Introduction to Cybersecurity

Chapter 5

Risk Assessment and Management

Cyber Defense (Next 4 Chapters)

Chapter 5. Risk assessment and Management

Chapter 6. Standard and Polices

Chapter 7. Endpoint Security

Chapter 8. Physical Security

Chapter 5: Risk assessment and Management

- IT Security Management Process
- Security Risk Analysis
- Risk Assessment Process
- What is Risk?
- Risk Levels
- Risk Level Scoring
- Ways of Treating Risk
- Explain the Risk Equation
- Cybersecurity Frameworks
- NIST CSF
- Creating a Risk Register
- Defense in Depth
- Defending the Enterprise

Would you rather have your social media hacked or your bank account hacked?

Why made you choose one over the other?

What is the biggest cybersecurity risk you face in your daily life?

- Phishing emails, weak/reused passwords, data breaches, public Wi-Fi, unpatched software, data leaks, fake software, , theft, robbery, social engineering

Now, imagine this on an enterprise scale! There are so many things you need protection from

What would you protect?
Can you protect everything?

How to Assure Security: Risk Management

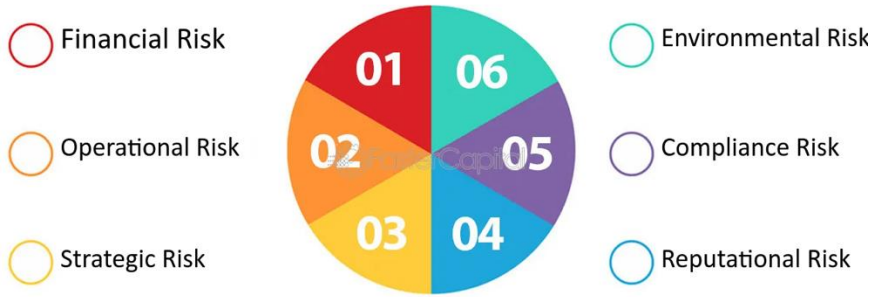
- We cannot secure everything!!
- Different vulns have different financial impacts
- We must prioritize remediation
- What is the business context?
- Information security becomes “risk management”

- Risk management is the process of identifying, analyzing, assessing, and mitigating potential risks that could negatively impact an organization, system, or individual

- Proactive approach to minimizing uncertainties and ensuring business continuity, security, and financial stability.

Types of Risk in Cybersecurity

- Financial Risk
  - Fraud, loss of revenue due to cyberattacks
- Operational Risk
  - System downtime, data breaches, ransomware attacks
- Compliance Risk
  - Violating regulations like GDPR, HIPAA, PCI-DSS
- Reputational Risk
  - Loss of customer trust after a security breach
- Strategic Risk
  - Poor decision-making due to lack of risk assessment
  - Not investing in security infrastructure can result in major data breaches
- Environmental Risk
  - Risks related to natural disasters or external factors affecting IT systems



Top Jobs in Risk Management

1. Cyber Risk Analyst
   - Skills: Risk assessment frameworks (NIST, ISO 27001), threat modeling, compliance knowledge
   - Certifications: CISSP, CRISC, CISM, $80,000 - $120,000 per year

2. Information Security Risk Manager
   - Skills: Cybersecurity frameworks, governance, risk management tools, business continuity planning
   - Certifications: CISM, CISSP, ISO 27001 Lead Implementer, $100,000 - $150,000 per year

3. Governance, Risk, and Compliance (GRC) Analyst
   - Skills: Compliance audits, risk reporting, regulatory frameworks
   - Certifications: CISA, CRISC, CGEIT, $85,000 - $130,000 per year

4. Risk and Threat Intelligence Analyst
   - Skills: Threat intelligence platforms (TIPs), OSINT, malware analysis
   - Certifications: CEH, GIAC, Security+, $90,000 - $140,000 per year

5. Chief Risk Officer (CRO)
   - Skills: Leadership, enterprise risk management (ERM), strategic planning
   - Certifications: FRM, PRM, CRISC, $150,000 - $300,000 per year

Note: Salaries and roles vary based on experience, location, and industry. Entry-level positions may start lower, while advanced roles offer higher pay. Gaining certifications and experience improves job prospects but there are no guarantees.

