CISSP Boot Camp

February 10, 2024

Email: info@bluecoattechnology.com

Course Outline

1	Security and Risk Management	15%
2	Asset Security	10%
3	Security Architecture and Engineering	13%
4	Communication and Network Security	13%
5	Identity and Access Management (IAM)	13%
6	Security Assessment and Testing	12%
7	Security Operations	13%
8	Software Development Security	11%

Domain 1

Security & Risk Management

Information & Cyber Security

Information Security

- Process of protecting information in digital, paper based or any other format

Cyber Security

- Process of protecting information in digital form
- Both types of Security is to protect information

3 Pillars of Cyber Security (CIA Triad)

1. Confidentiality

Information can only access by authorized user's

Example:

- Encryption of Personal Data
- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)

If a web server – availability & integrity is most important

If a payment platform, confidentiality & integrity is important

Ensure no one unauthorized can access the Data

IoT devices can be backdoor for any networks – can be threat for confidentiality

2. Integrity

- Only valid user can modify Data
- Accuracy of info always be maintained

Hashing – MD5, SHA2, Access Control, digital Signature

Ensure that Data is not modified without permission

Example: Intrusion Detection Systems (IDS)
Scenario: A financial institution operates a network of servers and Databases that process sensitive customer Data.

Example: Digital Signatures for Document Authentication
Scenario: A legal firm sends contracts and legal documents to clients electronically for review and approval.

3. Availability

- Information available all the time (24/7)
- When info needed its available
- If online transaction is doing
    - Network should be available
    - Application should be available

Hardware failure, application failure

Hot Sites
Cold Sites
Network Redundancy
Data backup (RAID)
Load balancers

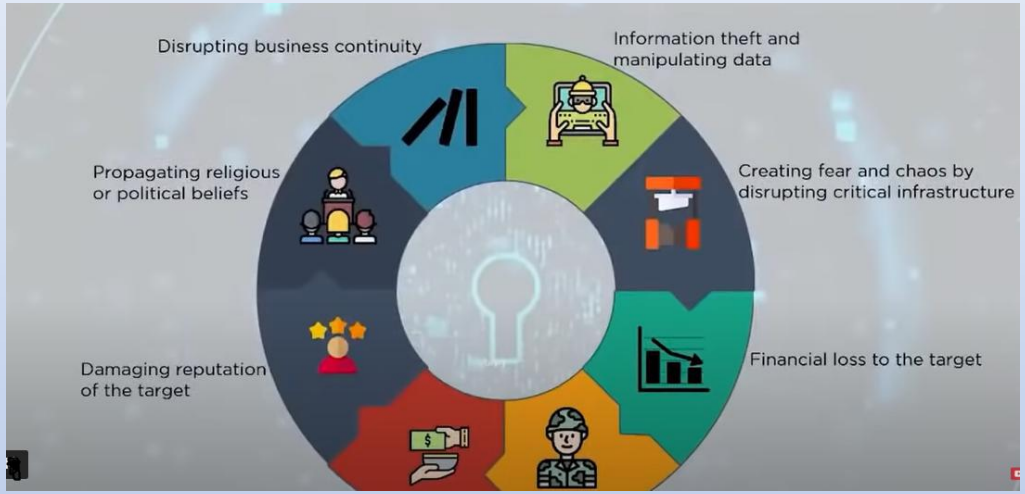
Examples:

- Redundant Servers for High Availability
- Data Backup and Disaster Recovery
- Content Delivery Networks (CDNs)
- Distributed Denial of Service (DDoS) Protection

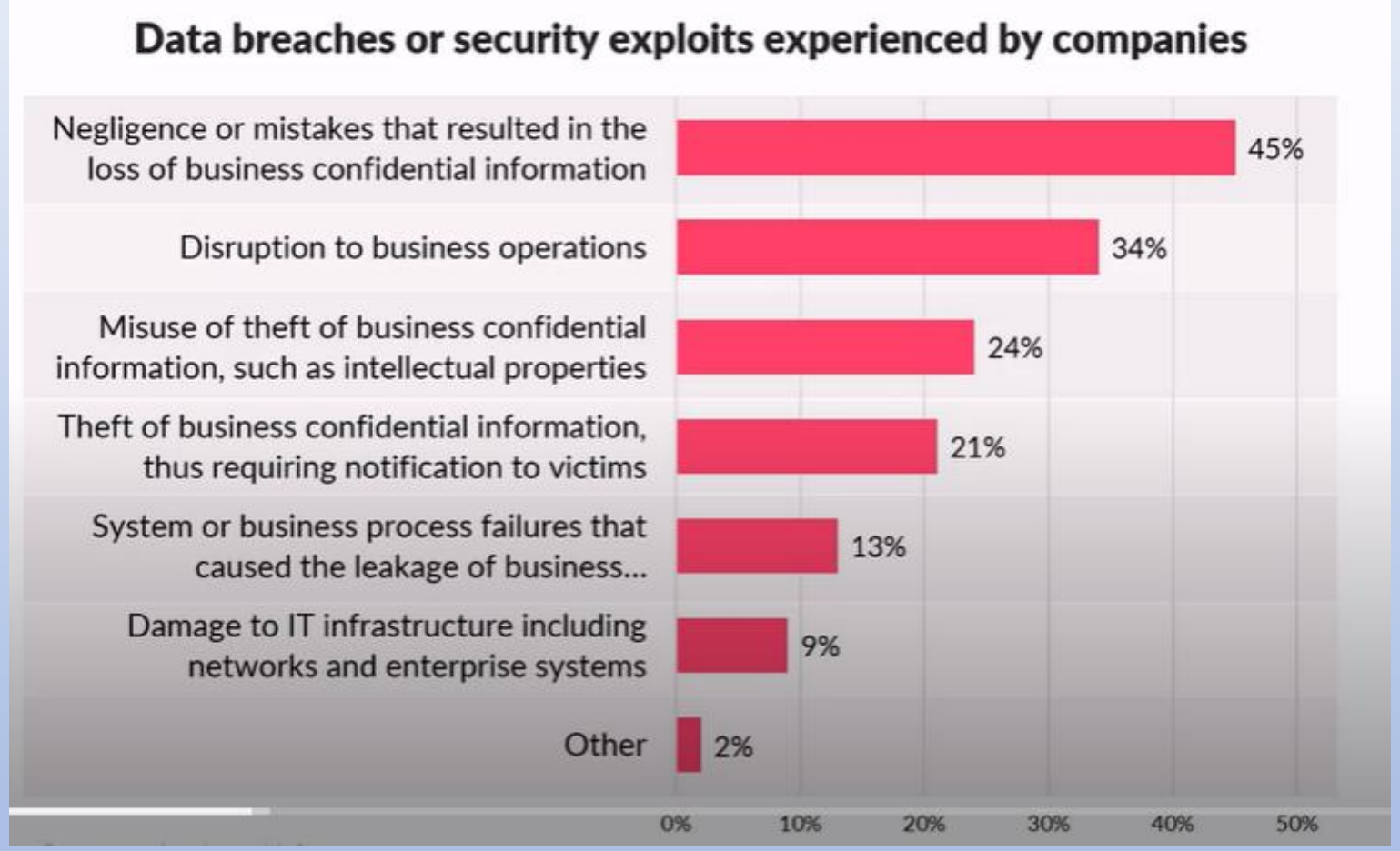
Why Cyber Security Important

- Rate of cyber crimes are increasing
- Work from Home increased after COVID
- If cyber attacks occur, org has
  - Financial losses
  - Reputational losses
  - Operational Impact

