

Course Details

Course Title: Attack, Reporting and Documentation

- **Course Code:** CSF4042B
- **Course Category:** Program Elective - IV

Course Layout

- Introduction to Cybersecurity Attacks, Reporting, and Documentation
- Incident Response Frameworks
- Cybersecurity Policy Documentation
- Cybersecurity and Contracting
- Incident Reporting Templates

Some Basics

- What is CIA in security ?
- What is Social engineering and how it poses threat to security?
- What is MFA ?
- What is firewall ?
- What is an IDS ?

Event vs. Incident

Aspect	Event	Incident
Definition	Any observable occurrence in a system.	An event or series of events causing harm or requiring action.
Nature	Neutral or expected; not necessarily harmful.	Negative or suspicious; often harmful.
Action Required	Typically no action needed.	Requires investigation and remediation.
Frequency	Occurs frequently in daily operations.	Less frequent but more critical.

Introduction to Cybersecurity Attacks, Reporting, and Documentation

➤ **Overview of Cybersecurity Threats and Attacks**

- What are Threats
- What are Attacks
- Attack Vectors and Techniques
- Cyber Kill Chain
- Advantages of Attack Reporting and Documentation

➤ **Importance of Reporting and Documentation**

- Risk Register
- Document Requirements for IT Audits

Cybersecurity Threats

- **Definition:** Potential dangers or vulnerabilities that could be exploited to cause harm to a computer system, network, or data.
- **Nature:** Threats are the possibility of a malicious event occurring. They exist whether or not they are acted upon.
- **Scope:** Encompasses a wide range of potential security issues, including both intentional and unintentional events.
- **Examples:**
 - Malware
 - Phishing
 - Zero-Day Vulnerabilities

Why Study Threats

➤ **Protection of Sensitive Data Loss**

- Cybersecurity threats target your personal information, financial details, or secret business ideas.
- Knowing about threats helps us stop unauthorized access and data breaches.

➤ **Prevention of Financial Loss**

- Cyberattacks like ransomware and phishing can lead to financial losses by stealing money, demanding ransoms, and causing system shutdowns.
- Being aware helps us protect systems and avoid expensive problems.

➤ **Mitigation of Operational Disruption**

- Threats like DDoS attacks can interrupt important business activities.
- Knowing about threats helps systems and networks stay strong and keep the business running smoothly.

Why Study Threats

➤ **Strengthening Incident Response**

- Understanding different threats helps organizations create strong response plans.
- Fast detection and response reduce damage and speed up recovery during a cyber incident.

➤ **Compliance with Legal and Regulatory Standards**

- Many industries must follow cybersecurity rules like GDPR, HIPAA, or ISO/IEC 27001.
- Knowing about threats helps follow rules and avoid fines.

➤ **Protection Against Evolving Threats**

- Cyber threats keep changing, as attackers use new methods and technologies.
- Keeping up with new threats makes sure our defenses stay strong.

Why Study Threats

➤ **Enhancing Personal Security**

- People face threats like identity theft, social engineering, and malware infections.
- Being aware helps people spot and avoid scams, keeping their personal information and devices safe.

➤ **Safeguarding National and Organizational Reputation**

- Cyberattacks can damage the reputation of businesses and governments, causing a loss of trust among stakeholders.
- Taking a proactive approach to cybersecurity shows responsibility and builds trust.

➤ **Encouraging a Security-First Culture**

- Knowing about threats builds a culture of security in organizations.
- Employees are more likely to follow best practices if they understand the risks of not complying or being careless.

Cybersecurity Attacks

- **Definition:** Actions taken by malicious actors to exploit vulnerabilities and execute harm on a computer system, network, or data.
- **Nature:** Attacks are the realization of threats. They involve active efforts to breach security and cause damage.
- **Scope:** Specific incidents where threats are actualized to compromise security.
- **Examples:**
 - Ransomware Attack
 - DDoS Attack
 - SQL Injection Attack

Threats vs. Attacks Key Differences

- **Potential vs. Action:** Threats represent the potential for harm, while attacks are the actions taken to exploit threats.
- **Broad vs. Specific:** Threats can be broad and theoretical, while attacks are specific and concrete instances of exploitation.
- **Preventive vs. Reactive:** Managing threats often involves preventive measures (e.g., securing vulnerabilities), while responding to attacks involves reactive measures (e.g., incident response).

Malware

➤ **Types of Malware**

- Viruses
- Worms
- Trojans

➤ **Infection Methods**

- Email attachments, drive-by downloads, infected software.

➤ **Impacts of Malware**

- Data loss, system downtime, financial loss.

Comparison of Malwares

Feature	Trojans	Viruses	Worms
Dependency	Requires user execution	Requires a host file	Operates independently
Replication	Does not self-replicate	Replicates by attaching to files	Self-replicates across networks
Primary Function	Deceptive access and payloads	File corruption and disruption	Rapid spreading and disruption

Example of know Malwares

- **Conficker/Downup/Downadup and Kido (Detected in Nov 2008)**
 - **Type:** Worm/virus hybrid.
 - **Spread:** Exploited Windows OS vulnerabilities (MS08-067 / CVE-2008-4250) to propagate across networks.
 - **Impact:** In January 2009, an estimated 9 to 15 million systems were estimated to be infected. Could have costed approximately \$9.1 billion to users/Organizations.