IT Security Management

- To effectively manage risk, organizations follow standardized security management processes
- **IT Security Management** is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability

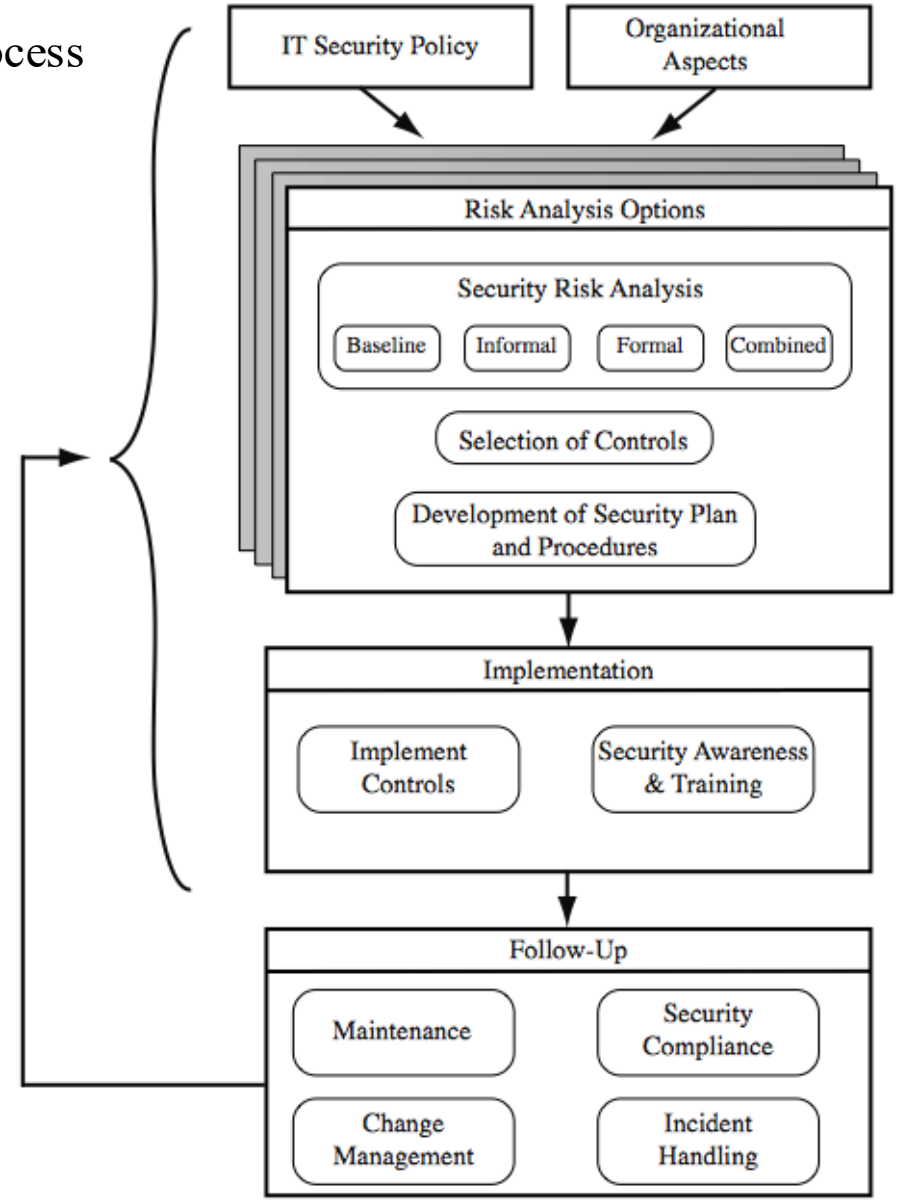
- IT security management functions include:
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security assets and requirements
  - **identifying and analyzing security threats to IT assets**
  - **identifying and analyzing risks**
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implement a security awareness program
  - detecting and reacting to incidents

