation to a high-speed gear', as Soto-Acosta terms it. Digital transformation is not simply trying digital technologies to change something, say, in business; it rather involves something transformational, i.e., driving significant changes in the enterprises' business models: 'The COVID-19 context has accelerated the digital transformation of businesses and entire industries such as retail, restaurants, and education. For instance, although electronic learning had been there before the pandemic, the COVID-19 pandemic accelerated and extended the digital transformation of traditional education organizations at all levels as the only possible way to continue their activities during the lockdown, but also in the new normal. Results on how schools and colleges have digitally transformed their business during the lockdown have been pretty decent'[205]. If Civid-19 has brought forth new techno-socio-cultural opportunities, it has done so by profoundly affecting the technological domain, demanding a fresh look at its assessment of risk potentials and evaluation of the affected technological domain, demanding a fresh look at its assessment of risk potentials and evaluation of the affected technological domains as such. KPMG has designed a framework for rapid impact assessment that will enable tech risk professionals to continuously assess technology risk in view of the ever changing risk landscape as organizations address the fallout from the global impact of COVID-19. This is needed for five reasons such as: 1. identifying emerging technology risks, vulnerabilities, and threats related to COVID-19 before they materialize in reality; 2. changing security controls and posture in light of COVID-19; 3. assessing the impact that COVID-19 will have on compliance and regulatory obligations; 4. summarizing quickly the effects that COVID-19 may have had on the technology organization and strategy; and 5. introducing new technologies or unexpected changes to the environment as a result of COVID-19. Table 33 describes in tabular for Covid-19 generated risk scenarios that are affecting the technological domain which also includes, among other things, the Cloud platform as well [313].

It is not wide out of the mark to suggest that Beck's risk society thesis and Cloud computing thesis, though belonging to disparate disciplinary realms, resemble to each other on many counts, so much so that it can be suggested that, in the **first** place, Cloud computing technology is a subset of risk society or what risk society stands for from the scientific and technological standpoint. It is further suggested here that both are products of what Beck might call the reflexive modernization processes beginning approximately since the 1970s and 1980s. Take for instance, the timeline of the birth from Cloud technology. Following Sharma in this regard and without going back to the 1960s when J. C. R. Licklider's work on Arpanet is seen as predecessor to the internet and when IBM pioneers virtualization, virtual memory, and time sharing of computer hardware, the 1980swas marked the computer era of mainframes, minicomputers, and the appearance of personal computers. The following decade of the 1990s

witnessed 'the dawn and widespread use of the Internet', facilitating and preparing the ground in a way for the emergence of'Cloud computing'—a term 'first coined at INFORMS (Institute for Operations Research and the Management Sciences) meeting in Dallas by Professor R. K. Chellapa' in 1997. Subsequently in 2006 Amazon launches public cloud services, building on its web services and at the same time 'Storage (S3) and compute (EC2) cloud services' were launched [38].**Second**, if risk society is termed as risk society because of overwhelming presence and dominance of a variety of risks in the society, then Cloud computing is also a risky technology wherein certain risks are specific to this technology as essential features since no discussion or use of Cloud technology can be complete without its attendant threats, vulnerabilities, attacks, and risks. Both risk society and Cloud computing as subset of risk society are characterized by or embody in themselves varying degrees and amounts of what Beck call 'bads' [159], despite the advantages and benefits they respectively offer in the modern industrial society. For Beck 'risk has become the central way of constituting and organizing society' [132]. In both the importance of the 'bad' can hardly be gainsaid by any serious analyst. **Third,** the bads in Cloud computing are threats, vulnerabilities and risks, as they are well known and publicized. Beck too mentions threats and risks. Beck also mentions threats, risks, and manufactured uncertainty, which can be analytically differentiated, but which in reality 'intersect and comingle' [159]. But he also talks of social vulnerability in the societal contexts of risk society. While risks and vulnerabilities are opposite sides of the same coin, 'social vulnerability is a cumulative concept that includes the means and possibilities available to individuals, societies or whole populations to cope (or not) with the risks – the 'unknown unknowns' – and the (social) uncertainties that mark their lives' [132]. **Fourth,** security has remained an elusive concept in the risk society. Beck differentiates security that was available the in the first mode rn industrial society from the elusive security in the risk society. In the risk society 'the 'fear business' will profit from the general loss of nerve. The suspicious and suspect citizen must be grateful when he is scanned, photographed, searched and interrogated 'for his own safety'. Security is becoming a profitable public and private sector consumer good like water and electricity'. Further, 'what differentiates the old nation-state security agenda of the first modernity from the new postnational security agenda of the second modernity is thus the *regime of non-knowing*, even worse, not just of known, but above all of unknown non-knowing – of 'unknown unknowns' ... and hence the collapse of ontological security. This is lost when at least one factor in the classical security equation – agent, intention, potential – becomes an unknown. In the case of terrorist networks, all three factors become unknowns' [142]. Turning to Cloud Computing, the situation is no better. Stallings and Brown, while discussing security, aptly remark that 'computer security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness while the designer must find and eliminate all weaknesses to achieve perfect security' [314].Roberts goes on to say that 'There will always be some degree of mismatch between the countermeasures on offer and the risks identified in the particular environment of the system. A matrix of risks perceived in the system against risks addressed by the selected countermeasures will show where there is overlap (and, perhaps, overkill) and where there are gaps. The gaps left by the countermeasures are collectively known as residual risk. It is important to understand that in any system there is an element of residual risk which must be accepted by the organization. A little thought will show that the security of a system can never be 100%. There will always be some small risk that information will leak (if only via subverted staff) or be corrupted (if only through mistakes made by careless staff)' [315]. De Decker would agree: 'There is no system that is 100% safe, except one that is switched off and kept in a bunker. Many security measures make the system less user- friendly. If the users are not convinced of the usefulness of the measure, they will subvert it, one way or the other. Humans are often the weakest link. Through continuous education, the users are kept vigilant and aware of their responsibility towards the overall security' [316].

Fifth, both the risk society and Cloud computing technology are in way products of reflexive modernization, which is a transition 'away from a first modernity locked within the national state, and towards a second, open, *risk-filled modernity characterized by general insecurity'*[153].The concept of reflexive modernization does not mean mere reflection but above all self-confrontation – an historical phase in which the process of modernity examines and critiques side-effects, i.e. hazards, produced by industrial modernity itself in the risk epoch [147]. To elaborate it for this purpose in the words of Elliott: 'It is the autonomous, compulsive

COVID-19 Illustrative Risk Scenarios In The Technology Domain

Domains	Risk scenarios	Domains	Risk scenarios
Strategy and governance	**— Key employees with requisite knowledge are not available for mission-critical tasks/key projects** **— Technology budgets may decrease and impact the ability to deliver services and solutions in alignment with the technology strategy** **— Key decisions are made in a ungoverned manner that go against technology policy and standards**	**Programs and implementation**	**— Increased cost/inefficiency to the business by deferring or discontinuing a project** **— Increased noncompliance with project management standards and procedures (i.e., user acceptance testing, conversions, etc.)** **— Inability to deliver projects due to resource capacity and lost knowledge (i.e., furlough, competing priorities, delay of consulting engagements)**
Security and data privacy	**— Cyber security vulnerability and patch management not maintained** **— Increase in COVID-19-related phishing activity without increase in security awareness efforts** **— Increased use of bring your own device (BYOD) and remote connectivity introduces new security vulnerabilities** **— Data movement, transfer, and storage of sensitive data in a remote working environment increase likelihood of**	**Identity and access management**	**— Terminated or furloughed employees still have access to corporate systems and sensitive data is not removed timely** **— Increased risk of unauthorized access and segregation of duties conflicts due to additional access rights being provisioned as part of the COVID-19 response**

	compromising sensitive data		
Availability and business disruption	**— Business continuity planning (BCP), disaster recovery planning (DRP), and incident management plans not fit for purpose in remote work environment — Increase in single points of failure as a result of remote operations — Increased supply chain availability risks — Lack of organizational preparedness as the economy and impact evolve**	**Operations**	**— Operations teams are not scaled to handle the increased volume of service requests — Processes do not allow for a rapid response and ongoing management of remote access technologies and infrastructure technology to accommodate the evolving needs of the business — Critical technology resources are not identified/available to support operations, impacting effective response and business continuity**
Emerging technology	**— New collaboration tools or digital tools deployed rapidly without full assessment of security and controls — New mobile devices, cloud solutions, or automation deployed without full assessment**	**Compliance**	**— Changes in technology processes may result in noncompliance with regulatory (e.g., privacy, SOX) requirements — Changes to regulatory requirements not being monitored timely**
Infrastructure and asset management	**— Critical facilities are inaccessible — Increased remote network traffic without proper capacity and stress testing — Improper use of VPN technologies — Inability to respond to the increase of service desk issues**	**Third party management**	**— Third parties may become insolvent or inaccessible and unable to continue performing services, causing disruption to business operations — Key technology third parties are unable to scale or flex to accommodate the changes needed or meet the demands of the business — The pandemic response of third parties is not effective or controlled, creating unknown operational, regulatory, or security risk to the business**

Table 33: COVID-19 illustrative risk scenarios in the Technological domain

dynamic of advanced or reflexive modernization that, according to Beck, propels modern men and women into 'self-confrontation' with the consequences of risk that cannot adequately be addressed, measured, controlled or overcome, at least according to the standards of industrial society. Modernity's blindness to the risks and dangers produced by modernization - all of which happens automatically and unreflectingly, according to Beck - leads to societal self-confrontation: that is, the questioning of divisions between centres of political activity and the decision-making capacity of society itself' [317]. The same thing holds good for Cloud computing technology as well, for different analysts and researcher in this field are not only confronting security issues in Cloud computing but are also actively engaged in seeking mitigation, if not elimination of, threats, vulnerabilities, attacks and risks from Cloud computing resources and processes to make Cloud computing safe and secure for all concerned entities including the consumers. It is more so when 'enhancements in technologies such as cloud computing, IoT, Industrial Internet of Things (IIoT; i.e., for smart manufacturing, smart factories, etc.), and data lakes are providing a platform for such a modern supply chain vision' [38]. **Sixth**, as shown in the preceding analysis, risk is inextricably interlinked with uncertainty. 'Risk is uncertainty that surrounds actual events and outcomes that may (or may not) take place' [73]. Both Beck's risk society thesis and Cloud computing technology are marked by conspicuous uncertainty, i.e., 'information deficiency including deficiency types of incompleteness, imprecision, fragmentation, unreliability, vagueness, or contradiction' [318]. For Beck 'risk, by its inner logic, means uncertainty and accentuates uncertainty, and not only negatively in the shape of catastrophes (collapse of the global economy, etc.), but also positively: the experience of the everyday 'real world' is beyond the horizon of this risk model science'. In fact, as Beck argues 'the pressing issue' in world risk society is to anticipate and prevent self-inflicted catastrophes, in short, to deal with manufactured uncertainties' even though it will create 'large and growing markets for technologies, experts, counter-experts and products – world risk society is big business!' [132]. The fact of the matter is that in the risk society era 'security experts can no longer offer quantifiable certainty of threats' [319] but , in the conflict between producers of risk definitions and consumers of risks , they can engage in only 'definitional struggles over the scale, degrees and urgency' for ensuring security[144]. As far as uncertainty in Cloud computing is concerned, it has been shown in Figure 27 and Table 30 uncertainty is no less there and, indeed quite remarkably present there. Beyond what has been said before, let cite an instance of uncertainty. Gunawi and others analyzed, in an empirical study of 32 popular Internet services and 597 media reported unplanned outages occurring between 2009 to 2015, 'outage duration, root causes, impacts, and fix procedures'. They pointed to the uncertainty continuance of outage in the functioning of the Cloud computing services. The concluding remarks of their analysis are quite suggestive. 'A big challenge lies ahead: features and failures are racing with each other. As users are hungry for new advanced features, services are developed in a much rapid pace compared to the past. As a ramification, the complexity of cloud hardware and software ecosystem has outpaced existing testing, debugging, and verification tools' [320].