    - Data Protection:
    - Privacy Concerns:
    - Economic Impact:.
    - Digital Transformation:.
    - Critical Infrastructure Protection:
    - Rising Cyber Threats:
    - Regulatory Compliance:
    - Remote Work and Mobility:
    - Nation-State Actors:
    - Supply Chain Risks:
    - Internet of Things (IoT):.
    - Individual Safety:



Data Breaches experienced by Companies



Approaches of Cyber Security

Ad-hoc based

- When any issue occurs, will take action
- No plan
- Not recommended approach

Example: Incident Response Without a Formal Plan

Compliance based

- Follow all regulations without any argument
- No need for Risk Assessment -> follow laws and regulations

Example: Data Protection Compliance

Risk based (Recommended)

- Every org has limited resources
- Budget
- Resource
- Time
- Technology

Example: Third-Party Vendor Risk Management

Code of Professional Ethics (ISC)2

Ethics

Every organization has their own set of rules

Set of best practices

Ethical considerations are essential in an industry where technology, Data, and personal privacy intersect. Here's an example of ethics in Cyber Security:

- **Example:** Responsible Disclosure of Vulnerabilities

Canons

- Protect society, the common good, necessary public trust and confidence and the infrastructure.
- Act honorably, honestly, justly, responsibly and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession.

Identification, Authentication, Authorization & Accountability (IAAA)

Identification

- Process of asserting the uniqueness of an entity
- ID cards like a state-issued driver’s license
- User name or email address

Authentication

- Checking if username/password is ok – Identified that you are the valid user…now start Authentication

Something you know – PIN, password

Example:

- User Authentication
- Remote Access Control
- Single Sign-On (SSO) Authentication
- Token-Based Authentication

Something you have – Token, ID, smart card

Something you are – Retina scan, finger prints, facial scan

- **Authorization**

Granting specific permissions and access rights to authenticated users, systems, or entities based on their roles, responsibilities

When user given access to certain Data

Example:

- File and Data Access Authorization:
- Network Access Authorization:
- Application Access Authorization:
- Database Access Authorization:

What type of access they have
RBAC – Role Base Access Control
DAC – Discretionary Access Control

Accountability

- Track all the activities

Types of audit

Monitor who performed such activities

Example:

- Audit Trails:
- System Logs:
- Application Logs:
- Digital Signatures:
- Incident Response Tracking:

Non-Repudation

Can prove easily which user performed those activities

Proof that someone taken an action and its confirmed

Security Governance & Security Management

Governance

- IT Governance
- Security Governance – Main goal is to reduce the risk to acceptable level

- Governance in Cyber Security refers to the framework, policies, procedures, and Controls that an organization establishes to guide its Cyber Security efforts

- **Information Security Policies:** guidelines for handling sensitive Data, user access, encryption, and Incident response.
- **Risk Management Framework:** NIST Cyber Security Framework or ISO 27005 to assess, manage, and mitigate Cyber Security risks
- **Cyber Security Roles and Responsibilities:** Clearly defined roles and responsibilities CISO
- **Compliance with Regulations:** GDPR, HIPAA, or PCI DSS
- **Security Training and Awareness Programs:**
- **Incident Response Plan:**
- **Vendor Risk Management:**
- **Security Audits and Assessments**
- **Change Management Process**
- **Business Continuity and Disaster Recovery Planning:**
- **Data Classification and Protection**
- **Regular Security Reviews and Assessments:**

IS Governance to verify

Controls are Implemented
Controls are working
Risks are minimized
Controls achieve the objectives

Risk Management

Identifying, assessing, and mitigating potential risks and vulnerabilities to protect digital assets and sensitive information

Key Components of Risk Management

- ❑ Risk Identification
- ❑ Risk Assessment
- ❑ Risk Mitigation
- ❑ Risk Monitoring
- ❑ Documentation and Reporting
- ❑ Continuous Improvement

Compliance

Adherence to legal, regulatory, and industry standards and requirements related to information Security and Data privacy

- Adhere to policies, laws, regulations, contractual terms, procedures, standards etc.
- Ensure org follow laws, regulations, policies etc.

- **Regulatory Compliance:** GDPR, HIPAA, PCI DSS
- **Legal Compliance: L**aws and regulations related to Data protection, privacy
- **Industry Standards:** NIST, ISO 27001
- **Data Protection:** Protecting personal and sensitive Data
- **Security Policies and Procedures:** Developing and enforcing clear Cyber Security policies, procedures, and guidelines
- **Incident Response:** Establishing protocols to respond effectively to Security Incidents, breaches, and Data breaches
- **Audits and Assessments:** Conducting regular internal and external audits

Due Diligence

Due Diligence

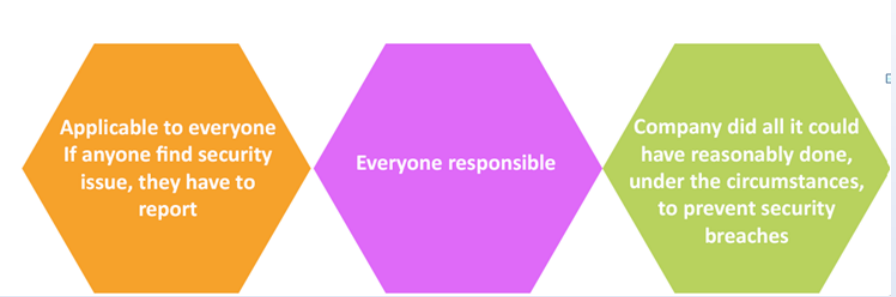
Do everything, if possible, to make sure Security issues will not happen in the org

- Top management responsibility
  - Company properly investigated all of its possible weaknesses and vulnerabilities
  - If company A wants to buy company B, first they have to investigate all the risk, weaknesses of Company B prior to take any decision
  - Developing a formalized Security structure containing a Security policy, standards, baselines, guidelines, and procedures

