IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# THREAT AND ASSET IDENTIFICATION THROUGH IISRA METHODOLOGY

**Keerti Dixit, Dr. Umesh Kumar Singh, Dr. Bhupendra Kumar Pandya**

**Institute of Computer Science, Vikram University, Ujjain**

**Abstract:** Information systems are regularly susceptible to a wide range of threats that can result in a wide range of harms and potentially catastrophic economic losses. Little losses to the total destruction of an information system are examples of information security risks. Threats can have a wide range of effects; some may compromise the integrity or confidentiality of data, whereas others could reduce a system's availability. Organizations are currently having difficulty identifying the threats to their information assets and figuring out how to get the tools they need to address them, which is a challenge. In this research paper we have proposed an IISRA methodology for identifying an organization's assets and threats. In order to assist enterprises in putting their information security strategy into practice, we have also developed taxonomy for threat categorization.

**Keywords:** Information Security Risk Assessment, Threat Categorization, Threat, Asset

## 1. INTRODUCTION

Organizations are more susceptible to numerous risks as a result of the advancement of information and communication technologies and the expansion of Internet accessibility. In truth, cyber threats and the destruction they do can access their information. Risks can emerge from a variety of places, including employee behaviour or hacking attacks. Because a large portion of damages result through smaller-scale security events that led to an overestimate of the risk to the security of information systems [9], it is typically difficult to pinpoint the financial losses brought on by security flaws [1-8]. Hence, managers must be aware of dangers that affect their assets and analyze their impact in order to decide what has to be done to prevent assaults by choosing the proper actions. Flaws in a system that an intruder could use to cause severe effects are known as vulnerabilities. A threat may express itself as a malicious attacker using a specific penetration approach to exploit weaknesses in a system [9, 10]. The possibility of major financial damage to companies is real. Based on the 11th Annual Computer Crime and Security Study [11], viruses, illegal access, theft of laptop or mobile hardware, and theft of confidential information account for 74.3% of massive losses. In fact, a study by McCue in [12] shows that

while 90% of security procedures are directed at external threats, 70% of fraud is committed by insiders as opposed to foreign criminals. In order to identify these threats and safeguard the information security assets beforehand, threat sources and specific system components that may be impacted must be understood [9, 10].

## 2. INTEGRATED INFORMATION SECURITY RISK ASSESSMENT (IISRA) METHODOLOGY

We have developed IISRA methodology that clearly defines secure risk assessment procedure in order to meet the research purpose. The methodology has been built makes it possible to address organizational security concerns in a well-organized way. IISRA's goal is to put in place the right measurement to reduce or eliminate the effects that various security related threats and vulnerabilities could have on organization. As a result, IISRA carries out six phase actions to strengthen methodology and offer a practical approach that can be applied in an organization's computing environment.