Seventh, both risk society thesis of societal elf-endangerment with risks and risks concomitant with Cloud computing are linked to, limited by and born with the crucible of capitalism – the ideological framework for the rise of (reflexive) modernization. As Beck puts it, **'**the diffusion and commercialization of risks do not break with the logic of capitalist development completely, but instead they raise the latter to a new stage. There are always losers but also winners in risk definitions. The space between them varies in relation to different issues and power differentials. Modernization risks from the winners' points of view are *big business*' [144]. If it is suddenly revealed, whether by media or otherwise, that certain products contain 'poison', capitalist logic is then set in motion, i.e., the 'causal autonomy of industrial capitalism' foretells not progress but 'ecological self-jeopardization of all life on earth'. Put otherwise, the 'whole markets collapse, and capital investment and production are devalued at a stroke. This 'ecological expropriation' thus constitutes a historically unprecedented devaluation of capital and productivity under constant property relations, usually without any change for the consumer in the appearance or utility of the goods' [145]. In the wake of the eclipse of controllability, certainty and security in the risk society of second modernity, a new kind of capitalism has appeared, along with ' a new kind of economy, a new kind of global order, a new kind of society, and a new kind of personal life'[142]. It is reflexive modernization that is producing not only 'a new kind of capitalism' but also concomitantly a whole set of

other entities, viz., a new type of labor, a new global order, a new society, new subjectivity, a new type of everyday life , and new kind of state [155]. Further Beck asserts that ' the neo-liberal regime' of capitalism is characterized by, among others, these key features**: '**Capital acquires access to the sources and norms of legal self-legitimation, allowing it to create legitimate systems autonomously and to institutionalize corresponding ways of regulating conflict; capital and the state thus merge into the 'capital-state', in which states, as 'autonomous units', make themselves the objects and subjects of a world order geared towards optimizing the interests of capital' [148]. Capitalism is unthinkable without its own market which it creates its own demands as it unfolds and expands. Risks have become 'a growing business' [163]. Risks are 'no longer the dark side of opportunities, they are also *market opportunities*'. Markets expand as new demands are created for security. In Becks' words, 'unlike demands, risks can be more than just called forth (by advertising and the like), prolonged in conformity to sales needs, and in short: manipulated. Demands, and thus markets, of a completely new type can be *created* by varying the definition of risk, especially demand for the avoidance of risk - open to interpretation, causally designable and infinitely reproducible. Production and consumption are thus elevated to a completely new level with the triumph of the risk society. The position of pre-given and manipulable demands as the reference point of commodity production is taken over by the *self-producible* risk'[144].The has led to the vicious circle of creating demands and expanding risk markets for security by the private companies in Europe and North America. Thus, Krahmann corroborates: 'the search for new sales opportunities has encouraged firms across a widening range of economic sectors, from healthcare and food to consumer goods, to indentify a wide variety of risks to the safety and wellbeing of peoples. This expansion of the private market in risks contributes to the perpetuation of the world risk society through its discourse of unknown and unknown-unknown risks' [321]. At the same time 'no one controls the markets risks since there is no world government, the market risk cannot be curbed on national markets. On the other side, no national market can seal itself off completely from the globalized markets' [132]. No less important is the fact that capital is global while work is basically local. 'Geographical distance thus loses much of its significance as a 'natural' limit to competition between different production sites. In the 'distanceless' space of computer technology, every location in the world now potentially competes with all others for scarce capital investment and cheap supplies of labour' [153]

Cloud computing has been enthusiastically adopted among the business enterprises of all sizes in the contemporary information capitalist societies. They realize that the benefits they will make by having easy to use computing services at a lower costand hence having 'a good computing system with the latest hardware and software technologies[322]. Two Tables, 34and 35 illustrate the spread of cloud computing across the world. The former shows the worldwide public Cloud service revenue forecast in billions of U.S. dollars [323], and the later reveals the revenue and market share of the leading corporations [324]. The concept of globalization implied here cannot be generalized. As Beck reminds: 'The power of not investing capital exists everywhere. Globalization is not a choice. It is nobody's rule. No one is in charge, no one started it, no one can stop it. It is a kind of organized irresponsibility. You keep looking for someone who is responsible, to whom you can complain. But there is nobody at the other end of the line, no e-mail address. The more the globalization discourse dominates all areas of life, the more powerful capital strategies become. But this still does not mean that managers are ruling the world' [159]. The importance of culture, in the **eighth** place, has been emphasized both in the risk society thesis and in the risk management/assessment of Cloud computing although in different contexts and ways. It has been stated that the role of risk management/assessment of Cloud computing is widely, if not

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	41.7	43.7	46.9	50.2	53.8
Cloud Application Infrastructure Services (PaaS)	26.4	32.2	39.7	48.3	58.0
Cloud Application Services (SaaS)	85.7	99.5	116.0	133.0	151.1
Cloud Management and Security Services	10.5	12.0	13.8	15.7	17.6
Cloud System Infrastructure Services (IaaS)	32.4	40.3	50.0	61.3	74.1
Total Market	**196.7**	**227.8**	**266.4**	**308.5**	**354.6**

Table 34:Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

Company	2018 Revenue	2018 Market Share (%)	2017 Revenue	2017 Market Share (%)	2018-2017 Growth (%)
Amazon	15,495	47.8	12,221	49.4	26.8
Microsoft	5,038	15.5	3,130	12.7	60.9
Alibaba	2,499	7.7	1,298	5.3	92.6
Google	1,314	4.0	820	3.3	60.2
IBM	577	1.8	463	1.9	24.7
Others	7,519	23.2	6,768	27.4	11.1
Total	**32,441**	**100.0**	**24,699**	**100.0**	**31.3**

Table 35:Worldwide IaaS Public Cloud Services Market Share, 2017-2018 (Millions of U.S. Dollars)

unanimously, recognized as an essential ingredient of ensuring security. ISO 31000 is very explicit to emphasize that 'human and cultural factors influence all aspects of risk management' [104]. In comparison, Beck states that risks are not things. 'Risks do not have any abstract existence in themselves. They acquire reality in the contradictory judgments of groups and populations. The notion of an objective yardstick against which degrees of risk can be measured overlooks the fact that risks count as urgent, threatening and real or as negligible and unreal only as a result of particular cultural perceptions and evaluations' [132]. He puts forward the logic that experts as well as cultural values and symbols play a significant role in the social construction of risk [148]. As far variation in risk perception is concerned among various sections of the population, Elena, who conducted a risk perception study using the psychometric method, states that 'some people assess all cloud computing applications positively, whereas others assess cloud computing applications in a generally negative way. Therefore, we could further examine the question of why different persons perceive cloud technology differently. Military and civilians differ in their perception of risks associated with cloud computing hazards. The military perceive higher levels of risk have more trust in governmental agencies to protect people's from cloud computing risks than the civilian does. Results of the present study are in line with previous research for other hazards' [325]. This corroborates Beck's views of differential risk perceptions by different groups of people. Van Schaik and others emphasize the importance of risk perception by saying that risk perception is both objective (fact-based) and subjective (socially constructed and emotional). It. is important for understanding 'the influences that inform risk perceptions because people will only take precautions if they have a genuine perception of the risks related to online activities' [326]. It is not irrelevant to note here as well that 'in fact, private security firms exacerbate risk perception in order to sell their services' [321].

Ninth, both Beck's risk thesis and Cloud computing are characterized by what may be appropriately called individualization of risk in the modern industrial capitalist society. For Beck, as previously said, individualization is the process and product of detraditionalization (viz. dissolution of traditional parameters of industrial society such as class culture and stratification, gender, and family roles) in the emergent late modern risk society. It is a process in which '*the individual himself or herself becomes the reproduction unit of the social in the lifeworld'* [144]. The individual, plainly speaking, bears all the risks in the society. 'The brutal fact of ontological insecurity always has an ultimate addressee: the recipient of the residual risk of the world risk society is the *individua*l. Whatever propels risk and makes it incalculable, whatever provokes the institutional crisis at the level of the governing regime and the markets, shifts the ultimate decision-making responsibility onto the individuals, who are ultimately left to their own devices with their partial and biased knowledge, with undecidability and multiple layers of uncertainty. This is undoubtedly a powerful source of right-wing radicalism and fundamentalism in the second modernity that is not easy to stem' [132**].** The tendency towards individualization was evident since the post-1960s which witnessed the breakdown of 'collective norms and hierarchies and the liberation of women'- disembedding- giving rise to disembodied individualization making the individual solely responsible for his action amid uncertainty and risk. Burgess, while stressing the point, suggests that **'**a stronger potential connection between the risk and individualization dimensions of his approach than was drawn out by Beck himself, through focusing upon the uncertainty created by disembedding. The uncertainty that follows from individualization suggests precautionary retreat into security and the construction of risk as a means of embodying and managing uncertainty'[327].This process of conjoining individualization with uncertainty and risk---individual responsibilization-- is also evident in the domain of cloud computing, especially cyber security domain. The neo-liberal message individual responsibilization is clear in matters of labor market, health care, crime and other matters. 'The rise of neo-liberalism since the 1980s has facilitated this responsibilization of citizens at the same time as it has favored private market over public service solutions to social needs and risks such as healthcare, transport and energy. Individualised responsibility detracts attention from collective and political responses to risks and focuses on how people can improve risk profiles through consumer choices' [321]. It is the individual who has to take care of himself and his interests, regardless of the consequences that he will have to bear. Thus, Renaud and others remind: 'In the *lingua franca* of the millennium, the computer owner has been *responsibilized* when it comes to managing the cybercrime risk. We believe this to be an accurate characterization because there is not very little support from the government or governmental bodies in terms of actively helping people to manage their cyber defences, nor is an official safety net put in place to support those who do fall victim to cyber attacks. As things stand, the most pervasive official strategy is the provision of advice. There is very little sign of the supportive infrastructure that one sees in areas such as physical crime, health and safety. ... It is time for ordinary citizens to insist that governments formulate effective cyber security risk regulation regimes.... It is every citizen's duty to hold his or her government to account in this matter. If we do not pressure them to take action, the cyber criminals will continue to wreak havoc. Allowing governments to continue with their responsibilization agenda, when it comes to cyber security, is no longer an option'[328]. The role of the private security business or risk management providers in expanding demand for its services is increasingly propped by their 'strongest marketing tool, .i.e., fear. 'The emergence of in risk societies directly benefits the private risk industry. This is created through the continuous discursive rehearsal of alleged dangers of life. In the UK and the US, the terms 'risk' and 'at risk' are thus 'used in association with just about any routine event' ...People might be able to resist the discourse of fear by pointing out the unverified and complex assumptions of expert calculations regarding unknown and unknown-unknown risks; but to do so is in itself a risk which people might not want to take' [321]. Risk has now been commodified, and risk exposure or risk avoidance rests with the 'individual responsibility and navigation' [317].

And last but by no means the least, a comparison of Beck's theoretical perspective on risk management and/or assessment with the usages of risk management and/or assessment in Cloud computing throws interesting light on the concerned issue. Although the Cloud computing researchers differ from each other in details or perspectives in this regard, there is very broad consensus among them about the necessity of risk management/assessment in search of ensuring security in Cloud computing as beneficial and profitable platform for individuals and organizations. As far as Beck is concerned, this process of risk management/assessment has little value in his schema of risk society, which has been analyzed earlier in Section IV. To summarize in his own words: 'Risks can no longer be dismissed as side effects. Instead they are becoming an internal problem of apparently self- enclosed social systems. At the same time, every attempt to manage the complexity of risk creates the need to fall back on abstractions and models which give rise to new uncertainties. This is the basis of a further institutionalized contradiction.

Risk and non-knowledge prompt the call for security and lead to new insecurities and uncertainties in the general groping about in the fog of insecurity and uncertainties. Moreover, the undecidability of problems, which nevertheless have to be decided, is growing along with the pressure to make decisions' [200]. In the risk society, which has become globalized, risks are 'systemic, unpredictable, uncertain and infinite' [151].Even in his first publication (1986) Beck argued that policy-oriented risk management, 'even in the most retrained and moderate objectivist account', will not succeed because risk, being a socially constructed phenomenon, is not 'reducible to the product of probability of occurrence multiplied with the intensity and scope of potential harm'[161].In order to come up with a more holistic perspective Beck expands the scope and prevalence of risks in other sectors of life not only in health and environment but also in liberty, equality, justice, rights, democracy, finance, terrorism etc.[134]. Looking at risk from this viewpoint, to borrow the words of Gross, 'rather like the precautionary principle, risk assessments are distinguished by the fact that they do not spell out what should be done but, at best, what should *not* be done. Just as more information does not necessarily reduce uncertainties, more knowledge often increases the awareness of ever more unknowns. In other words, awareness of ignorance is actively created alongside knowledge. Although Beck occasionally mentioned the relevance of the unknown in his writings after the mid-1990s, he still talked about risk when it came to labeling the overall phenomena he analyzed' [330].