  - Mergers and Acquisitions (M&A):
  - Cloud Service Provider Evaluation:
  - Data Sharing Agreements:
  - IT Asset Disposal:
  - Network Penetration Testing:

Due Care

- If anyone see sec issue -> they have to report
- Sec engineer – if they see alerts -> they have to take action



- Company did all it could have reasonably done, under the circumstances, to prevent Security breaches
- Company practiced common sense and prudent management and acted responsibly

- **Regular Software Patching:**
- **Data Encryption:**
- **Data Backups:**
- **Monitoring and Logging:**
- **Secure Coding Practices:**

Company properly investigated all of its possible weaknesses and vulnerabilities

If company A wants to buy company B, first they have to investigate all the risk, weaknesses of Company B prior to take any decision

Developing a formalized Security structure containing a Security policy, standards, baselines, guidelines, and procedures

Service Level Agreement (SLA's)

3rd party agreements with

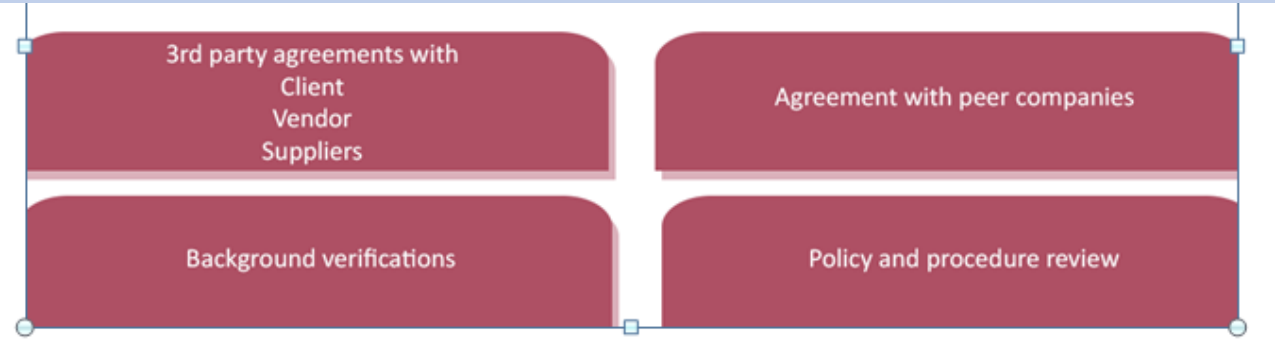
- Client
- Vendor
- Suppliers
- Contractors

How to do 3rd party agreements

- Background verifications
- Evaluate Security Controls
- Financial capability

- Once background done -> sign contract, NDA, SLA's

- Offshore -> Sensitive info travel from one geographical part to other



Intellectual Property Laws

Copyright

Protects the rights of the creator of an original work to control public distribution, reproduction, display, and adaptation of that original work

Protection against the unauthorized duplication of their work

Protects creative expressions and original works

- Pictures
- Documents
- Audio/video
- Design/source code
- Music

- 70-120 years -> After this time period info become public

- User can use but cant modify
- Author A & B written book, after death of Author A law protect 70 years
- Exclusive use of artistic, musical or literary works that prevents unauthorized duplication, distribution or modification)

70 years after creator's death or 95 years after creation

legal rights that protect the software (not the idea)

Trademark

- Logos, brands, slogan etc.
- Should never be similar to existing one
- Protected for 10 years, can extend for 10+10+…. years till infinite period
- A legal right that protects a word, name, product shape, symbol, color, or a combination of these used to identify a product or a company

Copyright protects business sales flyer, no one can produce the duplicate

Trademark protects business name, their product name

Trademark not protect the software

Trademark registered by United States Patent & Trademark Office (USPTO)

Patent

Protect inventive solutions and technologies

- Medicine formulas etc.
- New formula
- Can protect for 20 years after that it should be public.
  cant extend after 20 years
- Strongest form of intellectual property protection
- Provide protection to the creators of new invention
- A temporary monopoly for producing a specific item such as a toy

Patent duration – 20 years

A patent grants the owner a legally enforceable rights

Can protect for 20 years after that it should be public

Strongest form of intellectual property protection

Provide protection to the creators of new invention

A temporary monopoly for producing a specific item such as a toy

Trade Secret

Trade secret law protects certain types of information or resources from unauthorized use or disclosure.

Info should be secret for lifetime
Copyright/Patent/Trademark -> for specific time period
Trade Secret -> Protect for life time

Toyota, Coach, drink formula etc.

- Info should be secret for lifetime
- Copyright/Patent/Trademark -> for specific time period
- Trade Secret -> Protect for life time

- Implement Controls to become secret
- Minimum users can access

  drink formula etc.

Formula for coke

Developed a unique intrusion detection algorithm that is not publicly known

DMCA – Digital Millennium Copyright Act

LICENSES:

CONTRACTUAL LICENSE AGREEMENT:
Vendor -> written agreement -> contractor

SHRINK-WRAP LICENSE:
In CD/DVD there is license agreement in the bundle
Once open -> bound to follow the license

CLICKWRAP LICENSE:
When install the software - 'ACCEPT' once clicked -> we have to follow the instructions

CLOUD SERVICES LICENSE AGREEMENT:
It is similar to a clickwrap agreement and is mainly concentrated on the services provided by cloud vendors.

- If user access pirated Data through ISP, in this case ISP will not be responsible

- **Privacy**

  Protection of privacy information

    PII – Personal Identification Information

    Educational record of students

    Info of minor children

Licenses

Contractual License Agreement

Vendor -> written agreement -> contractor

Shrink wrap license

In CD/DVD there is license agreement in the bundle

Once open -> bound to follow the license terms and conditions

Example:

- SecureGuard Antivirus Software

Click wrap license

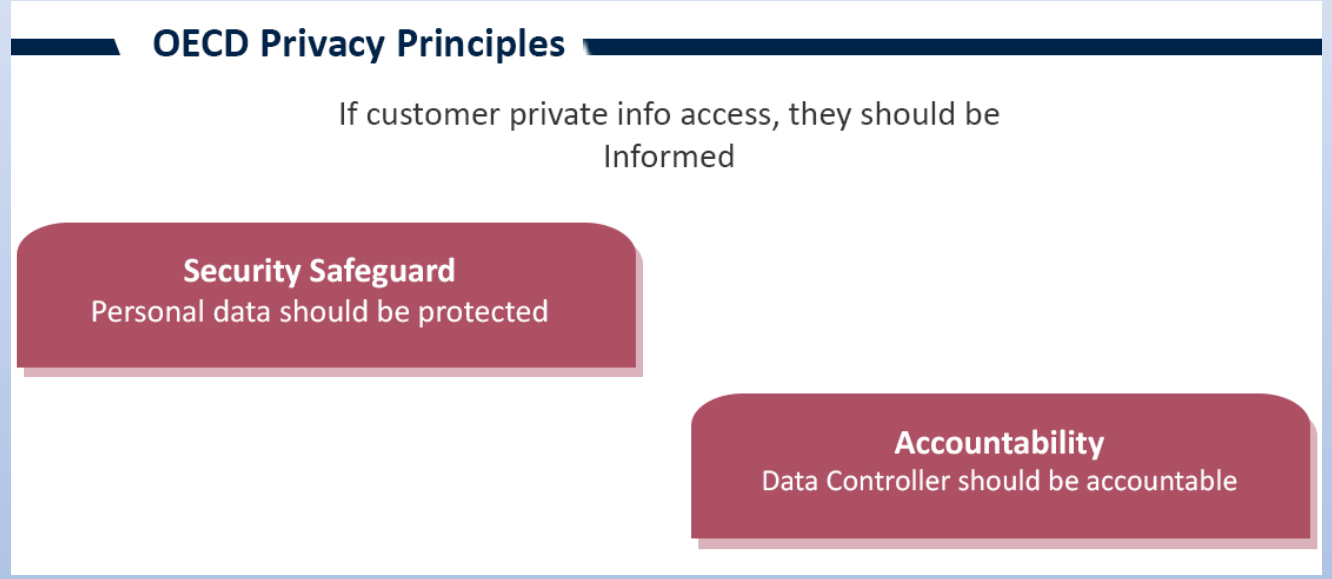
When install the software

See ‘ACCEPT’ once clicked -> we have to follow the instructions

OECD – Organization for Economic Cooperation & Development

If customer private info access, they should be informed

- **Privacy Principle**
  - Purpose
  - Collection limitation
  - Data quality
  - Use limitation
  - Security Safeguard
  - Accountability



General Data Protection Regulation (GDPR)

Regulation requires businesses to protect the personal data and privacy of EU citizens

Protection of privacy of EU citizens
Data cannot be stored outside EU

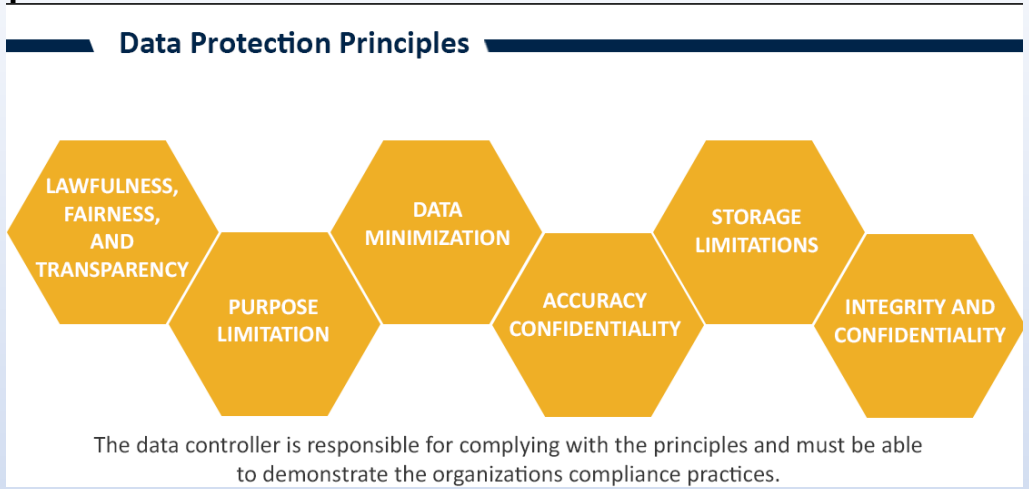
If there is data breach, must inform within 72 hours
Fine can go up to 4%

Comprehensive Data protection regulation implemented by the European Union (EU) to provide stronger and more consistent Data privacy rights and protections for individuals within the EU

Examples:

- Data Security and Breach Notification
- Data Protection Impact Assessment
- Vendor and Third-Party Management
- Cross-Border Data Transfer
- Incident Response and Reporting
- Penalties and Fines

Data Protection Principles



- **Lawfulness, Fairness & Transparency**
  - Org collect personal info from customers
  - Must be collected in legal way

- **Purpose Limitation**
  - When info collecting from customer -> org has to provide the purpose
  - Info only use for that particular purpose

- **Data Minimization**
  - Only the minimum info gather for the purpose
  - Nothing more should be collected

- **Accuracy**
  - Customer info change time by time -> org has to update their record once info changed

- **Storage Limitation**
  - Cannot store personal info for indefinite period
  - Once purpose over -> info should be removed

- Integrity & Confidentiality
  - Provide integrity and confidentiality to info

Types of laws

Criminal

- Harmful to society
- Prison

Society is the victim

Computer Fraud and Abuse Act (CFAA)

- Prohibits unauthorized access to computer systems, networks, and Data. It covers hacking, identity theft, and unauthorized Data access

Identity Theft Laws:

- These laws criminalize the unauthorized use of another person's personal information for financial gain or other fraudulent purposes

Data Breach Notification Laws:

- organizations to notify individuals and authorities in the event of a Data breach that compromises personel information

Civil

- If violate contract, there would be compensation/financial restitution
- Laws agencies not involved -> Only internal parties do investigation
- Financial restitution

- legal regulations and principles that address non-criminal disputes and liabilities

Breach of Contract:

- Service providers or vendors have contractual clauses if not completed may lead civil action

Copyright

- Unauthorized use, distribution, or reproduction of copyrighted material can lead to civil cl

Online dispute and Scams

Product Liability

Regulatory

- Fines and penalty

Security of digital systems, protect sensitive Data, and mitigate cyber risks

Examples:

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- California Consumer Privacy Act (CCPA)
- Federal Information Security Management Act (FISMA)
- Financial Industry Regulatory Authority (FINRA) Rules

Policies, Standards, Procedures & Guidelines

Policies

- High level docs/Strategic docs (Least changes)
- What needs to be done to protect assets
- Mandatory to follow
- Least changes

Policies are generic

Mandatory

Example: An "Information Security Policy" might state that all employees must follow Security best practices, use strong passwords and protect sensitive information.