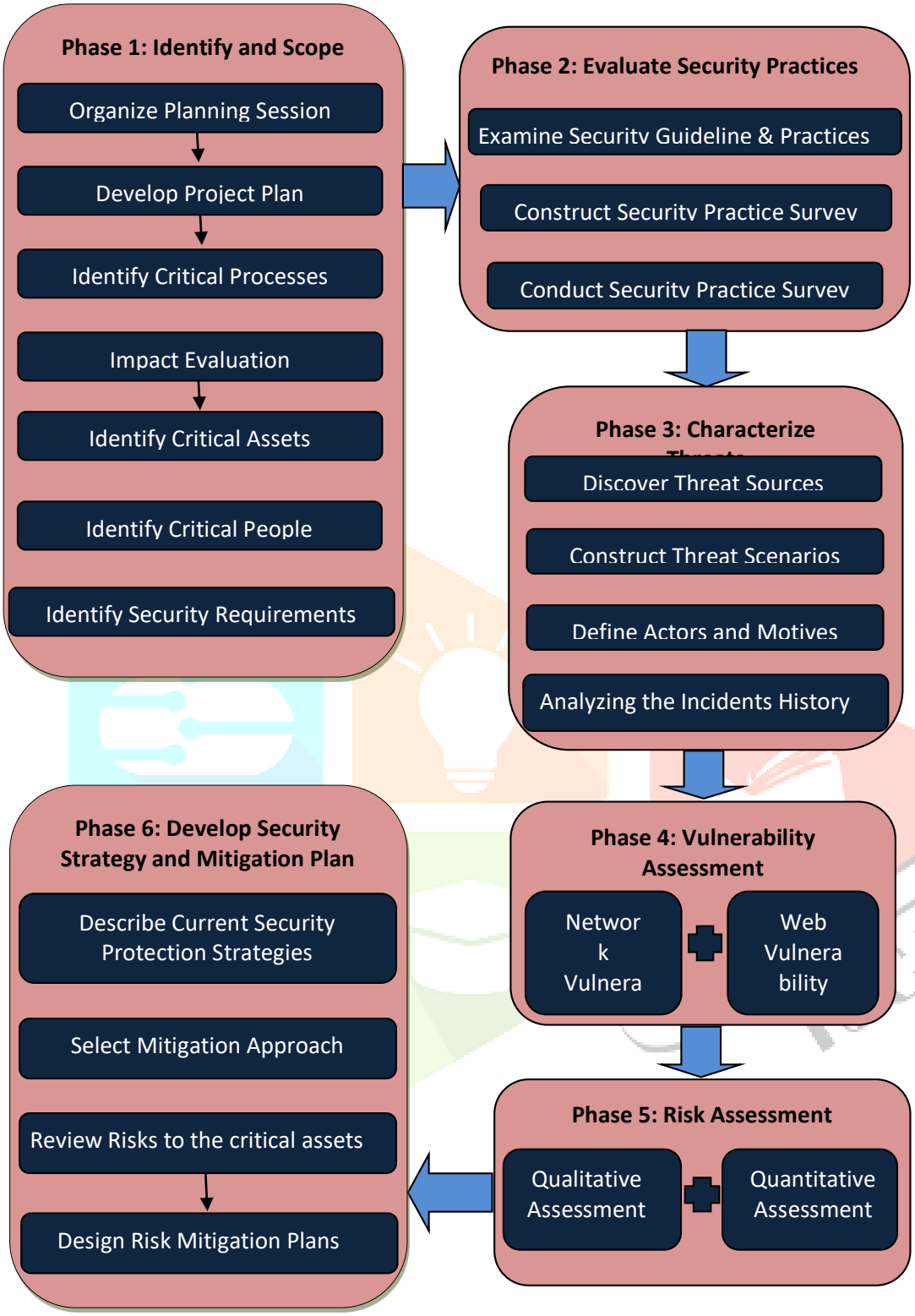


**Figure 1: Phases of Integrated Information Security Risk Assessment (IISRA) Methodology**

## 3. ASSET IDENTIFICATION

Asset identification is a critical component of information security risk assessment. It involves identifying all the assets that need to be protected within an organization, including hardware, software, data, and personnel.

The first step in asset identification is to create an inventory of all the assets within the organization. This inventory should include all hardware, such as servers, workstations, laptops, mobile devices, and networking equipment. It should also include all software applications, databases, and data storage devices. Additionally, it should include all the data assets that the organization stores, including customer data, financial data, and intellectual property.

Once the inventory is complete, the organization should categorize the assets by their importance to the organization's mission and their sensitivity. This categorization will help the organization to prioritize its security efforts and allocate resources to protect the most important and sensitive assets.

The asset identification process should also consider the personnel who have access to the assets, as well as the physical and environmental factors that can affect the assets' security. This includes physical access controls, such as locks and security cameras, and environmental controls, such as temperature and humidity controls.

Overall, asset identification is a crucial first step in information security risk assessment, as it provides the foundation for identifying and assessing risks to the organization's critical assets.

## 4. ASSET CATEGORIZATION

Asset categorization is the process of grouping assets based on their criticality, sensitivity, and importance to an organization's operations. The goal of asset categorization is to prioritize the organization's security efforts by focusing on the most important and sensitive assets.

There are several ways to categorize assets, but IISRA uses a three-tiered approach:

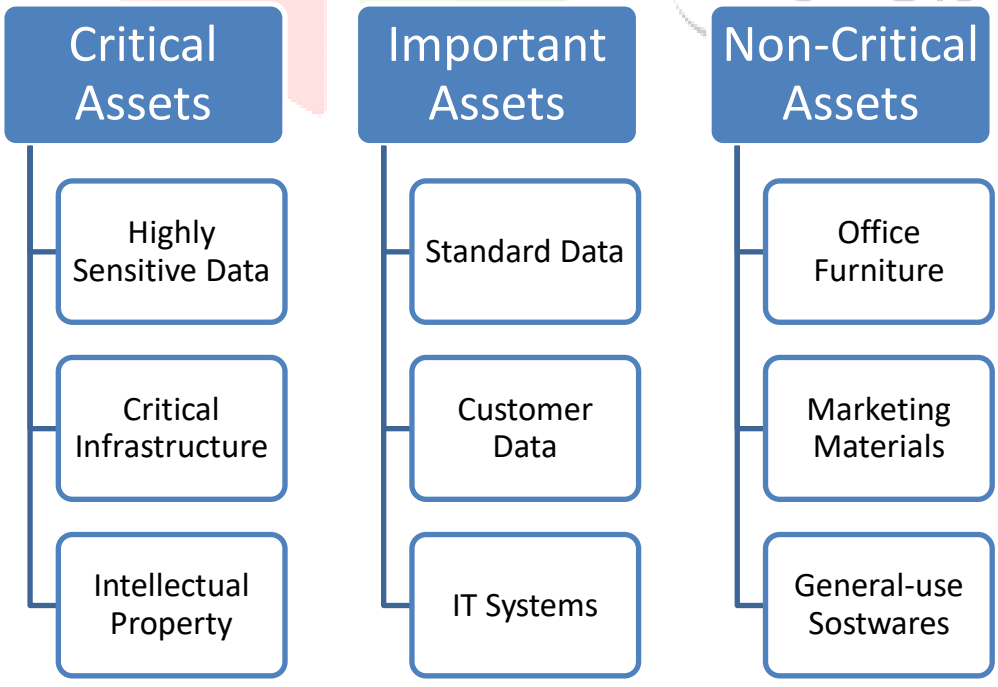


**Figure 2: Asset Categorization through IISRA Methodology**

**Critical Assets:** These are assets that are essential to the organization's mission and would have a severe impact if they were compromised. Examples of critical assets include highly sensitive data, critical infrastructure, and intellectual property.

**Important Assets:** These are assets that are important to the organization's operations, but not essential. Examples of important assets include standard data, customer information, and IT systems that support business processes.

**Non-Critical Assets:** These are assets that are not directly related to the organization's mission or operations, but still have some value. Examples of non-critical assets include office furniture, marketing materials, and general-use software.

Overall, asset categorization is a critical component of information security risk management. By identifying and prioritizing assets, organizations can allocate resources and implement security controls to protect their most critical and sensitive information.

## 5. THREAT IDENTIFICATION

Threat identification is the process of identifying potential sources of harm to an organization's assets, including hardware, software, data, and personnel. Threat identification is a critical component of information security risk management because it enables organizations to identify the most significant security risks and implement appropriate safeguards to mitigate those risks.

The process of threat identification through IISRA involves following steps:

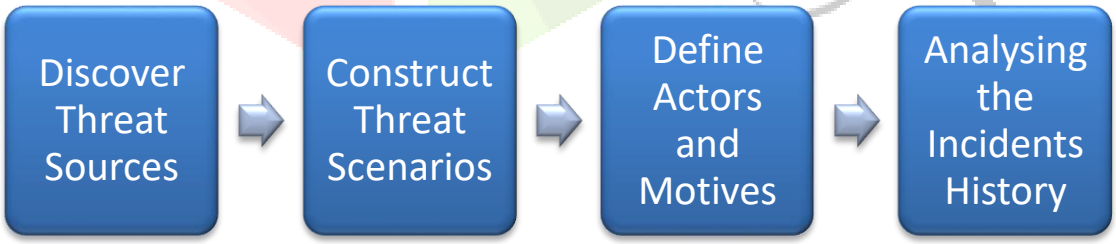


**Figure 3: IISRA Threat Identification Process**

**Discover Threat Sources:** These sources include external threats, such as hackers and cybercriminals, as well as internal threats, such as disgruntled employees or accidental actions. According to each important asset's use in a particular company, a unique threat profile can be developed starting with the generic threat profile. Threat scenarios can be identified by the connected asset, the individuals who might break the security, the way they gain access, and their motivation. The threat's final effect occurs when one or more of an asset's security requirements are broken, leading to disclosure, modification, destruction, or interruption. The participants in the

information risk assessment must take into account the specific threat profiles for each key asset, or piece of information.

**Construct threat scenarios:** Using the categories of threat sources, threats are graphically represented in a structure. Threat profiles differ for each key asset. Throughout the evaluation, every threat scenario must be examined, regardless of its significance, likelihood, or existing defenses.

**Define Actors and Motives:** Since insiders are the main perpetrators of security breaches, both outsiders and insiders are taken into account when identifying the actors. It is important to take into account how they will gain access to the priceless object, whether it be physically or over a network. The motivation of the actor and its advantages are determined.