There is more to it than this, as has already been hinted earlier. Commenting on the behavior of the profit seeking behavior of the private security industry, Becks says that their main concern is not with causes but rather with consequences of risk. In *Risk Society* (1986) he highlights this dimension of the capitalist motive of the security industry which attempts only with 'a 'coping' with the *symptoms and symbols* of risks. As they are dealt with in this way, the risks must *grow*, they must not actually be eliminated as causes or sources. Everything must take place in the context of a *cosmetics* of risk, packaging, reducing the symptoms of pollutants, installing filters while retaining the source of the filth. Hence, we have not a *preventive* but a symbolic industry and policy of eliminating the increase in risks' [144]. The argument is also echoed elsewhere [163]. The industry recommendation is thus usually mitigation of consequences rather than prevention or elimination of the causes of risk. No less important is the invisibility of risk. Stankiewicz elaborates: 'One of the major determinants of the process whereby risk is rendered invisible is the overlapping of science and big business. Science, both basic and applied, is becoming increasingly privatized and dominated by private concerns. Obviously, economic agents who reap profit from new technologies are loathe to advertise inherent risk. This is leading to conflict and tension between businessmen, public regulative institutions and public opinion. Scientists are the intermediaries in these conflicts. Unfortunately they are not always neutral although that is what is expected of them' [331]. Moreover, methodological refinement does not necessarily do this job, as he comments in an interview: 'Data analysis becomes more refined, excessively concerned with small details. This is the scientific reaction to uncertainties. However, this is usually accompanied by a loss of reflection. The perfection of methods seems to be a solution at first but this type of professionalization will not lead us to the way out of the insecurities that go hand in hand with the process of reflexive modernization. You can see this in the United States, where sociology is professionalized like in no other country in the world, and there, the testing of hypotheses and statistical analysis is the central line of the profession' [332]. In brief, Beck consistently opposed traditional risk management because it is incapable of dealing with manufactured uncertainties and implicit uncontrollability inherent in the global nature of risks in the modern industrial risk society. The existing regulatory institutions and established systems of liability and insurance have reached their limits and are antiquated [137].The way out of this jeopardy, as Beck would envisage, lies in power of emancipator metamorphosis to transfigure the concerned institutions into newer ones in the ongoing process of radical reflexive modernization aided by 'those affected by the risks which others produce' [131]. Put otherwise, 'the answer to better risk management for Beck, therefore, rests in large-scale societal metamorphosis. Global catastrophe, he posits, would result in social catharsis and the emancipatory impulses that would drive metamorphosis from a world risk society into reflexive modernization led by cosmopolitan communities around the world, united by risk and decline'[94]. If the public is encouraged about impending attacks and modes of attacks, then public awareness can be created and the public can be informed of countermeasures to be taken to mitigate the concerned risk [186]. Further, the public, through what Beck calls 'subpolitics' can mobilize and contest in political terms numerous issues – health, environment, science, business etc- whose origins can be traced back the risks and those produced them. Direct subpolitical activities include citizens' protest marches, blockades, consumer boycotts and so on [136].

In fine, it seems that the comparison between risks in Beck' perspective and risks in Cloud computing is both interesting and compelling. However, there is no space for any pessimism, for both, in spite of their deleterious consequences; there are positive dimensions in both. The positive dimension of the risk society is its progressive transfiguration of the risk society through emancipatory metamorphosis. 'Manufactured uncertainties, global risks are, highly ambivalent, paradoxically also a moment of hope, of unbelievable opportunities—a cosmopolitan moment' [159]. At the same rime concrete rewards flow from Cloud computing. An example of the rewards, i.e., advantages and benefits, that come from adoption of cloud computing can be cited from the study of Jones and others in recent times. Using the qualitative technique of case study enquiries, they investigated the implementation of cloud computing in both a practical setting and from an organizational user perspective three UK local government authorities which adopted cloud computing primarily with the intention of 'reducing costs and to strategically comply with the UK political mandate to implement cloud computing'. They sought to enhance existing 'taxonomies of rewards and risks' surrounding cloud computing in order 'to contribute to the normative literature by strengthening existing knowledge factors and providing new insights on cloud computing in the public sector especially from a local government perspective'. The Table 36 provided by them lists the rewards of cloud computing on the basis of existing literature [333]. While the risks in Beck's risk society have their genesis in the continuum between known and unknown unknown, especially within the domain of unawareness and non-knowledge, the same applies also to Cloud computing. Uncertainty characterizes the paradigms of both risk society thesis and Cloud computing, and, fortunately, both paradigms provide grist for their running mills for further research and analysis for their further improvement. The risk society thesis has received both critical acclaim and criticism from the researchers concerning its merit, drawbacks and future applications [133] [135] [149] [158] [178] [186] [334].Similar is the case with the new field of Cloud computing where numerous researchers are hailing it as new revolutionary paradigm of computing and pointing out its strengths and challenges including the controversy about the conflict over the definition of cloud computing itself [310] [335]

[336] [337]. While Logesswari and others hail Cloud computing as 'the new era for computing', Maniah and others consider it as one of the foundations that underlie the era of 4.0 Industrial Revolution [338] [339]. Pandi (Jain) and others find security of critical data as a major concern and a 'great barrier' for adoption and consider standard procedures for detecting security breaches 'still very immature' in cloud computing [340]. And yet at the same time, Varghese and Buyya piece together new trends and research directions for the next generation cloud computing [341].

Be that as it may, the issue of resolving threats, vulnerability, attacks along with uncertainty in cloud computing lingers on as thorny problems in way of eliminating and/or mitigating risks. Recently el Ata and Schmandt emphasize that 'to more precisely predict and plan for risk, it is important to understand the contribution of *dynamic complexity'* which is formed 'through interactions, interdependencies, feedback, locks, conflicts, contentions, prioritizations, enforcements, etc. Subsequently, dynamic complexity is revealed through forming congestions, inflations, degradations, latencies, overhead, chaos, singularities, strange behavior, etc'. It may then be said, as they do, that 'today management is handicapped by an inability to predict the future behavior of a system, corporation, economic, or industrial system, and the deficiencies of current approaches in their ability to rapidly diagnose and consequently fix problems before a risk may lead to a crisis and suddenly manifest itself. The cause of this predicament is the growing dynamic complexity that occurs over time and the negative effects it plays in a systemic implementation [342]. This conclusion seems commensurate with what Burgess and others suggest in their own analysis of

Rewards of cloud computing in Government organization

CLASSIFICATION FACTORSFACTORS	FACTORS	DESCRIPTION
Strategic	• Centralization of infrastructure	- Being able to centralize government infrastructure in locations with lower costs for example out-of-city centres.
	• Increased resilience	- The nature of cloud computing removes single points of failure and therefore provides a highly resilient computing environment for government organisations.
	• Device and location independence	- The independence of device and location enables users to access systems using a web browser regardless of location or device.
	• Release internal IT resources	- The reduction in the use government organisation's own computer system and peripherals.
	• Better Citizen Services	- Government organizations are redefining their businesses to deliver improved citizen services. For example, the Open Government initiative and Government as a Platform concept are good examples of better citizen services provided by governments informing and empowering the citizens through dashboards and scorecards about government and the flagship initiatives.
	• Green Technology	- Cloud storage services are more energy efficient than storage on local hard disk drives when files are only occasionally accessed. Additionally cloud services are more efficient than modern mid-range PCs for simple office tasks. Thus reducing an organisation's carbon footprint by saving energy.
Tactical	• Improved business continuity and disaster recovery	- Improved business continuity for government authorities and disaster-recovery capability by being on several cloud sites.
	• Improved agility and empowerment	- Improved agility and empowerment with users' ability to re-provision technological infrastructure resources themselves.
	• Faster implementation	Cloud-based implementation can be achieved relatively quickly accelerating the time required to make the new services available to internal users compared to traditional systems implementation.
	• Improved security	- Improved security by being able to leverage the cloud service providers' specialized security and privacy staff personnel and additional robust security systems and infrastructure
	• Scalability	- Allows servers and storage devices to be shared and utilization be increased or decreased as required
	• Easier application migration	- Ability to easily migrate application from one physical server (cloud) to another.
Operational	• Reduced costs	- Cost reduction as capital expenditure is converted to operational unit cost expenditure.
	• Reduced maintenance and support	- Reduced maintenance and support, especially for in-house IT teams, as software does not need to be installed on each user's computer and can be accessed from different places.
	• Flexibility of work practices	- Easier access from any appropriate internet-ready device, as infrastructure is off-site and provided by a third party and accessed via the internet, users can connect from anywhere.
	• Utilization and efficiency improvements	- Improved resource utilization and more efficient systems especially for systems that are often only 10–20% utilized.
	• Shared services	- Multi-tenancy enables sharing of resources and costs across a large pool of users.
	• Increased peak-load capacity	- When peak-load capacity increases users need not engineer for higher load-levels.

Table 36: Rewards of cloud computing in terms of its practices and functioning

Beck's sociological position: 'Related to his perspective on modernization, Beck's work should also be understood as a critique of science, or rather what is sometimes termed 'scientism' in an ecological perspective. This is not the science that embraces uncertainty but the hubris of a scientific management that denies it, and creates unrealistic expectations and claims that it can control what is actually uncontrollable. In a sense, Beck is proposing what we can recognize as mature risk management that recognizes that risk can only be managed or displaced rather than abolished, and trade-offs and unintended consequences are unavoidable. It is now widely understood that it is better to acknowledge and thus stay alert to uncertainty than to pretend it has been fixed through some technocratic means ... Beck's work was prescient in this regard. Challenging the denial of uncertainty is a vital theme developed by Beck' [343].

ACKNOWLEDGEMENT: The author gratefully acknowledges the important assistance received from Retired Professor Bipul Kumar Bhadra, PhD (McMaster), of Jadavpur University, Kolkata.