Should have

Purpose
Scope
Framework
Risk Assessment (acceptable risk/no impact on organization)
Security roles and responsibilities
Who will implement Security policies

Standards

- How to be done
- Mandatory activities to follow
- Minimal changes

Example:

All computers must have updated antivirus software installed

Procedures

Step by step instructions
Day to Day operations
Mandatory to follow
Maximum changes

Mandatory

Procedures are specific

Example:

- How to boot server
- How to configure firewalls
- Incident Response Procedure- how to respond, notify, & isolate affected systems

Baselines

Minimum to follow

BASELINES

Minimum level of security that systems should have

Minimum to follow

Exp: Linux systems should installed latest patch v7.1

Guidelines

Supporting docs
Logical assumptions
Discretion to follow

Guidelines are recommendations suggestions that provide flexibility - how tasks are completed

"Password Guidelines“ combination of uppercase, lowercase letters, numbers, and special characters

Non-Mandatory

BCP/DR

Need for Business Continuity Planning

Business operations are interrupted by unexpected events. Companies must develop Business Continuity and disaster recovery strategy

- Protect human life
- Continue normal business operations
- Minimum disruptions
- Prevent operational and financial losses

Disaster

Any incident that suspends normal business operations

Intentional or un-intentional

BCP focuses on minimize the effects disaster

DISASTER TYPES

- NATURAL
- HUMAN
- ENVIRONMENT

Disruption

- Natural (tornado, earthquake)
- Man-made (viruses, network attacks)

Disaster

- If any disruption > 1 day

Business Continuity Strategy

- Mission of organization
- Strategy
- Security Objectives
- Scope
- Security Team (CIO, CISO)
- Resources
- BCP Policies (signed by CEO)
- Business Impact Analysis (BIA)
- Identify Controls
- Implement Controls

RPO, RTO & WRT

Recovery Point Objective:
Data backup frequency
If system down for 3 hours -> no issue

Recovery Time Objective:
Time to recover system
If server down -> it should be recover in 2 hours

Work Recovery Time:
MTD-RTO = WRT
Once servers issue fixed -> start data backup

RTO – Recovery Time Objective (2hr)

- Time to recover system
- If server down -> it should be recover in 2 hours

Examples:

- **WebSite Availability**: Restore company webSite within 2 hours
- **Data Center Outage**: Recover critical systems within 4 hours
- **Email System Recovery**: Bring email server back online within 3 hours
- **Database Failure**: Restore customer Database within 1 hour

RPO – Recovery Point Objective (3hr)

- Data backup frequency
- If system down for 3 hours -> no issue
- Every 3 hours -> we have to take Data backup

Examples:

- **Database RPO**: Data loss should not exceed 15 minutes. This means that in the event of a Database failure, the organization can tolerate a maximum of 15 minutes' worth of Data loss.

- **File Server RPO**: Data loss should not exceed 1 hour. In case of a file server failure, the organization can tolerate up to 1 hour

Cloud Services RPO: For cloud-hosted services, ensure that Data loss does not exceed 1 hour

WRT – Work Recovery Time (2hr)

- Once server issue fixed -> start Data backup

Examples:

- **Ransomware Attack**: Recover and restore affected systems, applications, and Data within 48 hours
- **Distributed Denial of Service (DDoS) Attack**: Mitigate the impact of a DDoS attack and restore normal online service within 12 hours
- **Data Breach**: Investigate and remediate within 72 hours
- MTD-RTO = WRT

MTD – Maximum Tolerable Downtime (4hr)

If downtime 4 hours then system should recover within this time frame

MTD = RTO + WRT

MTBF – Mean Time between Failure

How many times server fails per year -> based on past experience

Choose higher MTBF servers

Frequency of failure

MTTR – Mean Time to Recover

If server fails -> how long it will take to recover based on past experience

Choose lower MTTR servers

Average time to repair

If downtime goes beyond MTD

- Not good for business, it should be improved

Downtime should be less or equal to MTD

MTD = RTO + WRT

MTD > RTO

If system hard drive failed, it should replaced (RTO)

Business Continuity Planning

PHASES

- SCOPE
- IDENTIFY CONTROLS
- PLANNING
- MAINTENANCE
- BUSINESS IMPACT ANALYSIS
- RECOVERY
- TESTING

Scope

* Create Scope

* Risk Analysis to identifying critical systems and potential outages

* Identify BCP resources included senior management, CFO, applications owners, business owners, data center point of contact etc.

Business Impact Analysis (BIA)

Determine the impact of disaster to the organization systems and processes

Identify and prioritize critical IT systems and components

BIA Objectives

Prioritization
Pioritize of critical business unit
Evaluation the impact

Maximum Tolerble Down Time
Downtime requires for business to survive
If downtime 4 hours then system should recover within this time frame
MTD = RTO + WRT

Steps to conduct BIA

01 Select resources for data gethering

02 Create techniques 'how to gather data'

03 Identify critical business processes, functions and apps

04 Identify resources according to business criticality

05 Calculate critical business survival without proper resources

06 Identify vulnerabilities and threats

07 Calculate Risk

08 Determoine Qualitative & Quantitative Impact

09 Document and Report

BCP: Identify Controls

Existing Controls
Process to mitigate effect of threat

Physical Controls
Access control systems, guards etc.

Procedural Controls
Hiring & clean desk policy

Logical Controls
DLP, IDS/PDS

Risk Management

What is IT Risk?

- Likelihood of something wrong and damage IT assets

Risks Impact

- Physical damage *(Fire, power failure, natural disaster*)
- Human Interaction *(Intentional or unintentional behavior can damage)*
- Internal or External Attacks *(Hacking, cracking)*
- Misuse of data *(Sharing trade secrets, fraud, theft)*
- Operational disruption
- Regulatory action
- Loss of reputation & revenue
- Loss of shareholder value

Why Risk Management needed

Identify organization critical assets and develop strategy to **protect**

Risk Management Process

Risk Assessment

- Components of Risk Assessment

1. **Vulnerability**

   Weakness in the system to be exploited

   - Polices are not updated
   - Patching not updated
   - Anti viruses' licenses expired
   - Router’s passwords not change since long
   - Server’s room door not locked

2. **Threat**

   Possible event that can damage Information System

   - Information disclosure
   - Service disruption

Exposure Factor (EF)

- Amount of asset can damage due to risk exposure show in percentage
- BCP Team consult with fire dept that building fire can destroy 80% if fire happen

Single Loss Expectancy (SLE)

- Loss expected each time if risk materialized
- SLE = AV x EF

Annualized Loss Expectancy (ALE)