Prevention and Mitigation

- Patch Management
- Firewalls and Intrusion Detection Systems (IDS)
- Antivirus Software
- Email Security
- Network Segmentation
- User Awareness Training

Key Characteristics of Phishing

➤ **Deceptive Communication**

- Phishing messages often mimic legitimate sources with logos, language, and design similar to authentic communications.

➤ **Urgency or Fear Tactics**

- Messages often create a sense of urgency, such as warnings about account breaches, unpaid bills, or other emergencies, to prompt immediate action.

➤ **Malicious Links or Attachments**

- Victims are lured to click on links leading to fake websites or open malicious attachments that execute malware.

➤ **Exploitation of Trust**

- Phishing campaigns rely on exploiting human trust and curiosity rather than technical vulnerabilities.

Types of Phishing

- Email Phishing
- Spear Phishing (specific person or group)
- Whaling (specific person or group)
- Smishing (SMS Phishing)
- Vishing (Voice Phishing)
- Clone Phishing (Email is cloned and resend)
- Pharming (Redirect user to fake website)
- Social Media Phishing (Fake accounts used)

Example of Phishing attack

➤ Google Docs Phishing Attack (2017)

- **Type** : Phishing/Worm
- **Spread** : Email, deceptive invitation to edit a Google Doc
- **Method** : Email a subject line stating a contact “has shared a document on Google Docs with you”.
- **Impact** : Approximately 1 million Gmail users received deceptive emails asking them to open a Google Doc, leading to unauthorized access to their email accounts and contacts.

Preventing Phishing Attacks

- Education and Awareness
- Verify Before Acting
- Avoid Clicking Links
- Use Spam Filters
- Enable Multi-Factor Authentication (MFA)
- Regular Software Updates
- Check Website URLs

Key Characteristics of Zero-Day Vulnerabilities

- **Undisclosed**

- The vulnerability is not yet known to the software vendor or security community.

- **Exploitable**

- Attackers can take advantage of the flaw to bypass security measures, compromise systems, or steal data.

- **High Risk**

- Since no patch or fix is available, affected systems are particularly vulnerable to exploitation.

How Zero-Day Exploits Work

- **Discovery**

- The attacker identifies a previously unknown vulnerability.

- **Development**

- The attacker develops an exploit to leverage the vulnerability.

- **Attack**

- The exploit is used in targeted or widespread attacks.

- **Detection**

- Once the exploit is detected, the vulnerability is disclosed to the vendor or public, prompting a response.

Example of Zero-day vulnerabilities

➤ **Log4Shell (2021)**

- **Type** : Zero-day vulnerabilities
- **Affected software** : Apache Log4j (CVE-2021-44228)
- **The Flaw** : By exploiting it, the attacker can easily execute any code from a remote source on the attacked target.
- **Impact** : Potential to affect hundreds of millions of devices and could have costed billions of dollars.

Protecting Against Zero-Day Vulnerabilities

- Use Endpoint Protection
- Adopt Zero Trust Security
- Limit Exposure by using UpToDate software
- Regular Backups
- Vendor Collaboration

Key Characteristics of a Ransomware Attack

- File Encryption
- Ransom Demand
- Payment in Cryptocurrency
- Double or Triple Extortion
- Wide Targets

How Ransomware Attacks Work

- Infection
- Propagation
- File Encryption
- Ransom Note Delivery
- Payment and (Possible) Decryption

Example of Ransomware

- **Ryuk Ransomware (2018–2020)**

- **Type** : Ransomware

- **Entry Point** : phishing campaigns

- **Impact** : Factoring in ransom payments, downtime and recovery, the total average cost

- **Large organizations** : \$5–10 million.

- **Smaller entities** : \$500,000 to \$1 million.

Prevention and Mitigation

- Regular Backups
- Employee Training
- Security Software (Like anti Virus)
- Patch Management
- Network Segmentation
- Incident Response Plan

DDoS Attacks


- **Definition :** Distributed Denial-of-Service (DDoS) attacks overwhelm a target's systems with a flood of traffic, rendering services unavailable.
- **Methods of Attack**
 - **Botnets:** Networks of compromised devices used to launch attacks.
- **Types of DDoS:** Volume-based, protocol attacks, application layer attacks.
- **Impacts:** Service outages, revenue loss, reputational damage.

Example of DDoS Attacks

- **Cloudflare Attack (2022)**
- **Type:** HTTPS Flood Attack
- **Description:**
 - Cloudflare mitigated a **26 million requests per second (RPS)** attack, making it one of the largest recorded application-layer DDoS attacks.
 - The attack was carried out using a botnet of hijacked virtual machines and servers.
- **Impact:** The attack was blocked with no downtime for Cloudflare-protected websites.
- **Lesson:** Application-layer attacks can be devastating without robust anti-DDoS mechanisms in place.

Prevention and Mitigation

- Strengthen Network Infrastructure
- Leverage Anti-DDoS Solutions
- Configure Network Defences
- Monitor and Detect Anomalies
- Strengthen DNS Security



What are Threats
What are Attacks

ATTACK VECTORS
AND TECHNIQUES

Attack Vectors

- **Definition :** An attack vector is a method or pathway used by attackers to gain unauthorized access to a system, network, or device.
- **Key Characteristics of Attack Vectors**
 - **Entry Point:** It's the starting point where the attacker might involve sending a phishing email, exploiting a software vulnerability, or attempting unauthorized access through weak credentials.
 - **Delivery Mechanism:** It involves the tools, techniques, or tactics used to carry out the attack like security flaws such as unpatched software, misconfigured systems, or human error (e.g., clicking on a malicious link) to breach the target.
 - **Objective:** Attack vectors help to escalate privileges, move laterally within a network, or exfiltrate data.