IT Security Management Process

Is the formal process of answering the questions:

- Ensures that critical assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

IT security management process



[**ISO13335**] provides a conceptual framework for managing security

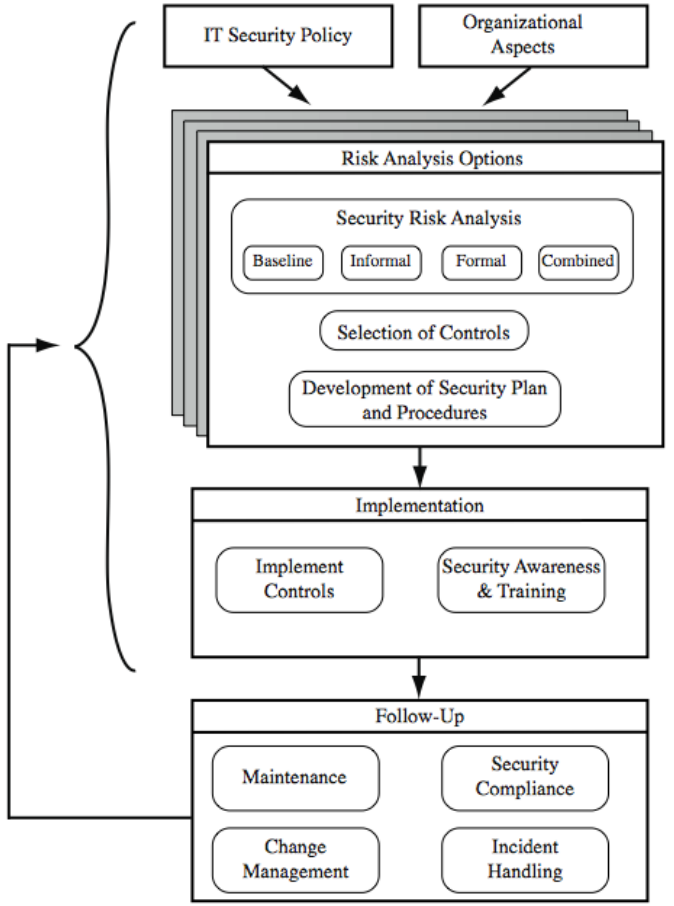
superseded by more modern and comprehensive security frameworks


pixelplex
8 essential cybersecurity risk management frameworks
NIST cybersecurity framework
FAIR framework
ISO 27001 & 27002
PCI-DSS
SOC2
HIPAA
CIS Controls
GDPR

More Later

Security Risk Analysis

- Critical component of IT security management process
  - ➢without it there is a significant chance that resources will not be deployed where most effective
  - ➢may have vulnerabilities or waste money
- Ideally examine every asset vs risk
  - ➢not feasible in practice
- Choose one of possible alternatives based on organization's resources and risk profile
  1. baseline
  2. informal
  3. formal
  4. combined



1. Baseline Approach

- Uses a predefined set of security controls based on industry standards and best practices
- Implement safeguards against most common threats
- Forms a good base for further security measures
- Doesn’t require the expenditure of additional resources in conducting a more formal risk assessment
- Use “industry best practice”
  - easy, cheap, can be replicated
  - but gives no special consideration to organization and applications
  - may give too much or too little security
- Baseline recommendations and checklist documents available from various bodies
- Recommended for small organizations without resources

Example Baseline

A small business follows NIST Cybersecurity Framework recommendations to implement a firewall, antivirus software, and employee security awareness training without conducting a detailed risk assessment

A university IT department follows the CIS (Center for Internet Security) Controls to secure their campus network. They implement basic password policies, software patching, and firewall rules based on standard security frameworks, without conducting an in-depth risk assessment