BIBLIOGRAPHY

[1]The World Bank, *World Development Report 2014: Risk and Opportunity-Managing Risk for Development*, The World Bank: Washington, DC, 2013, Pp. 53, 55.
[2] B. Fischhoff and J. Kadvany, *Risk: A Very Short Introduction*, Oxford University Press:New York, 2011,Pp.1, 4.
[3]P. Gooby-Taylor and Z.O. Zinn, *Risk in Social Science*, OUP: Oxford, 2006, p. 1.
[4]T.R.Koehler, *Understanding Cyber Risk: Protecting Your Corporate Assets*, Routledge: New York, 2018, Pp. 125-6.
[5] N.Postman, *Technopoly: The Surrender of Culture to Technology*, Vintage Books: New York, Pp.vii, 4-5.
[6] S. Mishra, "Exploitation of Information and Communication Technology by Terrorist Organisations", *Strategic Analysis*, 27(3), 2003, p. 439.
[7] B. Fischhoff et al., "Defining Risk", *Policy Sciences*, 17, 1984, p. 137.
[8]P. Hopkin, *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management*, London: Kogan Page, p. 37.
[9] P. Virilio and S. Lotringer, *Pure War: Twenty-Five Years Later*, Semiotexte,: Los Angeles, CA , 2008, p. 46.
[10] [C. Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?'*,Carnegie Endowment for International Peace: Massachusetts Avenue, 2019, p. 37.
[11] G. P. Nichols, "New Technologies, New Risks", *HDAIC Journal*, 4(1), 2017, p. 29.
[12]Jean-Marie Flaus, *Risk Analysis: Socio-technical and Industrial Systems*, ISTE: London, 2013, p. xiii.
[13] M. Davis, *The Monster Enters: Covid-19, Avian Flu, and the Plagues of Capitalism*, OR Books:New York, 2020.
[14]S. Tuli et al., "Predicting the growth and trend of COVID-19 pandemic using machine learning and cloud computing", *Internet of Things*, 11, 2020, p. 1.
[15]F. Furedi, *Culture of Fear: Risk-taking and the Morality of Low Expectation*, Continuum:London,2002, p. iv.
[16] S. Žižek, *Pandemic: COVID-19 Shakes the World*, Or Books: New York, 2020, Pp. 1, 15.
[17] J. Bezeau, *Coronavirus: Loss of Life & Normalcy*, 2020**.**
[18**]** L. Knorr, "Introduction" in L. Knorr et al., *After the Pandemic: Visions of Life Post-Covid-19*, Sunbury: Mechanicsburg, PA, 2020, p .1.
[19] World Economic Forum, *The Global Risks Report 2020*, World Economic Forum: Cologny/Munich, Switzerland
[20] I. Ghosh, "COVID-19: What are the biggest risks to society in the next 18 months?", 03, July, 2020, https://www.weforum.org/agenda/2020/07/covid19-future-economic-societal-geopolitical-risks.Retrieved on 23 December, 2020.
[21]Allianz Global Corporate & Specialty, "2020: Allianz Risk Barometer Appendix*", Allianz Global Corporate & Specialty SE: Munich, Germany*, 2020, Pp. 8, 11-3.Retrievedd on 08 October 2020.www.agcs.allianz.comw.
[22] Gartner, "Gartner Says Second Wave of COVID-19 Infections Continues to be the Top Emerging Risk Among Senior Executives ", 15 October 20, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-10-15-gartner-says-second-wave-of-covid19-infections-continues-to-be-the-top-emerging-risk-among-senior-executives0.Retrieved on 12 November 2020.
[23] Gartner, Gartner, 'Top 10 Emerging Risks of 3Q20',https://www.gartner.com/en/audit-risk/trends/top-ten-emerging-risks. Retrieved on 12November 2020.
[24]G. Carpenter, *Ahead of the Curve: Understanding Emerging Risks Report*, Marsh & McLennan, 2014, Pp. 3, 5,www.mmc.com. Retrieved on 12 November, 2020.
[25] L. T. Ostrom and C. A. Wilhelmsen, *Risk Assessment: Tools, Techniques, and Their Applications*, Wiley: Hoboken, NJ, 2020,Pp.7, 449-50, 454-6.
[26] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19", DOI: 0.1109/MITP.2020.2988330, IEEE 2020, Pp. 5, 9-10.
[27] S. Hakak et al., 'Have You Been a Victim of Covid-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies', *IEEE Access*, 8, 2020: DOI 10.1109/ACCESS.2020.3006172 Pp. 124135, 124136
[28] M. Boholm, *Risk, language and discourse*, Unpublished PhD Dissertation, Stockholm, 2016, kth.diva-portal.org,p. 2. Retrieved on 11 October, 2020.
[29]O. Renn, "Three decades of risk research: accomplishments and new challenges", *Journal of Risk Research* 1 (1), 1998, Pp. 49.
[30] T. W. Edgar, and D.O. Manz, *Research Methods for Cyber Security*, Syngress: Cambridge, MA, 2017, p. 71.
[31]S.Shafieian et al., "Attacks in Public Clouds:Can They Hinder the Rise of the Cloud?", in (eds.), Z. Mahmood, *Cloud Computing: Challenges, Limitations and R&D Solutions*, Springer: Heidelberg, 2014, p. 4.
[32] A. Zianiand A. Medouri, "Risks and Security Requirements for Cloud Environments', SCA '18: Proceedings of the 3rd International Conference on Smart City Applications,, https://doi.org/10.1145/3286606.3286865, 2018, p. 1.
[33] Reza Montasari, "An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities", in (eds.), A. Hosseinian-Far et al., *Strategic Engineering for Cloud Computing and Big Data Analytics*, Springer: Switzerland 2017, p. 189.
[34]I. Kateeb and M. Almadallah, "Risk Management Framework in Cloud Computing Security in Business and Organizations", *Proceedings of The 2014 IAJC/ISAM Joint International Conference,https://www.semanticscholar.org/paper/Risk-Management-Framework-in-Cloud-Computing-in-and-Kateeb-Carolina/f88fcc76bc513b84166889121b4b2f8d36b6cc03, 2014.*
[35] L. M. Vaquero et al., "A Break in the Clouds: Towards a Cloud Definition", *ACM SIGCOMM Computer Communication Review*, 39 (1), 2009, p. 51.

[36] P. Mell and T. Grance, *The NIST Definition of Cloud Computing-Special Publication 800-145*, National Institute of Standards and Technology: Gaithersburg, MD, 2011, p.2.
[37] H. Elazhary, 'Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions", *Journal of Network and Computer Applications*, 128, 2019, p. 106.
[38] V. Sharma, *The cloud-based demand-driven supply chain*, John Wiley: Hoboken, New Jersey, 2019, Pp. 33, 45-6,72, 74-5, 77-8, 81-2, 244.
[39] F. Shirazi et al., "Cloud Computing Security and Privacy: An Empirical Study", in (eds.), M. Kurosu, *Human-Computer Interaction: Interaction Contexts- 19th International Conference, HCI International 2017Part II, LNCS 10272*, Springer: Switzerland, 2017, p. 537. DOI: 10.1007/978-3-319-58077-7_43.
[40] R. Alosaimi and M. Alnuem, "Risk Management Frameworks for Cloud Computing: A Critical Review", *International Journal of Computer Science & Information Technology (IJCSIT)*, 8(4), 2016 Pp. 1-11.
[41] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey", *Computer Science Review*, 33, 2019, Pp. 7, 11.
[42] J. Nayak et al., "Nature Inspired Optimizations in Cloud Computing: Applications and Challenges" in (eds.), B. S. P. Mishra et al. *Cloud Computing for Optimization: Foundations, Applications, and Challenges*, Springer: Cham, Switzerland, 2018, p. 6.
[43] A. Ziani and A. Medouri, "Risks and Security Requirements for Cloud Environments", *SCA '18: Proceedings of the 3rd International Conference on Smart City Applications* , October 2018, ACM ISBN 978-1-4503-6562-8/18/10 $15.00, https://doi.org/10.1145/3286606.3286865.
[44] CRM Trilogix, "Cloud Resource Models – CRM", https://crmtrilogix.com/Cloud-Transformation/Cloud-Computing-Concepts/Cloud-Resource-Models---CRM/81, Accessed on 12 September 2020.
[45] D. Rountree and I. Castrillo, *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice*, Syngress: Waltham, MA, 2014, Pp. 35, 43-4.
[46] K.P. Narayana et al., "A Review on Different types of Deployment Models in Cloud Computing" ,*International Journal of Innovative Research in Computer and Communication Engineering*", 5(2), 2017 p. 1477.
[47] M.A. Bamiah and S. Brohi, "Exploring the Cloud Deployment and Service Delivery Models", *International Journal of Research and Reviews in Information Sciences (IJRRIS)*, 1(3), 2011, p. 77.
[48]R. Montasari, "An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities" in (eds.), A. Hosseinian-Far et al, *Strategic Engineering for Cloud Computing and Big Data Analytics*, Springer: Switzerland, 2017, p. 189.
[49] M. Rausand and S. Haugen, *Risk Assessment: Theory, Methods, and Applications*, Wiley: Hoboken, NJ, 2020, Pp, 10, 15, 62-3, 99-101.
[50] C. E. Althaus, "A Disciplinary Perspective on the Epistemological Status of Risk", *Risk Analysis*, 25 (3), 2005, p. 569. DOI: 10.1111/j.1539-6924.2005.00625.x.
[51] *P. Kelly, "*The evolution of risk management thinking in organizations", in (eds.),Kurt J. Engemann, *The Routledge Companion to Risk, Crisis and Security in Business*, Routledge: London, p.21.
[52]RAND Corporation, 'Systemic Risk: It's Not Just in the Financial Sector', http://www.jstor.com/stable/resrep24271.Retrieved on 15 August 2020.
[53] T. Aven, "The Risk Concept—Historical and Recent Development Trends", *Reliability Engineering and System Safety*, 99, 2012, pp.33–44.
[54]Phil Kelly, 'The evolution of risk management thinking in organizations ', in (eds.) Kurt J. Engemann, *The Routledge Companion to Risk, Crisis and Security in Business*, Routledge: New York2018, Pp. 21-32, 41.
[55] E. C. Nacol, *An Age of Risk: Politics and Economy inn Early Modern Britain*, Princeton University Press: Princeton, 2016, p. 2.
[56] T. A. Alexandru, "Defining the Concept of Risk Applied In Entrepreneurship. Conceptual Delimitation Risk - Entrepreneurial Uncertainty", *DOI: 10.1515/eras-2019-0004*, Pp.44, 46.
[57] C. Zabel, "The History and Theory of Risk", *Eighteenth-Century Life*, 42(3), 2018, .p.72.
[58]Jean-Marie Flaus, *Risk Analysis: Socio-technical and Industrial Systems*, ISTE: London: 2013, Pp. 4, 13-4.
[59]A. Šotićand R. Rajić, "The Review of the Definition of Risk", *Online Journal of Applied Knowledge Management*, 3(3), 2015, p. 19,
[60] Niklas Mo¨ller, "The Concepts of Risk and Safety", in (eds.), S. Roeser et al., *Hand book of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk*, Springer: Dordrecht. 2012, p. 58.
[61] J. O. Zinn, *Understanding Risk-Taking*, Palgrave Macmillan: Cham, Switzerland, 2020, Pp. 2, 17, 135.
[62]*J. F. Outreville, Theory and Practice of Insurance, New York: Springer, 1998, p. 2*.
[63] M. Boholm et al., "The Concepts of Risk, Safety, and Security: Applications in Everyday Language", *Risk Analysis*, 36(2), 2016, p.321.
[64] T. Aven and O. Renn, "On risk defined as an event where the outcome is uncertain", *Journal of Risk Research*, 12(1), 2009, Pp. 1-2, 6.
[65] D. Garland, "The Rise of Risk", in (eds.), R.V. Ericson and A. Doyle, Risk and Morality, Toronto University Press: Toronto, p.49.
[66] C. Yoe, *Principles of risk analysis: decision making under uncertainty* , Taylor and Francis, CRC Press: Boca Raton, 2019, Pp.1-2, 5, 7-9, 22., 99-101.
[67]C. Hohenemser et al., 'The Nature of Technological Hazard', in (ed.), P. Slovic *The Perception of Risk*,, NewYotrk:Earthscan, 2000, p.169
[68] A. Kozyreva et al., "Interpreting Uncertainty: A Brief History of Not Knowing", in (eds.), R. Hertwig et al., *Taming Uncertainty*, MIT Press: Cambridge, MA, 2019, p. 344.
[69] Z. Bauman, *Liquid Times: Living in an Age of Uncertainty*. Polity: Cambridge, 2007, p. 11].
[70] D. V. Lindley, *Understanding uncertainty*, Wiley: Hoboken, New Jersey, 2014, p. 2.
[71]D.J.C. Skinner et al., "A review of uncertainty in environmental risk: characterising potential natures, locations and levels", *Journal of Risk Research*, 17(2), 2014, p.196.
[72][M. C. Politi et al., 'Communicating the Uncertainty of Harms and Benefits of Medical Interventions' *Medical Decision Making*, Sep–Oct 2007, p. 682. DOI: 10.1177/0272989X07307270.
[73] G. Allen and R. Derr, *Threat Assessment and Risk Analysis: An Applied Approach*, Amsterdam: Butterworth Heinemann, 2016, Pp. 10, 14.
[74]T. Aven, "An Emerging New Risk Analysis Science: Foundations and Implications", *Risk Analysis*, 38(5), 2018, p. 880.
[75] F.H. Knight, *Risk, Uncertainty and Profit*, Boston: Houghton Mifflin, 1921, p. 19-20.
[76]A. Kozyreva et al., "Interpreting Uncertainty: A Brief History of Not Knowing", in (eds.), R. Hertwig et al., *Taming Uncertainty*, Cambridge, MIT Press: MA, 2019, p. 344.
[77]S. Gunn & J. Hillier, "When Uncertainty is Interpreted as Risk: An Analysis of Tensions Relating to Spatial Planning Reform in England", *Planning Practice and Research*, Vol. 29(1), p. 62 . http://dx.doi.org/10.1080/02697459.2013.848530.