Attack Vectors

➤ Examples of Entry Points:

- **Compromised Credentials:** Weak or stolen usernames and passwords
- **Phishing:** Deceptive emails or messages tricking users into revealing sensitive information
- **Malware:** Malicious software that can infiltrate systems and steal data.
- **Networks:** Open ports, unpatched network devices.
- **Zero-Day Vulnerability:** security flaw in software or hardware that is unknown to the vendor.
- **Software/Applications:** Exploiting flaws or vulnerabilities in software or applications

Attack Vectors

➤ Examples of Entry Points:

- **Devices:** Outdated software, insecure configurations
- **Third-party Vendors:** Supply chain vulnerabilities, compromised partners
- **Web Application Vulnerabilities:** Attackers exploit flaws like SQL injection or cross-site scripting (XSS) in a web application
- **Insider Threats:** Employees or associates with malicious intent or negligence.
- **Weak Encryption:** Inadequate encryption methods that expose data during transmission.

Attack Vectors

➤ **Significance of Entry Points in Cyberattacks**

- **Starting Point of the Attack Lifecycle:** Entry points are crucial as they let attackers start their series of steps to infiltrate and compromise systems.
- **Escalation Path:** Once inside, attackers can find more weaknesses, gain higher access, and take more control.
- **Critical to Defences:** Securing entry points is key to stopping attackers from getting in.

Examples

➤ Target Data Breach (2013)

- **Entry Point:** Attackers used stolen credentials from a third-party HVAC vendor to access Target's network.
- **Exploitation:** Once inside, attackers moved within Target's network to access payment systems, stealing data from over 40 million credit and debit cards.
- **Impact :** Significant financial losses, legal consequences, and damage to customer trust, with costs estimated at around \$292 million.
- **Lesson:** A small entry point (third-party vendor access) led to a huge breach, highlighting the need to secure all potential access points.

Examples

➤ **SolarWinds Supply Chain Attack (2020)**

- **Entry Point:** Attackers infiltrated SolarWinds' software supply chain, inserting a backdoor into the Orion platform.
- **Exploitation:** Organizations that downloaded the compromised updates allowed attackers to access their systems.
- **Impact:** The attack affected numerous organizations, including government agencies and private companies, leading to significant data breaches and security compromises.
- **Lesson:** This attack highlighted the importance of securing software supply chains and the potential widespread impact of such vulnerabilities.

Example

➤ The Mirai Botnet Attack (2016)

- **Entry Point:** The Mirai malware exploited weak or default credentials on IoT devices (e.g., IP cameras, routers).
- **Exploitation:** The Mirai malware scanned internet for IoT devices with open Telnet or SSH ports and created Botnet
- **Impact:** Dyn a major DNS provider was targeted resulting in disruption to websites like Twitter, Netflix, Reddit, and GitHub.
- **Lesson:** IoT devices must require unique and complex passwords upon setup. Disable default or hardcoded credentials in devices.

Attack Technique

- **Reconnaissance :**

- Gaining information about the target.

- **Techniques:**

- Passive: Monitoring open sources (e.g., social media, public websites)

- Active: Scanning networks or probing systems for vulnerabilities.

- **Exploitation:**

- Taking advantage of vulnerabilities to gain control or unauthorized access.

- **Techniques:**

- Code injection (SQL Injection, XSS)

- Exploiting unpatched software

Attack Technique..

- **Privilege Escalation**

- Gaining higher access rights within a system after initial access.

- **Techniques**

- Exploiting misconfigured permissions
 - Using credential dumping tools

- **Lateral Movement**

- Moving within the network to identify and compromise additional systems.

- **Techniques**

- Exploiting trust relationships between systems
 - Leveraging compromised credentials

Attack Technique..

- **Command and Control (C2)**

- Maintaining communication between the attacker and the compromised system.

- **Techniques:**

- Encrypted channels

- Using legitimate services (e.g., cloud platforms) to evade detection

- **Data Exfiltration**

- Transferring stolen data out of the organization.

- **Techniques:**

- Encrypted file transfers

- Steganography (hiding data in images or files)

Attack Technique..

- **Obfuscation and Anti-Forensics**
 - Hiding evidence of an attack or making it harder to trace.
 - **Techniques**
 - Encrypting malware code
 - Deleting logs or disabling monitoring tools

Attack Vectors and Techniques

CYBER KILL CHAIN

Key Features of Modern Cyber Intrusions

- **Characteristic of Modern Day Attacks**
 - SOPHISTICATED
 - WELL-RESOURCED
 - MOTIVATED
- **Advanced Persistent Threats (APT)**
 - Skilfully planned intrusion campaigns

The Evolution of Cyber Defense: The Kill Chain Approach

- Proposed by Lockheed Martin in 2011
- Introduced in a white paper titled
 - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
- Understand and counteract cyber threats systematically
- Helping organizations identify, detect, and disrupt adversaries