**Analyzing the Incidents History:** This is done by looking at any objective data that is available, including event data that has been documented.

## 6. THREAT CATEGORIZATION THROUGH IISRA METHODOLOGY

Threat categorization is the process of grouping threats based on their characteristics, potential impact, and likelihood of occurrence. The goal of threat categorization is to prioritize the organization's efforts to mitigate potential threats and allocate resources effectively.

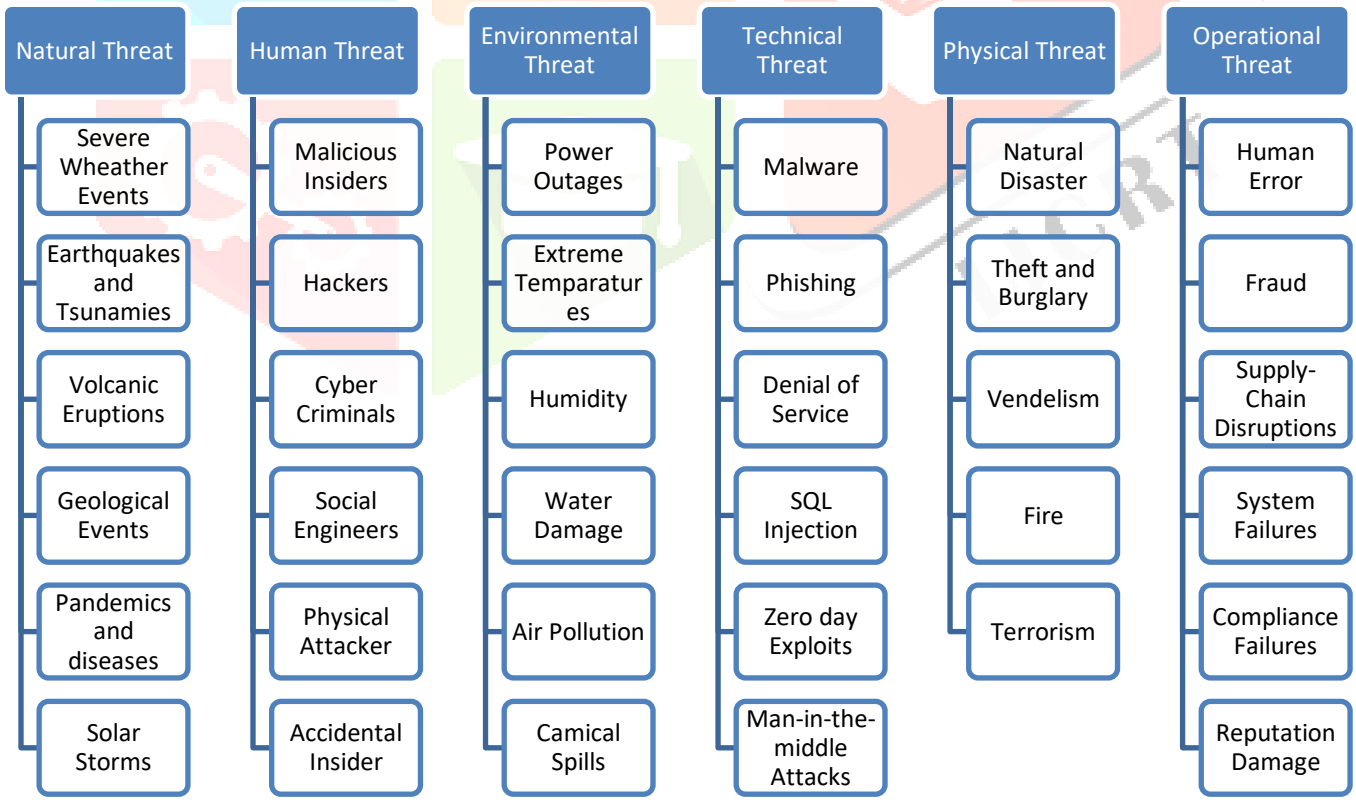


**Figure 4: IISRA Threat Categorization**

**Natural threats:** Natural threats are risks that occur due to natural phenomena or events that are beyond human control. Here are some examples of natural threats:

Severe weather events - This includes hurricanes, tornadoes, floods, and wildfires.

Earthquakes and tsunamis - These natural disasters can cause significant damage to buildings, infrastructure, and other assets.

Volcanic eruptions - These can cause ash clouds, lava flows, and other hazards.