[78]Wikipedia, "There are known knowns", https://en.wikipedia.org/wiki/There_are_known_knowns. Retrieved on December 22, 2020.
[79]M. Iqbal, "Known Risks and Unknown Risks –PMP/CAPM", https://mudassiriqbal.net/known-risk-and-unknown-risks/. Retrieved on 17 October, 2020.
[80]T. A. Dang, "Known Knowns, Unknown Knowns, and Unknown Unknowns**",** https://medium.com/datadriveninvestor/known-knowns-unknown-knowns-and-unknown-unknowns-b35013fb350d**.** Retrieved on 17, October2020.
[81] Management Yogi, "Risk Classification: Known-Knowns, Known-Unknowns, Unknown-knowns and Unknown-unknowns**"**, https://www.managementyogi.com/2019/09/risk-classification-known-knowns-known-unknowns-unknown-knowns-and-unknown-unknowns.html. Retrieved on 17 October, 2020.
[82]R. Rawson et al., "Known Knowns, Known Unknowns, Unknown Unknowns: The Predicament of Evidence-Based Policy", *American Journal of Evaluation*, 32(4), 2011, p. 519.
[83]H. Riesch 'Levels of Uncertainty' in (eds.), S. Roeser et al. (eds.), *Handbook of Risk Theory*: *Epistemology, Decision Theory, Ethics and Social Implications of Risk*, Springer: Dordrecht, Pp. 89, 97-9.
[84]M. C. Politi et al., 'Communicating the Uncertainty of Harms and Benefits of Medical Interventions' *Medical Decision Making*, Sep–Oct 2007, p. 682. DOI: 10.1177/0272989X07307270.
[85] S. Gunn & J. Hillier, "When Uncertainty is Interpreted as Risk: An Analysis of Tensions Relating to Spatial Planning Reform in England", *Planning Practice and Research*, 29 (1), 2014, p. 62. http://dx.doi.org/10.1080/02697459.2013.848530].
[86]Simona-Valeria Toma et al., "Risk and Uncertainty*", Procedia Economics and Finance*, 3, 2012, Pp.978-9.
[87]C. Tannert et al., "The Ethics of Uncertainty", EMBO *reports*, 8 (10), 2007, p. 893.
[88] K. Kampourakis and K. McCain, *Uncertainty: How It Makes Science Advance*, Oxford University Press: Oxford, 2020, p. 215.
[89]J.O. Zinn, 'A Comparison of Sociological Theorizing on Risk and Uncertainty. in J. O. Zinn (ed.), *Social Theories of Risk and Uncertainty: An Introduction*, Blackwell: Oxford, 2008, Pp. 178-9., 198-9.
[90]O. Renn, Risk Governance: Coping with Uncertainty in a Complex World, Earthscan: London, 2008, p. 15.
[91] R. Lidskogand G. Sundqvist, "Sociology of Risk", in (eds.), S. Roeser et al., Handbook of Risk Theory, Springer: Dordrecht, 2012, p. 1008.
[92]O. Renn, "Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts", *GAIA* 17(1), 2008, Pp. 50. 66.
[93] C. M. L. Wong & S. Lockie, "Sociology, risk and the environment: a material-semiotic approach", *Journal of Risk Research*, 21(9), 2018, p. 1090.
[94] C. M. L. Wong, *Energy, Risk and Governance: The Case of Nuclear energy in India*, Palgrave/Macmillan: Cham, Switzerland, 2018, Pp.29-30, 39-41, 48.
[95]A. Refsdal et al., *Cyber-Risk Management*, Springer: Cham Heidelberg, 2015, Pp.12,. 125.
[96] T.Aven, *The Science of Risk Analysis Foundation and Practice*, Routledge: London, 2020, Pp. 29-32, 44.
[97] T. Aven, *Misconceptions of Risk*, Wiley: Chichester, West Sussex, 2010, p. vii.
[98] P. Gardoni et al., "Risk Analysis of Natural Hazards: Interdisciplinary Challenges and Integrated Solutions", in (eds.), P. Gardoni et al, *Risk Analysis of Natural Hazards Interdisciplinary Challenges and Integrated Solutions* Springer: Cham Heidelberg, 2016, p. 3.
[99] T. Aven and O. Renn, *Risk Management and Governance: Concepts, Guidelines and Applications*, Springer-Verlag: Berlin, 2010, p. v.
[100] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How To Fix It*, Hoboken, New Jersey: Wiley, 2020, Pp. 7, 12-3, 106.
[101]B. Delogu, *Risk Analysis and Governance in EU Policy Making and Regulation*, Springer: Switzerland, 2016, Pp. 15, 38, 243, 245-6.
[102] J -Y.Yoo, "A Study on Risk Management in Digital Risk Society", IJISET - *International Journal of Innovative Science, Engineering & Technology*, 4 (2), 2017, p.265.
[103]International Organization for Standardization, "Risk Management ISO 31000**",** iso.org, 2018, Pp. 1, Appendix B-9-10.
[104] IRM, *Standard Deviations: A Risk Practioners Guide to ISO 3100 2018*, Institute of Risk Management: London, 2018, Pp. 5-12.
[105] C. Yoe, *Primer on Risk Analysis: Decision Making Under Uncertainty*, Boca Raton: Taylor & Francis, 2019, Pp. 57, 114, 118, 127-8.
[106] O. A. Lindaas and K. A. Pettersen, "Risk analysis and Black Swans: two strategies for de-blackening", *Journal of Risk Research*, 19 (10), 2016, Pp. 1231, 1233.
[107] P. Hopkin, *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, Kogan Page: London, 2018.
[108] J. Lam, *Implementing Enterprise Risk Management: From Methods to Applications*, Wiley: Hoboken, New Jersey, 2017, p. 367.
[109] P. Carrel, *The Handbook of Risk Management: Implementing a Post-Crisis Corporate Culture*, West Sussex: John Wiley & Sons Ltd., 2010, p. 3.
[110] G. Allen and R. Derr, *Threat Assessment and Risk Analysis: An Applied Approach*, Butterworth Heinemann: Waltham, MA, 2016. p. 6.
[111]National Institute of Standards and Technology (**NIST),** *Guide for Conducting Risk Assessments-NIST Special Publication 800-30 Revision 1*, National Institute of Standards and Technology: Gaithersburg, MD, 2012, p. 23
[112] M.R.M Talabis and J. L. Martin, *Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis*, Syngress: Waltham, MA, 2013, p. 1.
[113] N. Bhansali (ed.), *Data Governance: Creating Value from Information Assets*, CRC Press: Boka Raton, FL, 2014, Pp. 2-5.
[114] B. Engels, "Data Governance as the Enabler of the Data Economy", *Intereconomics*, 2019, 4, DOI: 10.1007/s10272-019-0827-y, p. 217-8.
[115] Society for Risk Analysis Glossary (SRA), *SRA Glossary-FINAL*, 2018, **p. 8.** www.sra.org. Retrieved on 10 September, 2020.
[116] P. C. Godfrey et al, *Strategic Risk Management: New Tools for Competitive Advantage in an Uncertain Age*, Berrett-Koehler Publishers**:** Oakland, CA, 2020.
[117] E. Lachapelle et al., "ISO31000:2018-Risk Management – Guidelines"**,**www.pecb.com, Retrieved on August 17, 2020, p.7.
[118]The Chartered Institute of Management Accountants (CIMA),*Risk Culture: How To Get It Right*, https://isca.org.sg/tkc/cogov/risk-management/risk-management/2018/may/risk-culture-how-to-get-it-right/, pp. 4, 18. Retrieved on 24 July, 2018.
[119]J. DeLoach, "The Importance of Risk Culture", https://www.corporatecomplianceinsights.com/the-importance-of-risk-culture/, May 2015. Retrieved on October 06, 2020.
[120]Deloitte Development LLC., *Cultivating a Risk Intelligent Culture: Understand, Measure, Strengthen, and Report*, www2 .deloitte.com, PDF, 2012, p. 2.
[121]E. Banks, *Risk Culture: A Practical Guide to Building and Strengthening the Fabric of Risk Management*, Hampshire: Palgrave Macmillan2012, Pp. 23-7.
[122]C. Levy et al., "Taking Control of Organization Risk Culture", *Risk Practice: McKinsey Working Papers on Risk*, 2010. www. Mckinsey. Com, PDF, Pp. 3-4.
[123] KPMG, *Your Risk Culture: An ERM Enabler or Barrier?*, KPMG Government Institute: kpmg.com/us/governmentinstitute, October 2018, p. 4.