Insights from the Cyber Kill Chain

- Defenders goal is to understand the aggressor's actions
- Understanding the aggressor's actions provides intelligence
- Cyber Kill Chain is a 7 Step Model
- Intruders succeed if and only if they move from Steps 1-6 and reach final objective

The 7 Stages of the Cyber Kill Chain

- **Reconnaissance**
- **Weaponization**
- **Delivery**
- **Exploitation**
- **Installation**
- **Command & Control (C2)**
- **Actions On Objectives**

Stage 1 Reconnaissance

Attackers

- Compile Email Lists
- Profile Staff on Social Platforms
- Review press releases, contract awards, conference attendee lists
- Identify Public-Facing Servers

Defenders

- Gather website visitor logs for alerts and history checks.
- Work with web admins to use current browser analytics.
- Create alerts for browsing patterns specific to reconnaissance.
- Focus defences on specific technologies or personnel based on reconnaissance activity.

Stage 2 Weaponization

Attackers

- Get a weaponize in-house or from public/private sources.
- For file-based exploits, choose a 'decoy' document to show the target.
- Choose a backdoor implant and suitable command and control setup for the operation.
- Assign a unique 'mission ID' and embed it in the malware.
- Build the backdoor and arm the payload.

Defenders

- Perform complete malware analysis – examine both the payload and its creation process.
- Create alerts for weaponizer – detect new campaigns and payloads through reused toolkit patterns.
- Review the timeline of malware creation vs. usage. Old malware is 'off the shelf,' while new malware may indicate active, customized operations.
- Gather files and metadata for later analysis.
- Identify common weaponizer artifacts in APT campaigns. Are they widely shared or closely held?

Stage 3 Delivery

Attackers

- Attacker-controlled delivery
 - Target web servers directly
- Attacker Released delivery
 - Malicious email
 - Malware on USB
 - Social media interactions
 - Compromised Website

Defenders

- Review delivery method – understand the source infrastructure.
- Know which servers and people are targeted, their roles, and the available information.
- Guess the adversary's intent based on their targets.
- Use weaponizer artifacts to spot new malicious payloads during Delivery.
- Check the time of day the operation started.
- Gather email and web logs for forensic analysis.

Stage 4 Exploitation

Attackers

- Software, hardware, or human weakness.
- Get or create a zero-day exploit.
- Attacker triggered exploits for server-based vulnerabilities
- Victim triggered exploits
 - Clicking malicious link
 - Open email attachment

Defenders

- Employee training on awareness and email testing
- Train developers in secure coding practices
- Regularly scan for vulnerabilities and perform penetration testing
- Strengthen endpoint security measures
- Audit endpoint processes to trace the exploit's origin

Stage 5 Installation

Attackers

- Webshell is added to the webserver
- Install a backdoor or implant on the victim's device
- Set up persistence by adding services, AutoRun keys, etc
- Some adversaries use 'time stomping' to make malware look like part of the standard OS install

Defenders

- Use Host-based Intrusion Prevention System to alert or block common installation paths like RECYCLER
- Check if the malware needs admin privileges or just user access
- Audit endpoint processes to find unusual file creations
- Get certificates from signed executables.
- Check when the malware was compiled to see if it's old or new

Stage 6 Command & Control (C2)

Attackers

- Set up two-way communication with C2 infrastructure.
- Common C2 channels: web, DNS, and email.
- C2 infrastructure can be owned by attackers or hosted on another victim's network.

Defenders

- ▶ Find C2 infrastructure through detailed malware analysis
- ▶ Network Harding:
 - ▶ Reduce the number of internet access points.
 - ▶ Use proxies for all traffic types (HTTP, DNS).
- ▶ Tailor C2 protocol blocks on web proxies.
- ▶ Block 'none' or 'uncategorized' domains on proxies.
- ▶ Use DNS sinkholing and server poisoning
- ▶ Do open-source research to find new attackers C2 infrastructure.

Stage 7 Actions On Objectives

Attackers

- Collect user credentials
- Privilege escalation
- Internal reconnaissance
- Lateral movement through environment
- Collect and exfiltrate data
- Destroy systems
- Overwrite or corrupt data
- Surreptitiously modify data

Defenders

- Create an incident response plan with executive engagement and a communication strategy.
- Detect data exfiltration, lateral movement, and unauthorized credential use.
- Prompt analyst response to all CKC7 alerts.
- Deploy forensic agents to endpoints for rapid triage.
- Capture network packets to recreate activity.
- Assess damage with subject matter experts.

Target Data Breach

- **Reconnaissance:** Attackers focused on a company that had permission to access Target's network. They collected details about the company's login information.
- **Weaponization:** Attackers created a malware designed to steal payment card information from Target's systems.
- **Delivery:** Spear-phishing emails were sent to the HVAC vendor employees, compromising their systems.
- **Exploitation:** Using stolen credentials, attackers gained access to Target's network.
- **Installation:** Malware was installed on Target's point-of-sale (POS) systems to capture card data during transactions.
- **Command and Control (C2):** Stolen data was sent to external servers controlled by the attackers.

Stage 1 Reconnaissance : Tools for Defenders

- **Nmap**: Discover devices and services on a network.
- **Google Dorking**: Find information using advanced Google search techniques.
- **theHarvester**: Gather OSINT (emails, subdomains, employee info).
- **Recon-ng**: Perform reconnaissance and information gathering.
- **Wireshark**: Analyze network traffic.
- **Sublist3r**: Enumerate subdomains of a domain.
- **Nessus**: Scan for vulnerabilities in systems and networks.
- **Metasploit**: Gather information for penetration testing.
- **Whois**: Query databases for domain/IP registrant info.