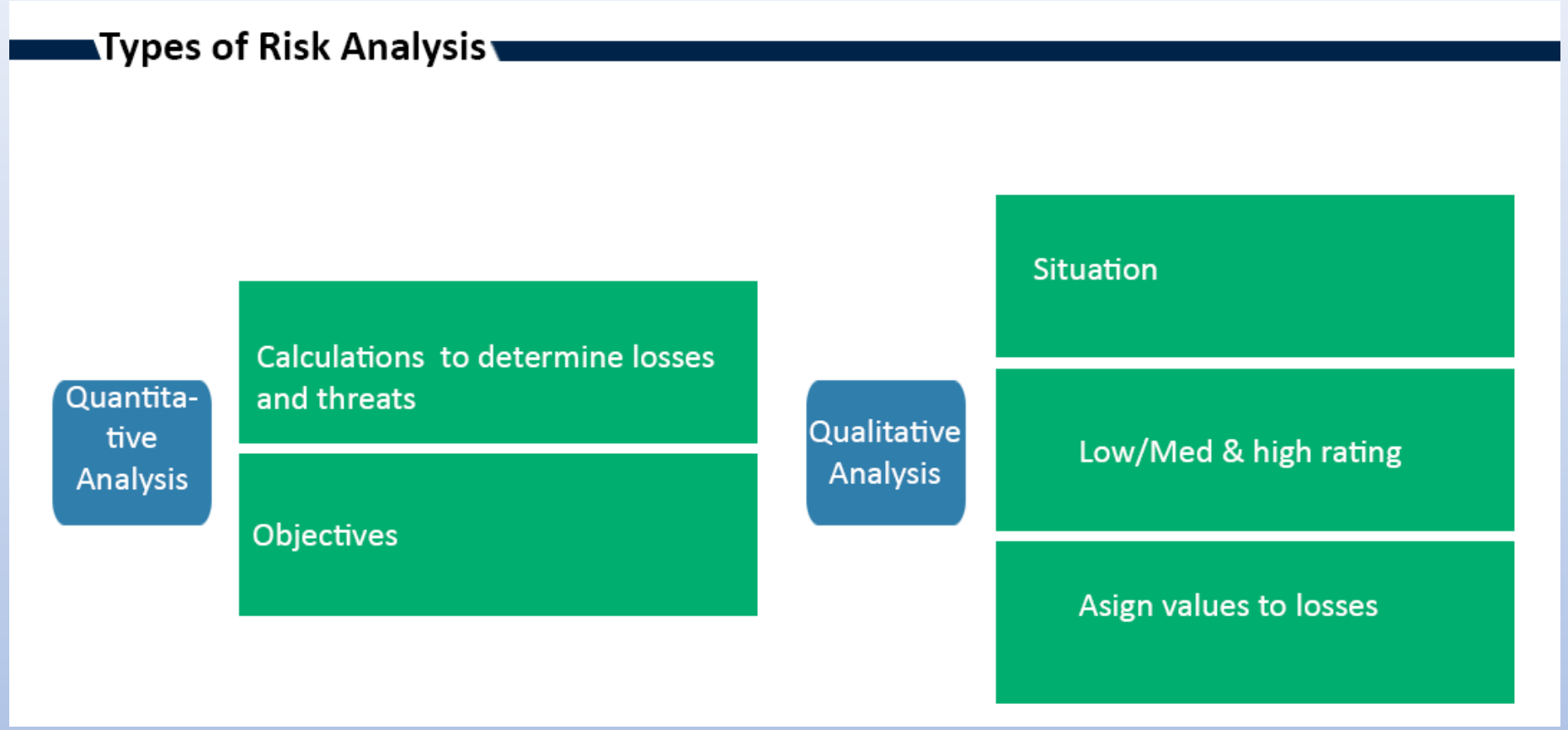
- Expected no of times disaster occurs each year
- ALE=SLE x ARO

Annualized Rate of Occurrence (ARO)

- Expect to disaster occur each year

Risk Analysis Team

Major stakeholders in risk analysis team



- Qualitative Risk Analysis done by **Financial** Department
- Qualitative Risk Analysis done by **Security** department

Quantitative Risk Analysis

Quantitative Risk Analysis

Annualized rate of Occurrence (ARO)	Frequency of threats occur a single year
Annualized Loss Expectancy (ALE)	Annual cost of threatst ALE = SLE * ARO
Annual Cost of Controls (ACS)	Cost of design, develop and implement controls ACS always less than ALE

Quantitative Risk Analysis

Asset	Tangible or intangible
Exposure Factor	One time loss Percentage of loss the organization would suffer if a risk materializes
Single Loss Expectancy (SLE)	SLE = AV* EF

How to handle Risks

1. Acceptance

- Implement Controls
- Risk come down to acceptable level

Risk is there but the cost of mitigation is more then the risk (low risk)

Examples:

Legacy Systems: Organization has older, unsupported systems that cannot be easily updated or patched and this is known Security risk.

But organization decides to continue using these systems due to budget constraints or operational dependencies

Third-Party Services: Organization uses third-party services like email storage in cloud.

Organization recognize the potential risk of Data exposure, but they decided to continue because cost benefits are much higher

Low-Impact Data: Organization has some internal documents which are not confidential or sensitive.

Risk is low so they don't want to invest to implement Controls

2. Mitigation

Reduce the risk

Provide encryption to the system, left over risk called mitigation

Examples:

Patch Management: Regularly applying software updates and Security patches to operating systems, applications, devices to minimize known vulnerabilities

Firewalls and Intrusion Detection Systems (IDS): Deploying firewalls and IDS to monitor network traffic, detect unauthorized access and block malicious activities

Multi-Factor Authentication (MFA): Password and SMS to access sensitive systems

Encryption
Endpoint Protection:
Security Training and Awareness:

3. Transfer

Transfer to 3rd party and they are responsible
But organization is still accountable

Examples:

Cyber Insurance: Example: An organization purchases cyber insurance to cover financial losses resulting from Data breaches, cyberattacks, and other Cyber Security Incidents

Third-Party Vendor Agreements: Example: When partnering with a cloud service provider, the organization includes terms in the service-level agreement (SLA) that specify the provider's responsibility for securing Data and their liability in case of a Security breach.

Joint Ventures and Partnerships:
Outsourcing Security Services:

4. Avoidance

Taking deliberate actions to eliminate or avoid activities, processes, technologies that can become Security risks

During cost/benefit analysis, found some Controls are not good - Only option to avoid the risk

Examples:

Discontinuing Outdated Systems: Organization retires legacy systems that are no longer supported or updated, due to Security risk

Blocking Risky WebSites and Applications: Implementing web filtering and application whitelisting to block access to avoid any Security risks.

Restricting Remote Access: Limiting remote access

Residual

Once Controls implemented still there is some risk
Risks come down to acceptable level

If Mitigation Cost > Asset Value = Accept the Risk
If Mitigation Cost < Asset Value = Implement Controls

Examples:

Zero-Day Vulnerabilities: Unknown vulnerabilities that have not yet been patched by software vendors

Human Error: After Training and awareness programs, employees might still make mistakes that lead to Data breaches or Security Incidents.