[124] A. Wood and A. Lewis–"Risk culture development and its impact: **the case of the Caribbean Development Bank",***International Journal of Business and Economic Development*, 6(1), 2018, Pp. 21-2.
[125]P.J. McConnell, "A Risk Culture Framework for Systematically Important Banks", *Journal of Risk and Governance*, 3(1), 2013, p. 39.
[126]D. Hillson, *Managing Risk in Projects*, Surrey: Gower: Surrey: England, 2009, pp. 89-90.
[127] A. Burgess et al., "Considering Risk: Placing the Work of Ulrich Beck in Context*", Journal of Risk Research*, 21(1), 2017, p. 1. DOI:10.1080/13669877.2017.1383075
[128]*P. O'Malley, "*Governmentality and the analysis of risk", in (eds.), *A. Burgess* et al., *Routledge Handbook of Risk Studies*, Routledge: London, 2016, p. 109.
[129]L. Kook, "Cyber Security and Risk Society: Estonian Discourse on Cyber Risk and Security Strategy", https://digitalcommons.unl.edu/scholcom/135, 2018, p. 36.
[130]W. Bonß and J. O. Zinn, "Risk and theory in Germany", in (eds.),A. Burgess et al.., *Routledge Handbook of Risk Studies*, Routledge: London, 2016, Pp. 95-6,103-4.
[131] G. Mythen and S. Walklate, "Not Knowing Emancipatory Catastrophism and Metamorphosis:Embracing the Spirit of Ulrich Beck", *Security Dialogue*, 47(5),Pp. 412,404, 407.
[132] U. Beck, *World at Risk*, Polity Press: Cambridge, 2009, Pp., vii, 5, 7, 9,13-4, 18, 21, 32, 35-6, 50, 52, 92, 115,117-8, 122-3, 126-7, 149,159, 178,183, 188, 195, 199.
[133]M. P. Sørensen and A. Christiansen, *Ulrich Beck: An Introduction to The Theory of Second Modernity and the Risk Society*, Routledge: New York, 2013, Pp. 2, 7, 15, 21, 31-4,52, 84, 104-5.
[134] M. Ekberg, "The Parameters of the Risk Society: A Review and Exploration*", Current Sociology*, 55(3), 2007, Pp.343, 345, 355, 360.
[135] L. Bergkamp, "The concept of *risk society* as a model for risk regulation – its hidden and not so hidden ambitions, side effects, and risks*", Journal of Risk Research*, 20 (10), 2017, Pp.1275-91.
[136] G. Mythen, "Reappraising the Risk Society Thesis: Telescopic Sight or Myopic Vision?", Current *Sociology*, 55(6), 2007,Pp.794, 798-9
[137] G. Mythen, "The Critical Theory of World Risk Society: A Retrospective Analysis", *Risk Analysis*, 2018, p. 4.DOI: 10.1111/risa.13159.
[138] D. Reed (ed.), *Structural Adjustment, the Environment and Sustainable Development*, Earthscan: London, 1996, Pp. 25-37.
[139] U. Beck, "Risk Society Revisited: Theory, Politics and Research Programmes", in (eds.), B. Adam et al., *The Risk Society and Beyond: Critical Issues for Social Theory*, Sage: London, 2005), Pp.212, 226.
[140] J.S. Picou and D.A. Gill, "The Exxon Valdez Disaster as Localized Environmental Catastrophe: Dissimarities to Risk Society Theory?" in (ed.), M. J. Cohen, *Risk in the Modern Age: Social Theory, Science and Environmental Decision-Making*, Palgrave: Hampshire, 2000, p. 145.
[141] J. Urry, "Preface", in (ed.), U. Beck, *Ulrich Beck: Pioneer in Cosmopolitan Sociology and Risk Society*, Springer: Cham Heidelberg, 2014, Pp. vi-vii.
[142] U. Beck, *World Risk Society*, Polity: London, 1999, Pp.2-3,6-7,9-10, 16, 19, 35-6, 40, 48, 51,53, 60, 63, 70, 73-5, 77, 121.
[143] D. S.L. Jarvis, "*Theorizing Risk: Ulrich Beck, Globalization and the Rise of the Risk Society*",
Lee Kuan Yew School of Public Policy: National University of Singapore, p. 2. Risk._RR3-u-Beck.pdf
[144] U. Beck, *Risk Society: Towards a New Modernity*, Sage: London, 1992, Pp.12, 19, 21, 23, 26,36-7,45-6, 49, 53,56-7, 58-9, 78-9, 88-90,130, 135, 140-50,156-62, 166-71, 177, 195, 234.
[145] U. Beck, *Ecological Politics in an Age of Risk*, Polity: Cambridge, 1995, Pp. 1, 67,73, 77-78, 101, 113, 119,125-6,139, 149.
[146]G. Mairal, "Has Risk a History?", in (eds.), B. Ghosh and B.Sarkar, *The Routledge Companion to Media and Risk*, Routledge: London, 2020 p. 34.
[147]D. Lupton, *Risk*, Routledge: London, 2005, Pp. 5-6, 66, 68-9, 71.
[148] U. Beck, *Power in the Global Age: A New Political Economy*, Polity Press: Cambridge, 2005, Pp.xii, 59, 101-2, 103-6, 121, 133, 243.
[149] J. V. Loon, *Risk and Technological Culture: Towards a Sociology of Virulence*, Routledge: London, 2002, Pp. 19,27, 31-32, 156.
[150] P. Strydom, *Risk, Environment and Society*, Open University Press: Buckingham, 2002, p. 57.
[151] U. Beck and J. Willms, *Conversations with Ulrich Beck*, Polity: Cambridge, 2004, Pp .60, 118, 124, 135-6,150,171.
[152] U. Beck, "The Reinvention of Politics: Towards a Theory of Reflexive Modernization", in (eds.), U. Beck et al., *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*, Stanford University Press: Stanford, 1994, p. 5.
[153] U. Beck, *The Brave New World of Work*, Polity: Cambridge, 2000. Pp. 18-9, 27, 70, 73-5.
[154] U. Beck, "The Reinvention of Politics: Towards a Theory of Reflexive Modernization", in (eds.), U. Beck et al., *Reflexive Modernization: Politics,Tradition and Aesthetics in the Modern Social Order*, Stanford University Press: Stanford, 1994, Pp. 2, 5, 14.
[155] U. Beck et al., "The Theory of Reflexive Modernization: Problematic, Hypotheses and Research Programme", *Theory, Culture & Society*, 20(2), 2003, Pp. 2-3, 13, 22.
[156] U. Beck, "Risk Society and the Provident State", in (eds.), S. Lash et al., *Risk, Environment & Modernity: Towards a New Ecology*, Sage: London, 1998, Pp. 27-8.
[157] H. Bulkeley, "Governing Climate Change: The Politics of Risk Society", Transactions of the Institute of British Geographers 26(4), 2001, p. 433. DOI: 10.1111/1475-5661.00033.
[158]E. A. Rosa et al., *The Risk Society Revisited: Social Theory and Risk Governance*, Temple University Press: Philadelphia, 2013, Pp. 26, 75, 131, 133.
[159]U. Beck, *Ulrich Beck: Pioneer in Cosmopolitan Sociology and Risk Society*, Springer: Cham, Switzerland, 2014, Pp.81-4, 86, 88, 160, 170.
[160]U, Beck, "Emancipatory catastrophism: What does it mean to climate change and risk society?"*Current Sociology*, 63(1), Pp.79, 83.
[161]U. Beck, "World Risk Society", in (eds.), J. K. B. Olsen et al., *A companion to the philosophy of technology*, Wiley-Blackwell: West Sussex, 2009. Pp. 496-7.499.
[162] R. Boyne, "Cosmopolis and Risk: A Conversation with Ulrich Beck", *Theory, Culture& Society*, 18(4), 2001, Pp.47-48, 56, 61-2.
[163]U. Beck, "On the Way toward an Industrial Society of Risk?"*International Journal of Political Economy*,20(1), 1990, Pp. 59, 61-2, 64.
[164] U. Beck, "The cosmopolitan perspective: sociology of the second age of modernity", *British Journal of Sociology*, 51(1), 2000, Pp. 80-81.
[165] E. Krahman, "The Commodification of Security in the Risk Society", Working Paper No. 06-08 PDF, School of Sociology, Politics, and International Studies, University of Bristol, Pp. 3-4.
[166]U. Beck, "The Social and Political Dynamics of the World at Risk: The Cosmopolitan Challenge", *AESOP*, July 2012, p. 8.
[167] U. Beck, "Global Generations in World Risk Society", *Revista CIDOB d'Afers Internationals*, No. 82/83, p. 215.
[168]U. Beck, "Living in the World Risk Society", *Economy and Society*, 35(3), 2006, Pp.332-3,336, 343, 340.
[169]U. Beck and E. Beck-Gernsheim, *Individualization: Institutionalized Individualism and its Social and Political Consequences*, Sage: London, 2002, Pp. xi, 3-4, 7, 26, 38,42, 47-8 ,201-2, 206-7, 210-12.
[170] S. Lash, "Foreword: Individualization in a non-linear mode", in U. Beck and E. Beck-Gernsheim, *Individualization: Institutionalized Individualism and its Social and Political Consequences*, Sage: London, 2002, Pp. vii, ix, xi.
[171] U. Beck and J. Willms, *Conversations with Ulrich Beck*, Polity: Cambridge, 2004, Pp. 62-6, 101, 171.
[172]U. Beck, "World Risk Society", in (eds.), J.K.B. Olsen et al., *A Companion to the Philosophy of Technology*, Wiley-Blackwell-West Sussex, 2009, Pp. 497-8.

[173] K. Marx, *Grundrisse*, Penguin Books: Harmondsworth, 1973, P. 107.
[174] D. Curran, "Risk Society and the Distribution of Bads: Theorizing Class in the Risk Society", *British Journal of Sociology*, 64(3), 2-14, Pp. 44-62.
[175] U.Beck, "Why 'class' is too soft a category to capture the explosiveness of social inequality at the beginning of the twenty-first century", *British Journal of Sociology*, 64(1), 2013, Pp. 65, 68, 72.
[176] U. Beck, What *is Globalization*? Polity: Cambridge, 2000, Pp.23, 11, 13, 20, 97. 105.
[177] S. Timcke, *Capital, State, Empire: The New American Way of Digital Warfare*, University of Westminster Press: London, 2017.
[178] D. S. L. Jarvis, "Risk, Globalisation and the State: A Critical Appraisal ofUlrich Beck and the World Risk Society Thesis", *Global Society*, 21 (1), 2007, p. 26.
[179] U. Beck, "World at Risk: The New Task of Critical Theory", *Development and Society*, 37(1), 2008, Pp.5, 8, 14-5, 19-20.
[180] U. Beck, "Living in the world risk society", *Economy and Society*, 35(3), Pp. 337-8.
[181] L.S. Keller, "Discovering and Doing: Science and Technology- An Introduction," in (eds.), G.Kirkup and L.S.Keller, *Inventing Women: Science, Technology and Gender*, Polity: Cambridge, 1992, p. 25.
[182] . A. Webster, *Science, Technology and Society.* Macmillan: Houndmills, 1991, Pp. 3-6.
[183] N. Mulkay, *Science and the Sociology of Knowledge*, George Allen and Unwin: London, 1979, Pp. 20-21.
[184]Editorial, "Considering Risk: Placing the Work of Ulrich Beck in Context", *Journal of Risk Research*, 21(1), 2017, Pp. 1, 3.
[185] J. Sand, "Living with Uncertainty after March 11, 2011", *The Journal of Asian Studies*, 71(2), 2012, Pp.313, 315.
[186] G. Mythen, "Thinking with Ulrich Beck: Security, Terrorism and Transformation*", Journal of Risk Research*, 21(1), Pp. 20-21, 24.
[187]U. Beck, "The Social and Political Dynamics of the World at Risk: The Cosmopolitan Challenge", *AESOP*, 2012, Pp..5, 7.
[188] J.V. Loon, "Virtual Risks in an Age of Cybernetic Reproduction", in (eds.), B. Adam et al, *The Risk Society and Beyond: Critical Issues for Social Theory*, Sage: London, 2005, p. 173.
[189] J. Adams, "Risk and culture", in (eds.), A. Burgess, et al., *Routledge Handbook of Risk Studies*, Routledge: London, 2016, p. 85.
[190]M.P. Sorensen, "Ulrich Beck: Exploring and Contesting Risk", *Journal of Risk Research* 21(1), 2018, Pp. 11-2.
[191] A. Irwin, *Sociology and the Environment: A Critical Introduction to Society, Nature and Knowledge*. Cambridge: Polity: Cambridge, 2001, p. 79.
[192]S. Dryhurst et al., "Risk perceptions of COVID-19 around the world", *Journal of Risk Research*, 23(7-8), 2020, Pp. 994-5.
[193] C. Bryce et al., "Resilience in the face of uncertainty: early lessons from theCOVID-19 pandemic", *Journal of Risk Research*, 23(7-8), 2020, p. 2.
[194] S. Matthewman and K. Huppatz, "A sociology of Covid-19", *Journal of Sociology*, DOI: 10.1177/1440783320939416, 2020, p. 2.
[195] A. Collins et al., "COVID-19 risk governance: drivers, responses and lessons to be learned", *Journal of Risk Research*, 23(7-8), 2020, p. 3.
[196] H-S. Kim, "Beyond Doubt and Uncertainty: Religious Education for a Post-COVID-19 World", *Religious Education*, DOI: 10.1080/00344087.2021.1873662, 19 Jan 2021, p. 7.
[197] J.O. Zinn, "'A monstrous threat': how a state of exception turns into a 'new normal'", *Journal of Risk Research*, 23(7-8), 2020, p. 1083.
[198]M. Freudendal-Pedersen andS. Kesselring, "What is the urban without physical mobilities? COVID-19-induced immobility in the mobile risk society", *Mobilities*, https://doi.org/10.1080/17450101.2020.1846436, 2020, p. 2.
[199]World Health Organization, "Communicating and Managing Uncertainty in the COVID-19 Pandemic: A quick guide", www.who.int › docs › searo › whe › coronavirus19 › ma..., PDF, 27 May 2020,
[200]U. Beck, "Critical Theory of World Risk Society: A Cosmopolitan Vision", *Constellations* 16(1), 2009, p.9.
[201]U. Beck, *The Metamorphosis of the World*, Polity: Cambridge, 2016
[202]W. Chen, et al., "A transnational networked public sphere of air pollution: analysis of a Twitter network of PM2.5 from the risk society perspective", *Information, Communication & Society*, 20(7), 2017, p. 1005.
[203] E. A. Rosa, "Metatheoretical foundations for post-normal risk", *Journal of Risk Research*, 1998,1 (1), p. 15.
[204]C. Bryce et al., "Resilence in the face of uncertainty: early Lessons from the Covid-19 Pandemic", Journal of Risk Researh, 23(7-8), 2020, p. 5.
[205] P. Soto-Acosta, "COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear", *Information SystemsManagement*, 37(4), p. 261.
[206] S. Jasanoff, "The Songlines of Risk*", Environmental Values*, 8(2), 1999, p. 150.
[207] M. Power, "Risk, Social Theories, and Organizations", in (eds.), P. Adler et el., *The Oxford Handbook of Sociology, Social Theory, and Organization Studies: Contemporary Currents,* Oxford University Press: Oxford, 2014, p. 280.
[208]C.M.L. Wong, *Energy, Risk and Governance: The Case of Nuclear Energy in India*, Palgrave Macmillan: Cham, Switzerland, 2018, Pp. 29-30.
[209] E. Bosco and G.M.D. Giulo, "Ulrich Beck: Considerations on His Contributions and Challenges to the Studies in Environment and Society", *Ambiente & Sociedade*, São Paulo v. XVIII, n. 2, abr.-jun. 2015, p.146.
[210] S. Pearson, "Privacy, Security and Trust in Cloud Computing", in (eds.), S.Pearson and G. Yee, *Privacy and Security in Cloud Computing*, Springer:: London, 2013, p. 21.
[211] M.M. Alani, *Elements of Cloud Computing Security*, Springer: Switzerland, Pp. 16-7.
[212]M. Lagana, "Information security in an ever-changing threat landscape", in (eds.), K. J. Engemann, The *Routledge companion to risk, crisis and security in business*, Routledge: New York, 2018, p.255
[213] M. Jouini and L.B.A. Rabai, **"**A Security Risk Management Metric for Cloud Computing Systems", *International Journal of Organizational and Collective Intelligence*, 4(3), 2014, Pp. 10, 17.
[214]S. Liu, "Securing the Clouds: Methodologies and Practices" in (eds.), S. Murugesan and I Bojanova, *Encyclopedia of cloud computing*, John Wiley & Sons, Ltd: Chichester, 2016, p. 220-21.
[215]A.Razaque et al, "Enhanced Risk Minimization Framework for Cloud Computing Environment"
2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA),
IEEE *Xplore, 2019,* DOI**:** 10.1109/AICCSA.2018.8612785.
[216]M. Hawedi et al., "Security as Service for Cloud Tenants (SaaS)", Procedia Computer Science, 130, 2018, p. 1025.
[217] M. S. Akshaya and G. Padmavathi. "Taxonomy of Security Attacks and Risk Assessment of Cloud
Computing", in (eds.), J.D. Peter et al., *Advances in Big Data and Cloud Computing: Proceedings of ICBDDD18*, Springer: Singapore, 2019, p. 57
[218]P. Samarati and S. D. C. di Vimercati, "Cloud Security: Issues and Concerns", in (eds.), S. Murugesan and I. Bojanova, *Encyclopedia of Cloud Computing*, Wiley: Hoboken, NJ, 2016, Pp.209-10.
[219] B. De Decker, "Introduction to Computer Security", in (eds.), B. Preneel and V. Rijmen, *State of the art in applied cryptography: Course on Computer Security and Industrial Cryptography* Leuven, Belgium, June 3-6, 1997, Revised Lectures, Springer: Berlin, 1998, p.381.
[220] D. W. Roberts, "Security Management – The Process", in (eds.), Bart Preneel and Vincent Rijmen, *State of the art in applied cryptography : Course on Computer Security and Industrial Cryptograph*y Leuven, Belgium, June 3-6, 1997,Revised Lectures, Springer: Berlin, 1998, p. 374.