Stage 2 Weaponization : Tools for Defenders

- **Metasploit:** Identify and exploit vulnerabilities.
- **Wireshark:** Capture and inspect network traffic.
- **Nessus:** Scan for system vulnerabilities.
- **Cuckoo Sandbox:** Analyze and detect malware.
- **Snort:** Detect and prevent network attacks.
- **Threat Intelligence Platforms:** Get threat intelligence (e.g., MISP, OTX).
- **YARA:** Classify malware with patterns.

Stage 3 Delivery : Tools for Defenders

- **Email Filtering:** Proofpoint, Mimecast – Block malicious emails.
- **Web Filtering:** Cisco Umbrella, Websense – Block harmful websites.
- **Endpoint Protection:** Symantec, McAfee – Protect and monitor endpoints.
- **Network Intrusion Prevention:** Snort, Suricata – Monitor and block network threats.
- **Sandboxing:** FireEye, Palo Alto WildFire – Analyze and block malware.
- **SIEM Systems:** Splunk, IBM QRadar – Analyze security logs.
- **DNS Security:** OpenDNS, Infoblox – Prevent DNS-based attacks.

Stage 4 Exploitation: Tools for Defenders

- **IDS:** Snort, Suricata – Monitor network traffic for threats.
- **EDR:** CrowdStrike, Carbon Black – Detect and block endpoint threats.
- **Vulnerability Scanners:** Nessus, OpenVAS – Scan for system vulnerabilities.
- **HIDS:** OSSEC, Tripwire – Monitor host systems for threats.
- **App Security Testing:** OWASP ZAP, Burp Suite – Identify web app vulnerabilities.
- **Memory Analysis:** Volatility, Rekall – Detect malicious code in memory.
- **SIEM:** Splunk, ArcSight – Analyze security logs for threats.
- **Network Traffic Analysis:** Zeek, Wireshark – Capture and analyze network traffic.

Stage 5 Installation : Tools for Defenders

- **EPP:** Symantec, McAfee – Real-time malware protection.
- **HIDS:** OSSEC, Tripwire – Detect unauthorized changes.
- **App Whitelisting:** AppLocker, Carbon Black – Only allow approved apps.
- **FIM:** OSSEC, Tripwire – Monitor and alert on file changes.
- **SIEM:** Splunk, IBM QRadar – Analyze logs for suspicious activities.
- **Behavioral Analysis:** Cylance, CrowdStrike – Block malicious behavior.
- **EDR:** CrowdStrike, Carbon Black – Advanced endpoint threat detection.
- **Anti-Malware:** Malwarebytes, Kaspersky – Scan and prevent malware.

Stage 6 Command & Control (C2) : Tools for Defenders

- **IDS:** Snort, Suricata – Monitor network for C2 communication.
- **NIPS:** Palo Alto, Cisco Firepower – Block suspicious C2 traffic.
- **EDR:** CrowdStrike, Carbon Black – Detect and block C2 on endpoints.
- **SIEM:** Splunk, IBM QRadar – Analyze logs for C2 activity.
- **DNS Security:** OpenDNS, Infoblox – Block malicious DNS queries.
- **Traffic Analysis:** Zeek, Wireshark – Analyze network traffic.
- **Threat Intel Platforms:** MISP, ThreatConnect – Identify C2 domains/IPs.
- **Firewall/Proxy:** Fortinet, Blue Coat – Block known C2 IPs/domains.

Stage 7 Actions On Objectives : Tools for Defenders

- **SIEM Systems:** Splunk, QRadar – Analyze security logs.
- **EDR:** CrowdStrike, Carbon Black – Detect and stop endpoint threats.
- **DLP:** Symantec, Digital Guardian – Protect sensitive data.
- **NTA:** Zeek, Darktrace – Monitor network traffic.
- **Incident Response:** TheHive, Cortex XSOAR – Automate incident response.
- **Forensic Analysis:** EnCase, FTK – Analyze compromised systems.
- **Threat Intel Platforms:** ThreatConnect, MISP – Provide threat intelligence.
- **UEBA:** Exabeam, Securonix – Detect anomalies in user behavior.
- **IDS/IPS:** Snort, Suricata – Monitor and block network threats.

Cyber Kill Chain

Advantages of Attack
Reporting and
Documentation

Advantages of Attacks Reporting and Documentation

- **Improves Incident Response:**

- **Root Cause Analysis:** Identifies attack origins for better prevention.
- **Faster Recovery:** Ensures quick mitigation in future incidents.

- **Enhances Organizational Learning:**

- **Lessons Learned:** Teams improve strategies from post-incident reviews.
- **Training Material:** Reports provide real-world examples for training.

- **Strengthens Security Posture:**

- **Threat Pattern Recognition:** Helps identify recurring attack patterns and trends.
- **Improved Defenses:** Enhances firewalls and intrusion detection systems.

Advantages of Attacks Reporting and Documentation

- **Supports Regulatory Compliance:**

- **Audit Trail:** Regulations require detailed documentation (e.g., GDPR, HIPAA).
- **Avoiding Fines:** Proper reporting ensures compliance during audits.