Supply Chain Risks: Even with supply chain Security, supplier's software or hardware can still introduce risk to

Technological Limitations: Some vulnerabilities might be inherent

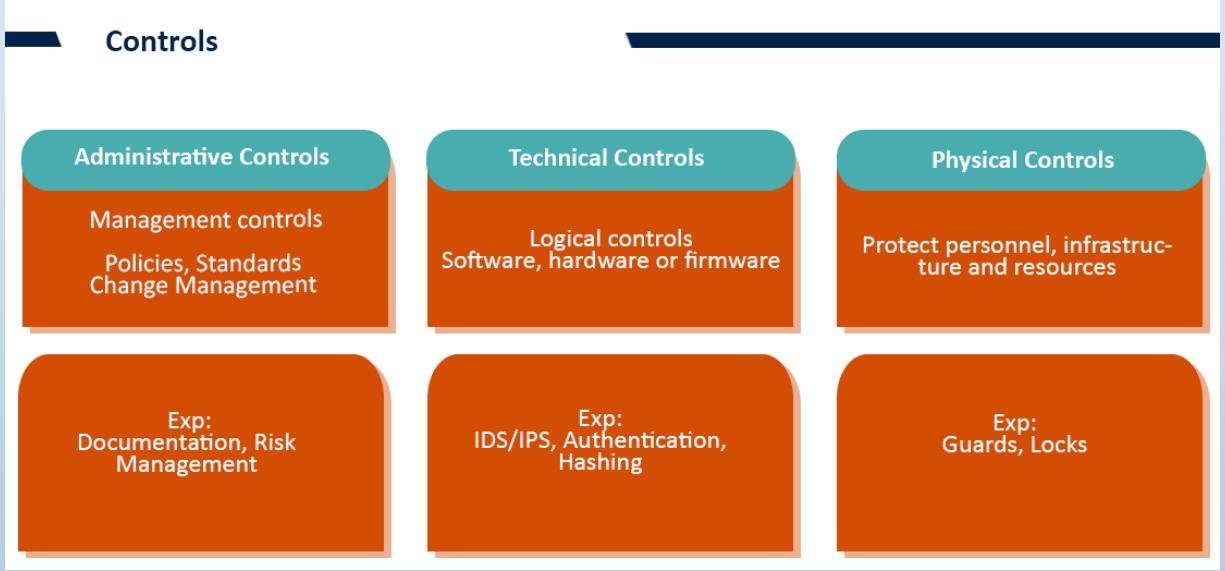
Legal and Regulatory Risks: Organizations might comply with current regulations, but changes in laws or new interpretations might lead to residual risk in terms of compliance.

How to Mitigate the Risk – Implement Controls

- **Administrative**
  - Soft Controls
  - Policies, Procedures
  - Standards
  - Change Management
  - Visitors entering Control

- **Physical**
  - Operational Controls
  - Gates, CCTV, Access Control
  - Fence
  - HVAC
  - Power
  - Biometrics

- **Technical**
  - Logical Controls
  - IT related Controls
  - Encryption
  - Antimalware
  - Firewalls
  - IDS/PDS



Categories of Control

- **Deterrent Controls**
  - Discourage potential attackers from targeting an organization's systems, networks, and Data
  - Stop sign

Mantraps, Security guards, fences, dogs

Discouraging someone trying to gain access

Cameras are major deterrent to crime

Example:

- Legal Action Warnings:
- Regular Security Audits:
- Simulated Attacks (Red Team):

Preventive Controls (Access Controls)

Pro active control to stop or minimize Security Threats

- Firewall
- Ati-malware
- Data Encryption
- Applications whitelisting

IPS, Least Privilege, encryption, drug test

Detective Controls (monitor Security violations)

Identify and detect Security Incidents, breaches, and unauthorized activities after they have occurred

CCTV
IDS
SIEM

Examples:

- Security Information and Event Management (SIEM): Collect and analyze logs to identify unusual or suspicious activities

- Log Analysis:
- Vulnerability Scanning and Assessment:
- Network Traffic Analysis
- Forensic Analysis

- **Corrective Controls**
  - Bring the system back to normal
  - Respond to mitigate Security Incidents, breaches, or vulnerabilities that have been identified

To correct any problems resulting from a Security Incident

Backup and restore plans to ensure that lost Data can be restored

Examples:

- Patch Management:
- Data Recovery:
- User Account Revocation:
- Change Management Processes:

- **Recovery Controls**

Restore normal operations, systems, and Data after a Security Incident or breach, or other disruptive events.

- If server connected to power supply -> due to some reason power failed - > Recovery Controls have stand by power supply
- If server is on DoS attack -> have backup server to remediate

Examples:

- Data Backups and Restoration:
- Business Continuity Plans:
- Redundant Systems and Failover:
- Documentation and Playbooks:

- **Compensating Controls**

Alternative Controls in place to mitigate risks when primary Controls are not feasible

- Support other existing Controls in place of other Controls
- In server -> Implemented antimalware solution -> In addition patching done
- If server has bug -> vendor doesn't have patch -> so for the time being -> they would implement compensating Controls -> Move server to different VLAN

- **Biometric Authentication for Single Sign-On**: instead of traditional passwords to enhance Security
- **Data Loss Prevention (DLP)**: to prevent Data leakage, implement DLP solution to compensate the risk of sensitive Data leaving the organization

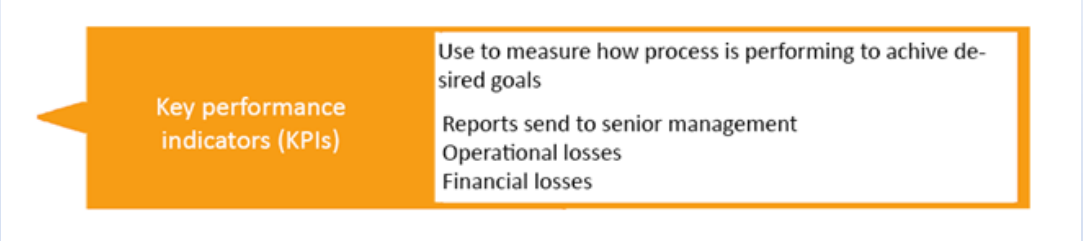
When other Controls are costly

To improve effectiveness of primary control or alternate option in the event of primary Controls fail

If building has fire, it should have backup Site as Compensating control

Risk Monitoring & Measurement

- Overview of the organization's Cyber Security performance and the effectiveness of its Security measures
- To ensure risks always on acceptable level



- **KPI's**
  - During Risk Assessment identified many Controls
  - Cant implement all 114 Controls by ISO 27001
  - Monitor high risks and then apply Controls

Examples:

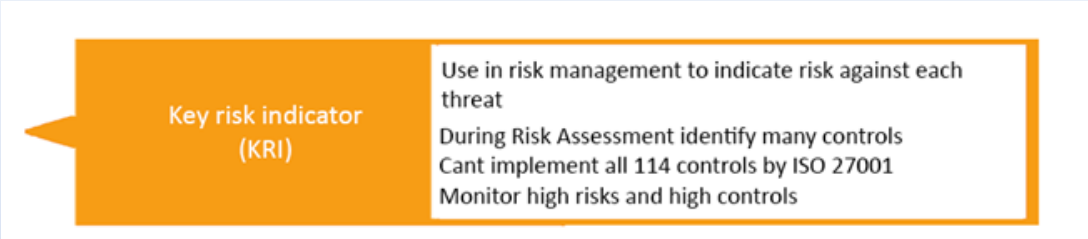
- Number of Security Incidents
- Phishing Click Rate:
- Security Policy Violations:
- Number of Vulnerability Assessments:
- Data Loss Incidents:

Recommendations

- If patch completing target is 95% per month -> if achieve 93%
- Then go for corrective actions

KRI's

- Critical risks that the organization faces



Examples:

- Average Time to Detect Incidents
- Number of Unauthorized Access Attempts
- Percentage of Devices with Outdated Antivirus Signatures:
- Number of Data Breaches

- **Report included**
  - How many Security issues in last quarter
  - Any Security issues related to operational
  - Management take decision

- **Continuous Improvement**
  - Incident reduces by 5% but it should be improved by 8%

Risk Management Framework

Structured approach that organizations use to identify, assess, mitigate, and monitor risks

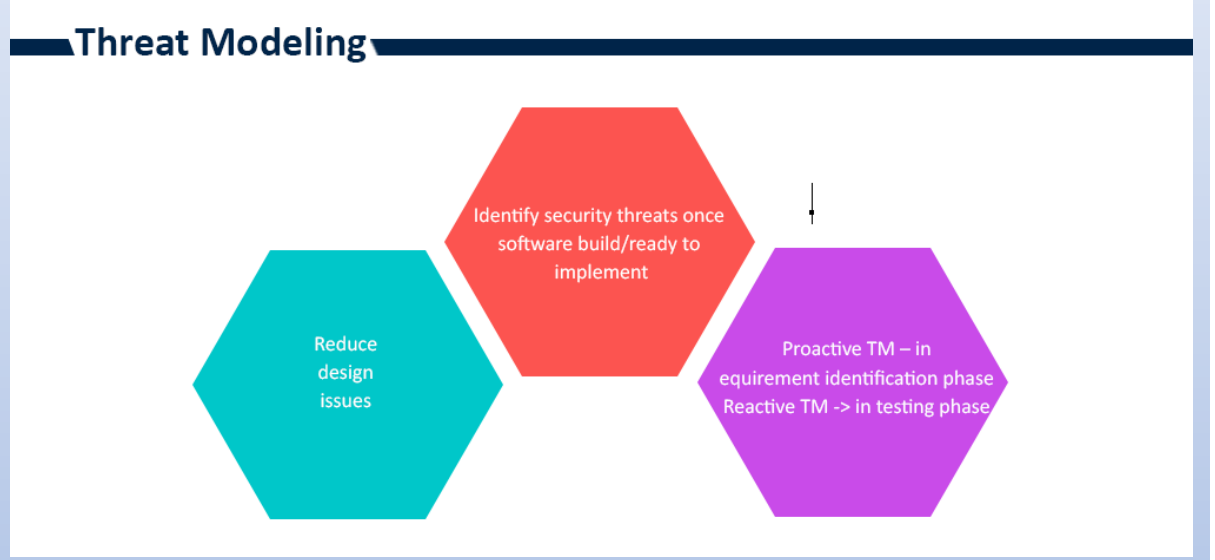
NIST Framework

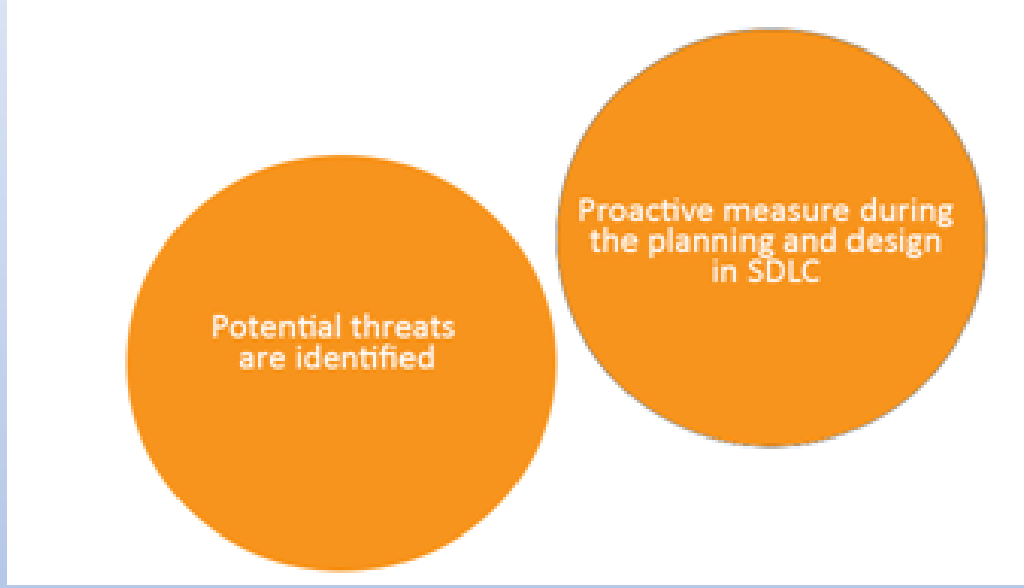
1. Categorize information system
2. Select Security control
3. Implement Security control
4. Assess Security control
5. Authorize information system
6. Monitor Security control

- NIST RMF (SP 800-37)
- ISACA Risk IT
- ISO 31000

Threat Modeling

Structured approach to systematically identify, assess, and mitigate potential Threats and vulnerabilities in software applications, systems, or processes.





Threat Modeling Steps

Threat Modeling Steps

Identifying threats

Identify Asset
Identify Threat
Rate the Threat
Identify Controls

Categorization of threats

STRIDE model

Identify attacks

Data flow diagrams

Reduction Analysis

Trust boundaries

Prioritization and response

DREAD model

Threat Modeling Techniques

STRIDE Approach (Developed by Microsoft)

Identify and categorize potential Threats and risks associated with software applications, systems, or processes

- **Spoofing**
  - Use false identity -> attacker use their false identity
  - Wrong IP, wrong Mac
- **Tampering**
  - Attackers gain access and modify software
  - Someone gain un-authorized access
- **Repudiation**
  - If user denying the activity -> software has features to prove it
  - User did some changes, can software prove denying the activity
- **Identification disclosure**
  - If sensitive info leakage
  - What level of software
- **Denial of Service (DoS)**
  - If attacker succeed to attack on software or hardware
- **Elevation of Privilege**
  - limited user account transformed with greater privileges, powers and access