[221] M. Ahmed and M.A. Hossain, "Cloud Computing and Security Issues in the Cloud", *International Journal of Network Security & Its Applications*, 6(1), 2014, p.30.
[222] D. Antonucci, *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, John Wiley & Sons, Inc.:, Hoboken, New Jersey, 2017, p. 46.
[223] S.N. Mthunzi et al., "Cloud computing security taxonomy: From an atomistic to a holistic view", *Future Generation Computer Systems*, 107, 2020, Pp. 622, 642.
[224]M. Huth, 'From Risk Management To Risk Engineering: Challenges In Future ICT Systems', in (eds.), E. Griffor, *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems*, Cambridge, MA: Syngress, 2017, Pp. 131, 169.
[225]S.Jasper and J. Wirtz, "Cyber Security", in (eds.), R. Dover et al., *The Palgrave Handbook of Security, Risk and Intelligence*, Palgrave Macmillan: London,, 2017, p, 158.
[226]R. Kissel , *Glossary of Key Information Security Terms: NISTIR 7298 Revision 2*, National Institute of Standards and Technology (NIST): Gaithersburg, MD, July 3, 2019, p. 57.
[227]L. Fichtner, "*What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches*", Internet Policy Review, 7(2), 2018, p. 1.
[228] Check Point, 2020 *Cyber Security Report(PDF)*, Check Point Software Technologies Ltd., www.ntsc.org, Pp. 5, 56, 60.
[229]Deloitte, *Covid-19's Impact on Cyber Security* PDF, www2. Deloitte.com, March 2020.
[230] Deloitte, *COVID-19 Global Cyber risks: Attack surfaces expand amid return to work* efforts PDF, www2.Delotte.com, Issue 7, May 20, 2020.
[231] N.A Khan et al, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic" DOI: 10.36227/techrxiv.12278792.v1.
[232] Information Systems Audit and Control Association, (ISACA), *State of Enterprise Risk Management 2020*, Schaumburg, IL, : ISACA, 2020 www.isaca.org, Pp. 14, 16, 19.
[233]K. J. Engemann, "Developments in risk security", in (ed.), K. J. Engemann, *The Routledge companion to risk, crisis and security in business*, Routledge: New York, 2018, p. 12.
[234] A. R. Wani, et al., "Analysis and Countermeasures for Security and Privacy Issues in Cloud Computing", in (eds.), P.K. Kapur et al., *System Performance and Management Analytics*, Springer: Singapore, 2019, p. 49.
[235] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey", *Computer Science Review*, 33, 2019, p. 11.
[236] Buyya et al., "A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade", ACM Computing Surveys, Vol. 51, No. 5, Article 105, November 2018, p. 105.5. https://doi.org/10.1145/3241737
[237]K. Chandrasekaran, *Essentials of Cloud Computing*, CRC Press: Boka Raton: London, 2015, p. 344.
[238] I. M. Khalil et al., "Cloud Computing Security", Computers, 3, 2014, p. 6.
[239]A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey", *Journal of Network and Computer Applications*,79, 2017, p. 100.
[240] S. Singh et al., "A Survey of Cloud Computing Security: Issues, Threats, and Slutions", *Journal of Network and Computer Applications*, 75, 2016, p. 204.
[241] N. Subramanian and A. Jeyaraj, "Recent Security Challenges in Cloud Computing", *Computers and Electrical Engineering*, 71(2018), p. 31.
[242] C.B.O.M.E. Moctar and K, Konate, "A Survey of Security Challenges in Cloud Computing*", 978-1-5090-4442-9/17/$31.00_c 2017* IEEE, 2017, p. 847.
[243] Puri et al., "A Review on Cloud Computing*", 978-1-5386-5933-5/19/$31.00_c 2019 IEEE*, 2019, p. 64.
[244] F. Wulf et al., "Information Security Risks, Benefits, and Mitigation Measures in Cloud Sourcing*", 2378-1971/19/$31.00 ©2019 IEEE*, 2019, Pp. .259-62. DOI 10.1109/CBI.2019.00036.
[245] R. Doshi and V. Kute, "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models", *978-1-7281-4142-8/$31.00 ©2020 IEEE*, 2020, Pp. 1-2.
[246] S. Maroc and J. Zhang, "Comparative Analysis of Cloud Security Classifications, Taxonomies, and Ontologies", *ACM ISBN 978-1-4503-7150-6/19/07*, 2019, p. 671 : https://doi.org/10.1145/3349341.3349487
[247]T. Maurer and G. Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace: Washington, DC, 2020, p. 25
[248] B. Grobauer et al., "Understanding Cloud Computing Vulnerabilities", *IEEE Cloud Computing*, May/June 2017, p. 14.
[249] S. Bhowmik, *Cloud Computing*, Cambridge University Press: Cambridge, 2017, p. 272.
[250] K. Dahbur et al., "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", ISWSA '11: Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, 2011, https://doi.org/10.1145/1980822.1980834.
[251] A. Magnusson, Practical Vulnerability Management: A Strategic Approach to Managing Cyber Risk, No Starch Press: SAN Francisco, 2020, p. 4.
[252]D. Kim and M.G. Solomon, *Fundamentals of Information Systems Security*, Jones Bartlett Learning: MA, 2018, p. 253.
[253] Cloud Security Alliance, "CSA Releases New Research - Top Threats to Cloud Computing: Egregious Eleven", 2019.https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/, Retrievedon 23 January, 2021.
[254] H. Tabrizchi and M.K. Rafsanjani, "A Survey on Security Challenges in Cloud Computing:, Issues, Threats, and Solutions", The Journal of Supercomputing, 76, 2020, Pp. 9521-26.
[255] M. Ahmed and A.T. Litchfield, "Taxonomy for Identification of Security Issues in Cloud Computing Environments", *Journal of Computer Information Systems*, 58(1), 2018, Pp. 83, 86.
[256] D. Catteddu and G. Hogben (eds.), *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, ENISA (European Network and Information Security Agency) ,http://www.enisa.europa.eu/, 2009, pp. 23-64.
[257]ENISA, Benefits, risks and recommendations for information security, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment, 2012, Accessed on 17 August, 2020, pp. 17-49.
[258] V. Malik and S. Singh, "Cloud, Big Data &IoT: Risk Management", *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con), India, 14th -16th Feb 2019*, 978-1-7281-0211-5/19/$31.00 2019 ©IEEE, Pp. 58-9.
[259]C. Belberguiet et al., "Cloud Computing: Overview and Risk Identification Based on Classification by Type" m (eds.), M. Zbakh et al., *Cloud Computing and Big Data: Technologies, Applications and Security*, Springer Nature: Switzerland AG, 2019, Pp. 29-32.
[260] F. Liu et al., *NIST Cloud Computing Reference Architecture: NIST SP 500-292*, NIST: Gaithersburg, MD, 2011, p. 20.
[261] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems*, 28, 2012, p. 586-7