- **Facilitates Communication:**

- **Internal Stakeholders:** Explains incident impact and resolution to executives and teams.
- **External Parties:** Provides details for law enforcement or third-party investigators.

- **Aids in Legal and Insurance Claims:**

- **Evidence Preservation:** Accurate documentation serves as evidence in legal disputes.
- **Insurance Claims:** Detailed reports are often required by cybersecurity insurance policies.

Advantages of Attacks Reporting and Documentation

➤ **Enhances Threat Intelligence:**


- **Data Sharing:** Contributing attack information improves global cybersecurity efforts.
- **Collaborative Defense:** Sharing insights with peers strengthens defenses.

➤ **Builds Customer and Stakeholder Trust:**

- **Transparency:** Reassures customers and stakeholders with thorough documentation and actions.
- **Reputation Management:** Proactive reporting mitigates reputational damage.

➤ **Enables Better Decision-Making:**

- **Resource Allocation:** Informs better investment in cybersecurity tools and personnel.
- **Policy Updates:** Refines security policies based on documented incidents.



Advantages of Attack
Reporting and
Documentation

Risk Register and
Enterprise Risk
Profile

Risk Register and Enterprise Risk Profile

- **What is Risk?**
 - Uncertainty that may impact organizational goals.
 - Operational Risks, Financial Risks, Compliance Risks, Security Risks
- **Importance of Risk Management:**
 - Enhances preparedness for incidents.
 - Aligns security efforts with business objectives.
- **Risk Register:** A structured document that lists potential risks, their impact, likelihood, and how to manage them.
- **Enterprise Risk Profile (ERP):** A summary of the organization's risk landscape.

Risk Register

- **Components of a Risk Register:**
 - **Risk ID:** Unique Identification
 - **Risk Description:** What the risk is.
 - **Impact:** What happens if the risk occurs.
 - **Probability:** Likelihood of the risk happening.
 - **Mitigation Strategies:** Ways to reduce or manage the risk.
 - **Risk Owners:** People responsible for handling the risk.
 - **Priority Ranking:** Order of importance for addressing risks.