Geological events - Such as landslides and sinkholes that can cause property damage, injury, and loss of life.

Pandemics and diseases - These are infectious diseases that can rapidly spread and cause illness and death.

Solar storms - These can cause electromagnetic interference and disrupt communication systems, including satellites, power grids, and other electronic systems.

Natural threats can have a severe impact on an organization's operations and assets. Therefore, it is crucial to include natural threats in the risk assessment process and develop appropriate measures to mitigate potential damage and losses. Organizations can take proactive steps to prepare for natural disasters, such as implementing emergency response plans, establishing disaster recovery and business continuity plans, and investing in appropriate infrastructure and equipment to minimize the impact of natural threats.

**Human threats:** Human threats are risks that are caused by people, either intentionally or unintentionally. Here are some examples of human threats:

Malicious insiders - These are employees, contractors, or partners who intentionally cause harm to the organization by stealing data, sabotaging systems, or other malicious activities.

Hackers - These are individuals or groups who use various techniques, such as phishing, social engineering, and malware to gain unauthorized access to an organization's systems or data.

Cybercriminals - These are individuals or groups who use computer systems to commit crimes, such as stealing sensitive data, ransomware attacks, or other malicious activities.

Social engineers - These are individuals who manipulate people to obtain sensitive information or access to an organization's systems or data.

Physical attackers - These are individuals who attempt to gain unauthorized access to an organization's facilities, systems, or data by physical means, such as breaking into a building or stealing equipment.

Accidental insiders - These are employees or other insiders who unintentionally cause harm to the organization by mistake, such as sending sensitive information to the wrong recipient or clicking on a phishing link.

Human threats can have a significant impact on an organization's security and can result in financial losses, reputational damage, and legal liabilities. Therefore, it is crucial to include human threats in the risk assessment process and develop appropriate measures to mitigate potential risks. Organizations can take proactive steps to prevent human threats, such as implementing security awareness training, establishing access controls, and implementing security policies and procedures.

**Environmental threats:** Environmental threats are risks that result from environmental factors or events that are beyond human control. Here are some examples of environmental threats:

Power outages - These can occur due to severe weather events, equipment failures, or other causes and can disrupt business operations.

Extreme temperatures - These can cause damage to equipment, affect worker productivity and comfort, and increase the risk of fire.

Humidity - High humidity can cause damage to equipment and electronics, and mold growth, which can be a health hazard.

Water damage - This can occur due to flooding, leaks, or other causes and can cause significant damage to property and equipment.

Air pollution - Poor air quality can impact the health of workers and cause damage to equipment and materials.

Chemical spills - Accidental spills of hazardous chemicals can cause health hazards, environmental damage, and property damage.

Environmental threats can have a severe impact on an organization's operations and assets. Therefore, it is crucial to include environmental threats in the risk assessment process and develop appropriate measures to mitigate potential damage and losses. Organizations can take proactive steps to prepare for environmental threats, such as implementing environmental controls, establishing emergency response plans, and investing in appropriate infrastructure and equipment to minimize the impact of environmental threats.

**Technical threats:** Technical threats are risks that result from vulnerabilities in technology systems or infrastructure. Here are some examples of technical threats:

Malware - This is malicious software designed to damage or disrupt computer systems or steal sensitive data.

Phishing - This is a technique used to trick users into divulging sensitive information, such as login credentials or credit card numbers.

Denial of Service (DoS) attacks - These are attacks that flood a network or server with traffic to make it unavailable to users.

SQL injection - This is a technique used to exploit vulnerabilities in web applications by injecting malicious SQL statements.

Zero-day exploits - These are vulnerabilities in software or hardware that are unknown to the vendor and can be exploited by attackers.

Man-in-the-middle attacks - These are attacks where an attacker intercepts communications between two parties and can eavesdrop on or modify the communications.

Technical threats can have a significant impact on an organization's security and can result in financial losses, reputational damage, and legal liabilities. Therefore, it is crucial to include technical threats in the risk assessment process and develop appropriate measures to mitigate potential risks. Organizations can take proactive steps to prevent technical threats, such as implementing firewalls, antivirus software, intrusion detection and prevention systems, and patching systems to fix vulnerabilities.

**Physical threats:** Physical threats are risks that result from physical events or actions that can damage or disrupt an organization's operations, facilities, or assets. Here are some examples of physical threats:

Natural disasters - These can include earthquakes, floods, hurricanes, tornadoes, and wildfires, which can cause significant damage to buildings, infrastructure, and other assets.