[262]T. Maurer and G. Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, Washington, DC, Pp. 4, 28, 30-31.
[263] S. Cadzow, "Overcoming Fear of the Threat Model", in (ed.), T. Tryfonas, Human Aspects of Security, Privacy and Trust", Springer Nature: Cham, Switzerland, 2017, Pp. 14-5,18.
[264] M. Goman, "Current State of IT Risk Analysis in Management Frameworks: Is It Enough?",2019 60th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), 2019. DOI**:** 10.1109/ITMS47855.2019.8940653.
[265] I. Agrafiotis et al., "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", *Journal of Cybersecurity*, 2018, Pp. 2- 3, 7-8. DOI: 10.1093/cybsec/tyy006.
[266] M.Schuilenburg, *The Securitization of Society: Crime, Risk, and Social Order*, New York University Press: New York, 2015, p. 23.
[267]Hitachy Systems Security, "Why Do A Cloud Security Assessment?", 10 January 2020, https://hitachi-systems-security.com/why-do-a-cloud-security-assessment/. Retrieved on 12 December, 2021.
[268] T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation*", European Journal of Operational Research*, 253(1), 2016, Pp. 1–13.
[269] M. Medhioub and T-H Kim, "Adaptive Risk Management Framework for Cloud Computing", *2017 IEEE 31st International Conference on Advanced Information Networking and Applications*,2017, pp1154-61, DOI: 10.1109/AINA.2017.143.
[270] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland, 2020, pp. 1-5, doi: 10.1109/CyberSA49311.2020.9139638.
[271]S. J. Lincke, "Integrating Ethics and Risk Management",*2016 4th International Symposium on Digital Forensic and Security (ISDFS)*, Little Rock, AR, USA, 2016, pp. 78-83, doi: 10.1109/ISDFS.2016.7473522.
[272]M. Iorga, and A. Karmel, **"**Managing Risk in a Cloud Ecosystem", *IEEE Cloud Computing*, 2(6), 2015, Pp. 51-57.
[273] A. O. Akande et al., "Management Issues with Cloud Computing", ICCC '13: Proceedings of the Second International Conference on Innovative Computing and Cloud Computing, December 1–2, 2013, Wuhan: China, 2013 ACM 978-1-4503-2119-8/10/06, p. 123.
[274] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security",2010 IEEE 3rd International Conference on Cloud Computing, *Miami, FL, USA, 2010*, Pp. 280-288, doi: 10.1109/CLOUD.2010.22.
[275] S. Tanimoto et al., "Risk Management on the Security Problem in Cloud Computing", "Risk Management on the Security Problem in Cloud Computing," *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, Jeju, Korea (South), 2011, Pp. 147-152, doi: 10.1109/CNSI.2011.82.
[276] J.O. Fitó et al., "Toward business-driven risk management for Cloud computing*",*2010 International Conference on Network and Service Management, *Niagara Falls, ON, Canada, 2010*, Pp. 238-24. DOI: 10.1109/CNSM.2010.5691291.
[277] X. Zhang et al., "Information Security Risk Management Framework for the Cloud Computing Environments*",*2010 10th IEEE International Conference on Computer and Information Technology, *Bradford, UK, 2010*, Pp. 1328-1334, doi: 10.1109/CIT.2010.501.
[278] M. Almorsy et al., "Collaboration-Based Cloud Computing Security Management Framework," *2011 IEEE 4th International Conference on Cloud Computing*, Washington, DC, USA, 2011, Pp. 364-71. DOI: 10.1109/CLOUD.2011.9.
[279] F. Xie et al, "A Risk Management Framework For Cloud Computing", *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, Hangzhou, China, 2012, Pp. 476-480, doi: 10.1109/CCIS.2012.6664451.
[280]Albakri et al, "Security risk assessment framework for cloud computing environments", *Security and Communication Networks*, 7(11), 2014, Pp. 2114-24, https://doi.org/10.1002/sec.923.
[281] K. Djemame et al., 2011, "A risk assessment framework and software toolkit for cloud service ecosystems", In 2nd International Conference on Cloud Computing, GRIDs, and Virtualization, Citeseer, 2011, Pp. 119-26.
[282] O. Akinrolabu et al., "Cyber risk assessment in cloud provider environments: Current models and future needs", *Computers & Security* 87, 101600, 2019, https://doi.org/10.1016/j.cose.2019.101600, Pp. 15-6.
[283] A.S. Sendi and M. Cheriet., "Cloud Computing: A RISK Assessment Model", 2014 IEEE International Conference on Cloud Engineering, *Boston, MA, USA*, 2014, Pp. 147-152. Doi: 10.1109/IC2E.2014.17.
[284] E. Cayirci et al., "A Cloud Adoption Risk Assessment Model", *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, London, UK, 2014, Pp. 908-13. Doi: 10.1109/UCC.2014.148.
[285] E. Cayirici, et al., "A risk assessment model for selecting cloud service providers", *Journal of Cloud Computing:* Advances, Systems and Applications, 5(14), 2016, Pp. 1-12. https://doi.org/10.1186/s13677-016-0064-x
[286] S. Drissi and H. Medromi, "Toward A Risk Assessment Model Based On Multi-Agent System For Cloud Consumer", *International Journal of Computer and Information Engineering*, 8 (6), Pp. 1001-1005, 2014. ISNI:0000000091950263
[287] C. Mellon et al., "Operationally Critical Threat, Asset, and Vulnerability Evaluation (Octave),"Carnegie
Mellon University, Software Engineering Institute: Pittsburgh, PA , June 1998.
[288] Method Harmonized Risk Analysis (MEHARI), *Principles and Mechanisms* CLUSIF, issue 3, October 2004.
[289]Mannane et al., "Survey: Risk Assessment Models for Cloud Computing-Evaluation Criteria" ,2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 979-15386-1115-0/1, **IEEE *Xplore 2018.*** DOI**:** 10.1109/CloudTech.2017.8284712
[290]R. Latif, et al., "Cloud computing risk assessment: a systematic literature review", *Future Information Technology:FutureTech*, 276, 2013, Springer, p. 3.
[291] RSA, *Digital Risk Report, 2020*, Dell Inc.: Bedford, Massachusetts, 2020, p. 5.
[292]S. Morris, "Cloud Computing Tops List of Emerging Risks", September 2018. https://www.gartner.com/smarterwithgartner/cloud-computing-tops-list-of-emerging-risks/. Retrieved on 07 August, 2020.
[293]D. Rotolo et al., 'What is an emerging technology?' *Research Policy*, 44, 2015, p. 1828.
[294]E. Brocal et al., "Emerging Risk Management in Industry 4.0: An Approach to Improve Organizational and Human Performance in the Complex Systems", *Complexity*, 2019, Article ID 2089763, 2019, p. 3. DOI: https://doi.org/10.1155/2019/2089763].
[295]P .Denys, "Efficiency of Risk Assessment Methods", *TCSET'2006, February 28-March 4, 2006, Lviv-Slavsko, Ukraine*, 2006, p. 353.
[296] A. Tchernykh et al., "Towards Understanding Uncertainty in Cloud Computing Resource Provisioning", *Procedia Computer Science*, 51, 2015, Pp.1774-5.
[297]H. Mezni et al., "The Uncertain Cloud: State of the Art and Research Challenges", *International Journal of Approximate Reasoning*,103, 2018, Pp.141-2.
[298]M. Al-Ruithe et al., "Key Dimensions for Cloud Data Governance", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, DOI 10.1109/FiCloud.2016.60, 2016, Pp. 379,384.
[299]R. Haymond, "Why cloud governance is important", https://www.lucidchart.com/blog/cloud-governance-framework.Retrieved on 16 January on 2021.
[300]B.Price,"4 Reasons Why Cloud Governance Matters", https://www.cloudtamer.io/4-reasons-why-cloud-governance-matters/, 2018. Retrieved on16 January, 2021.
[301]M. Al-Ruithe et al., "Data Governance Taxonomy: Cloud versus Non-Cloud", *Sustainability*, 10, 95, doi:10.3390/su10010095, 2018, Pp. 2-3, 6-7.

[302]M. Al-Ruithe et al., "A systematic literature review of data governance and cloud data governance", *Personal and Ubiquitous Computing*, 23, 2019, p. 854.
[303]https://www.google.com/search?ei=T787YMWjKZPA3LUPxIu9iA4&q=what+is+the+projection+of+the+big+data+accumulation+in+2020&oq=what+is+the+projection+of+the+big+data+accumulation+in+2020&gs_lcp=Cgdnd3Mtd2l6EAw6FAgAELADEIoDELcDENQDEOUCEIsDOhEIABCwAxCKAxC3AxDlAhCLA1CaswFYnJACYImlAmgEcAJ4AIAB-QGIAYwXkgEGMC4yMC4xmAEAoAEBqgEHZ3dzLXdpesgBCrgBAsABAQ&sclient=gws-wiz&ved=0ahUKEwiFh7bf-ozvAhUTILcAHcRFD-EQ4dUDCAw. Retrieved on 18 January 2021.
[304] R. Abraham et al, "Data governance: A conceptual framework, structured review, and research agenda", *International Journal of Information Management*, 49, 2019, p. 424.
[305] J. Ladley, *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*, London: Academic Press, 2020, pp. 1, 125.
[306]Cloud Standards Customer Council, "Security for Cloud Computing Ten Steps to Ensure Success: Version 3.0", *Cloud Standards Customer Council* , 2017, Pp. 35-7. www.omg.org.
[307M. O. Alassafi et al., "Security in Organisations: Governance, Risks and vulnerabilities in Moving to the Cloud", in (eds.), V. Chang et al., *Enterprise Security*, Cham Switzerland: Springer, 2017 Pp. 248, 254**.**
[308] J. Kaplan et al., "Protecting information in the Cloud", Mckinsey & Company,2012, p.18. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/protecting-information-in-the-cloud.
[309] J. S. Lim et al, "Exploring the Relationship between Organizational Culture and Information Security Culture", Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2017, http://ro.ecu.edu.au/ism/12, 2017, Pp.88, 93.
[310] *N. Sultan and S. van de Bunt-Kokhuis*, "Organisational culture and cloud computing: coping with a disruptive innovation", *Technology Analysis & Strategic Management*, 24(2), Pp. 173, 176.
[311] H. W. Glaspie and W. Karwowski, "Human Factors in Information Security Culture: A Literature Review", in (eds.).D. Nicholson, *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17–21, 2017*, Springer: Switzerland, 2018, Pp. 269-70.
[312] I. Corradini and E. Nardelli, "Building Organizational Risk Culture in Cyber Security: The Role of Human Factors", in (eds.), T.J. Ahram and D. Nicholson, *Advances in Human Factors in Cybersecurity*, Springer Nature: Cham, Switzerland, 2019, Pp. 193-4.
[313] KPMG, Technology Risks in the light of Covid-19: Performing a rapid technology impact assessment, May 15, 2020, Pp.2-3, www.kpmg.com. Retrieved 18 December, 2020.
[314] W. Stallings and L. Brown, *Computer Security: Principles And Practice***,** Pearson Education Limited, *Brown: Essex 2015*, p. 36
[315]D. W. Roberts, "Security Management – The Process", in (eds.), B. Preneel and V. Rijmen, *State of the art in applied cryptography: Course on Computer Security and Industrial Cryptography, Leuven, Belgium, June 3-6, 1997, Revised Lectures*, Springer: Berlin, 1998, p. 374.
[316] B. De Decker, "Introduction to Computer Security", in (eds.), B. Preneel and V.Rijmen, *State of the art in applied cryptography: Course on Computer Security and Industrial Cryptography Leuven, Belgium, June 3-6, 1997,Revised Lectures*, Springer: Berlin, 1998,p. 381.
[317] A. Elliott, "Beck's Sociology of Risk: A Critical Assessment", *Sociology*, 36(2), 2002, Pp.297, 305.
[318] B. M. Ayyub, *Risk Analysis in Engineering and Economics*, CRC Press: Boka Raton, p. 33.
[319] M. J. Williams, "(In) Security Studies, Reflexive Modernization and the Risk Society", *Cooperation and Conflict*, 43(1), 2008, p. 67.
[320]H. S. Gunawi et al, "Why Does the Cloud Stop Computing? *Lessons from Hundreds of Service Outages*", *ACM Symposium on Cloud Computing*, 2016, Pp.1, 12. DOI: http://dx.doi.org/10.1145/2987550.2987583.
[321]E. Krahmann, "Beck and beyond: selling security in the world risk society", Review *of International Studies*, 37 2011, p. 350, 357-8, 360, 362.
[322] S. Srinivasan, *Cloud Computing Basics*, Springer: New York, 2014, p.101.
[323] Gartner, Newsroom Press Release, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020", https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020,Retrieved on 23 January 2021.
[324]Gartner, "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018", ,https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018. Retrieved on 20December 2021.
[325]G. Elena, "Risk Perception and Cloud Computing Security", www.dcs.gla.ac.uk. Retrieved on 08 January 2021.
[326] P. van Schaik et al., "Risk as affect: The affect heuristic in cybersecurity", *Computers & Security*, 90, 2020, *101651*, p. 1.
[327]A. Burgess, "Individualization revisited: global family developments, uncertainty and risk", *Journal of Risk Research*, 21(1), 2018, p. 83.
[328] K. Renaud et al., "Is the responsibilization of the cyber security risk reasonable and judicious?", *Computers& Security*, 78, 2 018, Pp.199, 209.
[329]M. Smith, "Risk Society and Ethical Responsibility", *Sociology*, 39(3), 2005, p.545.
[330] M. Gross, "Risk as zombie category: Ulrich Beck's unfinished project of the 'non-knowledge' society", *Security Dialogue*, 47(5),2016, p.390.
[331] P. Stankiewicz, "Invisible Risk: The Social Construction of Security", *Polish Sociological Review*, 161, 2008, p.65.
[332] U. Beck, "Living In the Risk Society" *Journalism Studies*, 7(2), 2006, p. 345.
[333] S. Jones et al., "Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies", *Information Systems Frontiers*, 21, 2019, Pp. 359-60,364.
[334] G. Mythen, "Reappraising the Risk Society Thesis: Telescopic sight or Myopic Vision", *Current Sociology*, 55(6), Pp.793-813.
[335] L. M. Vaquero et al., "A Break in the Clouds: Towards a Cloud Definition", *ACM SIGCOMM Computer Communication Review*, 39(1), 2009, Pp. 50-55.
[336] J. Voas and J. Zhang, "Cloud Computing: New Wine or Just a New Bottle", *IT Professional*, 11, no. 2, 2009, Pp.15–7.
[337] R. Grossman, "The case for cloud computing". *IT Professional*,11(2), 2009, Pp. 23–7.
[338]S. Logesswari et al., "A Study on Cloud Computing Challenges and Its Mitigations", Matrials Today:Proceedings, , https://doi.org/10.1016/j.matpr.2020.10.655, p. 5.
[339] Maniah et al., "A Systematic Literature: Risk Analysis in Cloud Migration", *Journal of King SAUD University –Computer and Information Sciences*,doi: https://doi.org/10.1016/j.jksuci.2021.01.008, p.1.
[340] G. S Pandi (Jain) et al., "Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation", *Procedia Computer Science*, 167, 2020, p. 171.
[341]B. Varghese and R. Buyya, "Next Generation Cloud Computing: New Trends and Research Direction", *Future Generation Computer Systems*, 79, 2018, Pp. 849-61.
[342]N. A. el Ata and R. Schmandt, *The Tyranny of Uncertainty*: *A New Framework to Predict, Remediate and Monitor Risk*, 2016, Pp. ix, 13.

[343] A. Burgess et al., "Considering risk: placing the work of Ulrich Beck in context", *Journal of Risk Research*, 21(1), p. 3. DOI:10.1080/13669877.2017.1383075.
[344]M. Arias-Maldonado, "COVID-19 as a Global Risk: Confronting the Ambivalences of a Socionatural Threat",*Societies* 10 (92), 2020, p. 13.Doi:10.3390/soc10040092