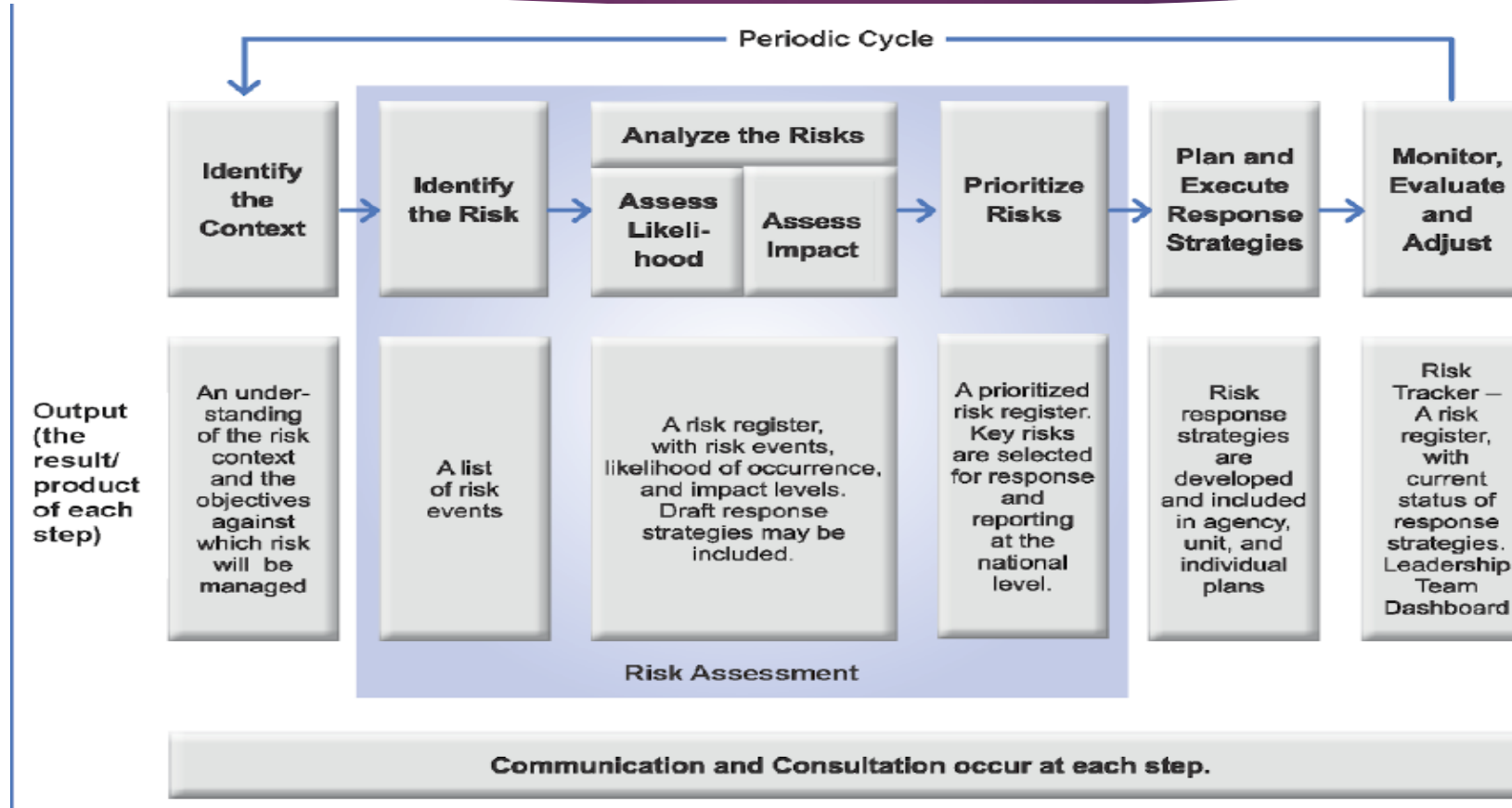
Risk Register

Risk ID	Description	Impact	Probability	Mitigation Strategy	Owner	Priority Ranking
001	Data loss due to ransomware attack.	Business disruption, financial loss, reputational harm.	High	Regular backups, employee awareness training, endpoint protection solutions.	IT Security Team	Critical
002	System downtime due to cloud provider outages	Service disruptions, customer dissatisfaction, financial loss.	Medium	Multi-cloud strategy, failover systems, service level agreements with providers	Cloud Infrastructure Team	High

Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment					Risk Response Type	Risk Owner	Status
				Financial Impact	Reputational Impact	Mission Impact	Likelihood	Exposure Rating			
001	High	Unauthorized access to sensitive customer data due to cyberattack.	Cybersecurity/Operational Risk	High (Opex H, CapexH)	High	Critical	Likely	Severe	Mitigation	IT Security Manager <Named Person>	Active
002	Medium	Disruption in the supply chain due to geopolitical events.	Operational	Medium (Opex M, Capex M)	Low	Moderate	Possible	Moderate	Contingency	Supply Chain Manager <Named Person>	Monitoring

Risk Management Life Cycle



Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment					Risk Response Type	Risk Owner	Status
				Financial Impact	Reputational Impact	Mission Impact	Likelihood	Exposure Rating			
001	High	Unauthorized access to electronic health records (EHR) leading to data breaches.	Cybersecurity /Operational Risk	High	High	Critical	Likely	Severe	Mitigation	IT Security Officer	Active
002	Medium	Unexpected failure of critical medical devices such as ventilators or MRI machines.	Operational	Medium	Medium	High	Possible	Moderate	Contingency	Biomedical Engineer	Monitoring

Risk Register

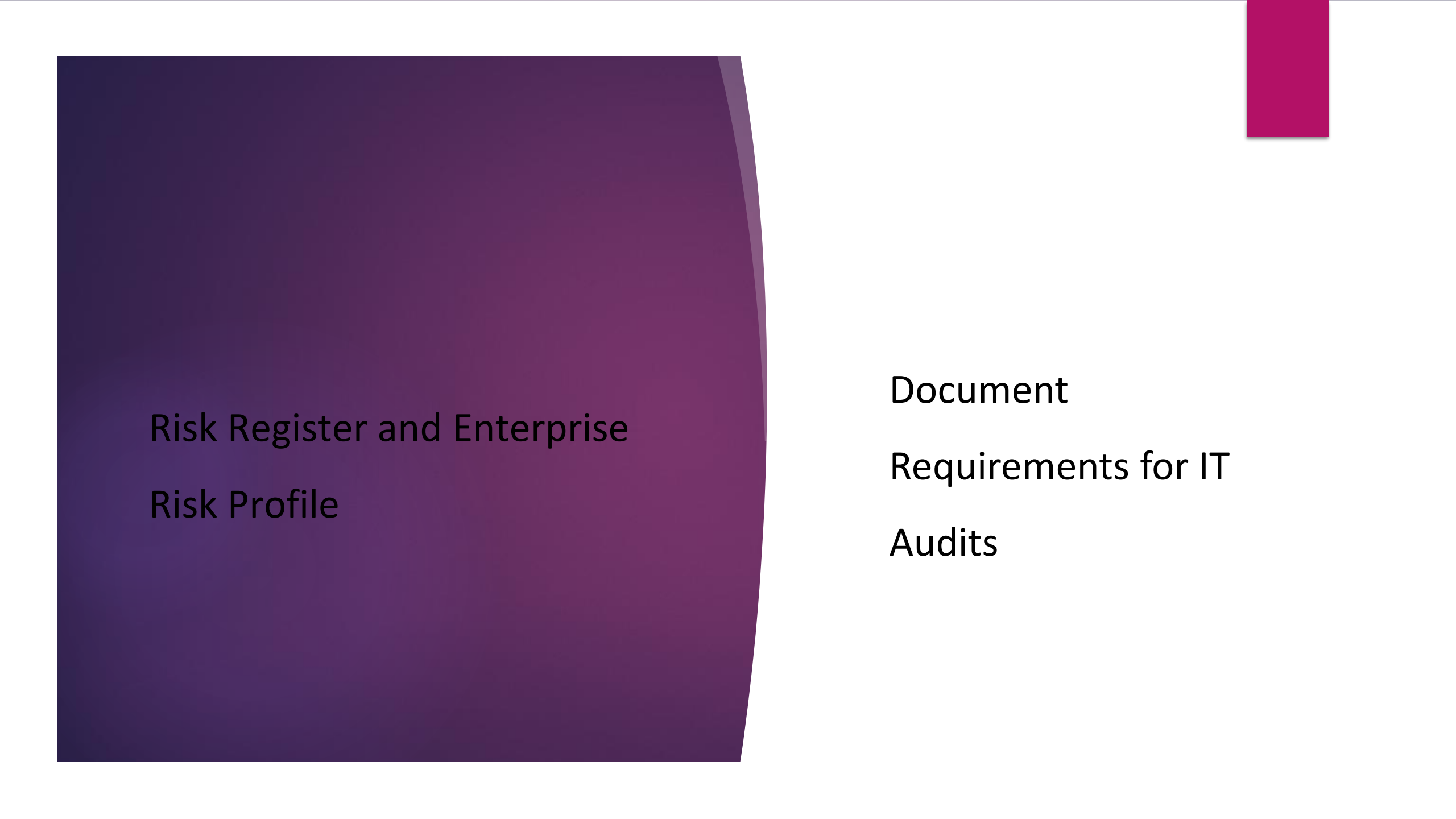
				Current Assessment							
ID	Priority	Risk Description	Risk Category	Financial Impact	Reputational Impact	Mission Impact	Likelihood	Exposure Rating	Risk Response Type	Risk Owner	Status
001	High	Shortage of raw materials or critical components (e.g., semiconductors) leading to production delays.	Supply Chain/Operational	High	Medium	Significant	Likely	High	Contingency	Supply Chain Manager	Active
002	Medium	Injury or accident in the assembly line due to equipment malfunction or human error.	Health & Safety/Compliance	Medium	Low	Moderate	Possible	Moderate	Mitigation	Safety Officer	Monitoring