2. Informal Approach

- Conduct informal, experience-based risk analysis on organization's IT systems
- Relies on expert judgment and knowledge of analysts
- Risks are assessed based on qualitative evaluations rather than quantitative data
- **Advantages**:
  - Fairly quick and cheap
  - Addresses some organization-specific risks
  - Suitable for environments where security risks change frequently
- **Disadvantages**:
  - Some risks may be incorrectly assessed pr overlooked
  - Biased by analysts views, varies over time
  - Difficult to justify to regulators or external stakeholders

- Suitable for small to medium sized orgs where IT system is not necessarily essential (security is important but does not require formal risk analysis)

Example: Informal

An IT manager at a startup identifies potential risks by interviewing employees, reviewing past incidents, and making security improvements without using formal documentation or methodologies

A retail store owner suspects Wi-Fi security risks and asks an IT consultant to perform a quick check. The consultant notices that the store’s wireless network lacks encryption and recommends switching to WPA3 encryption and updating the router firmware. There is no formal documentation, just expert advice and quick fixes.

3. Formal Risk Analysis

- A structured and comprehensive analysis with clearly defined steps
- Uses quantitative and qualitative risk assessment models
- Necessary for organizations handling sensitive data
- Often required by regulatory standards (e.g., ISO 27005, NIST RMF)
- Evaluates risk based on likelihood, impact, and mitigation measures

- **Advantages**:
  - Provides a detailed and accurate assessment of risks
  - Ensures compliance with legal and industry standards
  - Helps in budgeting and resource allocation for risk mitigation
- **Disadvantage**: Costly and slow, requires expert analysts

- Suitable for large organizations with IT systems critical to their business objectives

Example: Formal Risk Analysis

A hospital conducting a HIPAA compliance assessment follows a structured risk assessment process, including threat modeling, impact analysis, and formal documentation to evaluate patient data security risks

A government agency handling classified data performs a detailed risk assessment using FAIR (Factor Analysis of Information Risk) methodology. They quantify the financial impact of data breaches, insider threats, and cyber-attacks, document the findings, and implement controls aligned with NIST 800-53 standards

4. Combined Approach

- Mixes elements of baseline, informal, and formal approaches
- Starts with baseline security measures on all systems
  - Uses informal analysis to identify all critical risks
  - Conducts a formal risk assessment on these systems
  - Iterated and extended over time
- Advantages:
  - Cost effective while addressing key risk, better use of time and resources
  - Better security initially that evolves over time
- Disadvantages:
  - May miss some risks early, initial implementation may be complex
  - Requires continuous monitoring and updating
- Best for most large organizations or enterprises that need both efficiency and security.