Theft and burglary - These are criminal acts that can result in the theft of valuable equipment, data, or other assets.

Vandalism - This is intentional damage to property, such as graffiti or destruction of equipment.

Fire - This can cause significant damage to property and equipment and pose a risk to the safety of employees and visitors.

Power outages - These can occur due to severe weather events or equipment failures and can disrupt business operations.

Terrorism - This is the use of violence or the threat of violence to intimidate or coerce a government or population.

Physical threats can have a severe impact on an organization's operations and assets. Therefore, it is crucial to include physical threats in the risk assessment process and develop appropriate measures to mitigate potential damage and losses. Organizations can take proactive steps to prevent physical threats, such as implementing security measures such as security cameras, access controls, and security personnel, establishing emergency response plans, and investing in appropriate infrastructure and equipment to minimize the impact of physical threats.

**Operational threats:** Operational threats are risks that result from internal processes, procedures, or human errors that can cause damage to an organization's operations or reputation. Here are some examples of operational threats:

Human error - This can include accidental deletion of data, misconfigured systems, or unintended disclosure of sensitive information.

Fraud - This can include embezzlement, theft, or other financial crimes committed by employees or external parties.

Supply chain disruptions - These can result from the failure of suppliers to deliver goods or services, causing delays or disruptions in operations.

System failures - These can result from equipment failures, software bugs, or other technical issues that can disrupt operations.

Compliance failures - These can result from failure to comply with regulatory requirements or industry standards, resulting in legal or financial penalties.

Reputation damage - This can result from negative publicity, social media backlash, or other factors that can harm an organization's image or brand.

Operational threats can have a significant impact on an organization's operations, reputation, and financial health. Therefore, it is crucial to include operational threats in the risk assessment process and develop appropriate measures to mitigate potential risks. Organizations can take proactive steps to prevent operational threats, such as implementing effective training programs, establishing strict security protocols and procedures, and conducting regular audits to identify and mitigate potential vulnerabilities.

## 7. CONCLUSION

In this research paper we have proposed an Integrated Information Security Risk Assessment (IISRA) Methodology for information security risk assessment. We have clearly described the IISRA asset and threat identification process. Further, we have provided a categorization of threats. By categorizing threats, organizations can prioritize their efforts to mitigate potential threats and allocate resources more effectively. This approach can help organizations to focus their security efforts on the most significant threats, reducing the overall risk to the organization.

## 8. REFERENCES

[1] Keerti Dixit, “Information Security Risk Assessment in Higher Educational Institutions-Issues and Challenges” presented in 36th M.P. Young Scientist Congress, March 23 - 26, 2021

[2] K. Dixit, U. K. Singh, B. K. Pandya, “Comparative Framework for Information Security Risk Assessment Model”, ICCIDS-2022 International Conference on Computational and Intelligent Data Science (Elsevier) 21 May 2022.

[3] Howard JD. An Analysis Of Security Incidents On The Internet 1989 – 1995. Doctoral Dissertation, Carnegie Mellon University Pittsburgh, PA, USA; 1998.

[4] Farahmand F, Navathe SB, Sharp GP, Enslow PH. A Management Perspective on Risk of Security Threats to Information Systems, Information Technology and Management archive; 2005;6: 202-225

[5] Shiu S, Baldwin A, Beres Y, Mont MC, Duggan G. Economic methods and decision making by security professionals. The Tenth Workshop on the Economics of Information Security (WEIS); 2011.

[6] Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A. A cybersecurity model in cloud computing environments. Journal of King Saud University – Computer and Information Sciences; 2012; 1: 63-75.

[7] Jouini M, Ben Arfa Rabai L, Ben Aissa A, Mili A. Towards quantitative measures of Information Security: A Cloud Computing case study. International Journal of Cyber-Security and Digital Forensics (IJCSDF); 2012; 1(3): 265-279.

[8] Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A.. An economic model of security threats for cloud computing systems. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec); 2012. 100-105.

[9] Geric S, Hutinski Z. Information system security threats classifications. Journal of Information and Organizational Sciences; 2007. 31: 51.

[10] Alhabeeb M, Almuhaideb A, Le P, Srinivasan B. Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops: 2010. p. 208-213.

[11] Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI Computer Crime and Security Survey – 2006. 11th Annual CSI/FBI Computer Crime and Security Survey; 2006.

[12] McCue A. Beware the insider security threat, CIO Jury; 2008.