Enterprise Risk Profile

- The Enterprise Risk Profile (ERP) is a comprehensive assessment of the critical risks that an organization faces at the enterprise level.
- It is derived from the Enterprise Risk Register (ERR), which contains a detailed list of all identified risks, their potential impacts, and their likelihood of occurring.
- As per NIST the Enterprise Risk profile must identify sources of uncertainty, both positive (opportunities) and negative (threats).
- Enterprise-level decision makers use the risk profile to choose which enterprise risks to address, allocate resources, and delegate responsibilities to appropriate risk owners
- ERM programs should define terminology, formats, criteria, and other guidance for risk inputs from lower levels of the enterprise.

Key Features of Enterprise Risk Profile (ERP)

- Subset of ERR:
- Risk Prioritization:
- Judgment and Assessment:
- Governance Tool:
- Support for Decision-Making:



Risk Register and Enterprise
Risk Profile

Document
Requirements for IT
Audits

Typical areas covered in IT audit

- **Governance and Compliance:**

- Alignment with regulatory frameworks
- Policy and procedure documentation.
- Roles and responsibilities within IT governance.

- **Risk Management:**

- Identification and assessment of IT risks.
- Implementation of risk treatment plans.
- Continuous monitoring and risk mitigation strategies.

Typical areas covered in IT audit

➤ **Access Controls:**

- User access management (authentication, authorization)
- Privileged account management.
- Periodic review of access rights.

➤ **Data Security and Privacy:**

- Protection of sensitive and personally identifiable information (PII).
- Data retention and disposal policies.
- Encryption and data masking techniques.

Typical areas covered in IT audit

➤ **Change Management:**

- Documentation and tracking of changes in IT systems.
- Testing and approval procedures for changes.
- Rollback and contingency planning.

➤ **Incident Management:**

- Incident response procedures.
- Root cause analysis and corrective actions.
- Documentation and reporting of security incidents.

Typical areas covered in IT audit

- **Business Continuity and Disaster Recovery:**

- Availability of business continuity plans (BCP) and disaster recovery plans (DRP).
- Testing and maintenance of backup solutions.
- Recovery time objectives (RTO) and recovery point objectives (RPO).

- **Network and System Security:**

- Firewall and intrusion detection system (IDS) configurations.
- Patch management and vulnerability scanning.
- Endpoint security controls.

Typical areas covered in IT audit

➤ **Audit Trails and Logging:**

- Monitoring of critical systems.
- Log retention policies.
- Detection of anomalies and suspicious activities.

➤ **Third-party Management:**

- Vendor risk assessments.
- Contractual agreements regarding data security.
- Compliance with service-level agreements (SLAs).

Key Documents Required for IT Audit

- Audit Trail
- Compliance
- Incidence Reports
- Policy and Processes

Audit Trail

- **Ensuring All Actions Are Traceable**
 - Logs of system access and changes.
 - Transaction records and approvals.
 - Monitoring reports and security logs.
- **Examples of Audit Trail Documents**
 - Access control logs.
 - Change management records.
 - Event Logs

Compliance Documents

➤ **Necessary Documents to Meet Standards/Certification**

- Information Security Policy.
- Statement of Applicability (SoA).
- Risk assessment and treatment reports.
- Internal audit reports.

➤ **Examples**

- Security compliance checklists.
- Records of corrective actions.
- Evidence of regulatory compliance.

Incident Reports

- **Detailed Records of All Incidents**

- Description of the security event.
- Impact analysis and classification.
- Actions taken to mitigate risks.

- **Format and Content of Incident Reports**

- Incident identification number.
- Date and time of occurrence.
- Root cause analysis and lessons learned.
- Evidence of continual improvement.

Policy and Procedures

- **Documentation of All Security Policies and Procedures**
 - Access control policies.
 - Business continuity and disaster recovery plans.
 - Data protection and retention policies.
 - Risk management procedures.