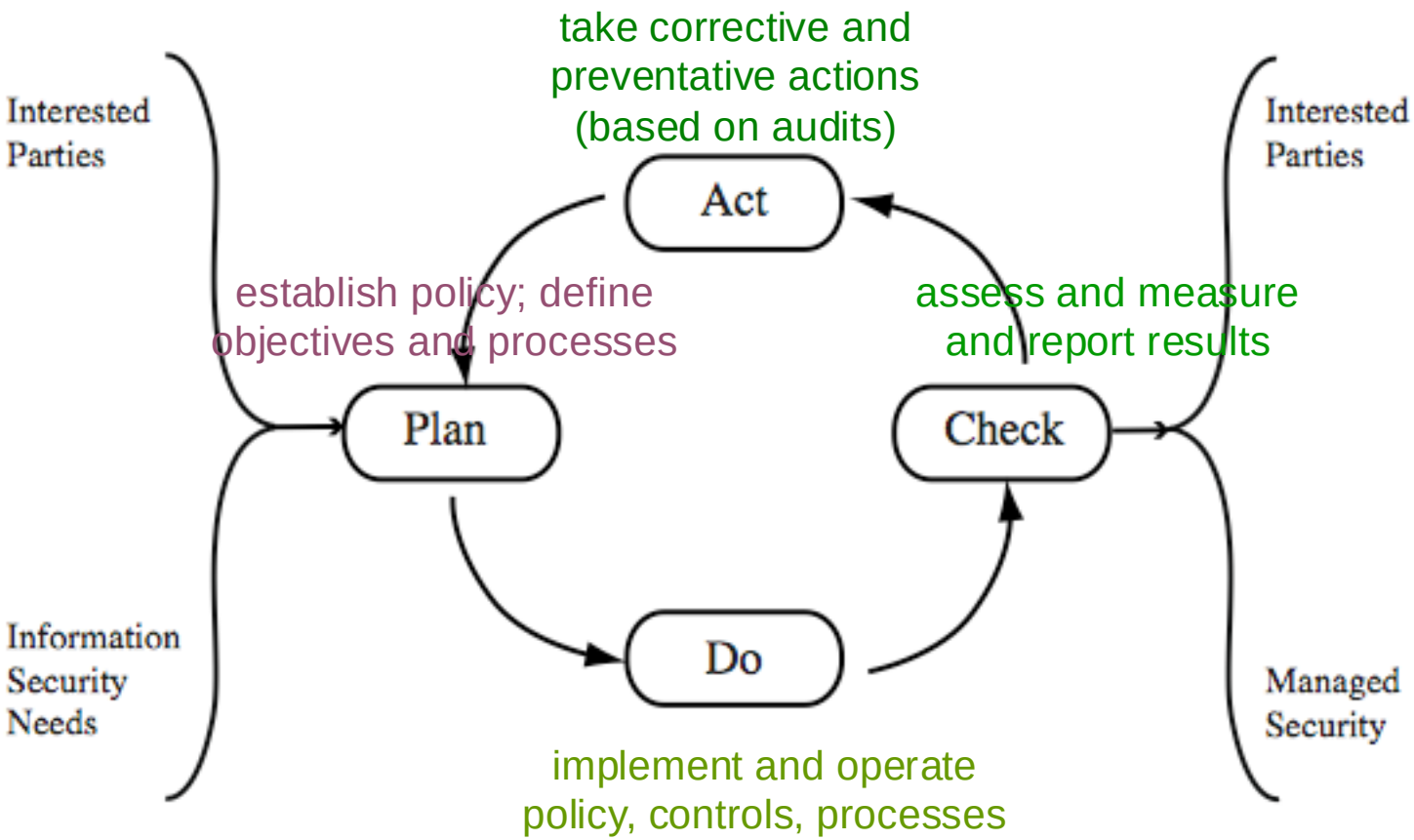
Example: Combined Approach

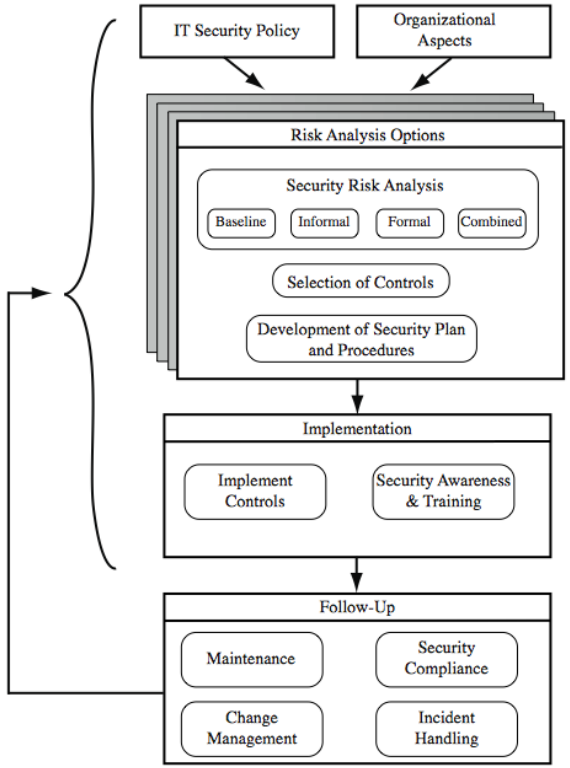
A financial institution uses a baseline approach for general security controls, informal discussions for emerging threats, and formal risk assessments for compliance with PCI DSS (Payment Card Industry Data Security Standard)

A health insurance company uses a baseline approach for general security controls (e.g., firewalls, MFA, access controls), an informal approach for evaluating new threats in emerging AI-based fraud detection, and a formal risk assessment for meeting HIPAA and GDPR compliance requirements

Plan - Do - Check – Act (PDCA Model)

- Alternate model process for managing information security [ISO27001]
- This standard details a model process for managing information security





ISO13335 Model

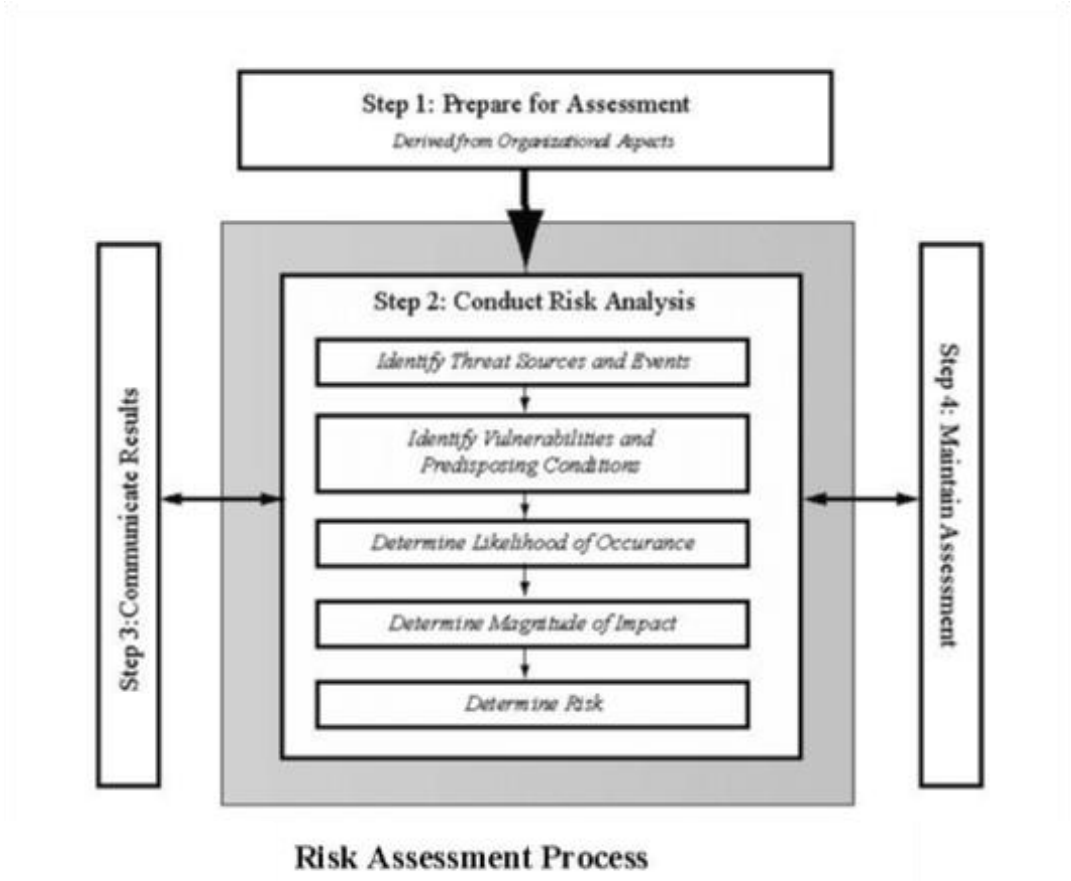
What is Cyber Risk?

- Cyber risk is the probability of exposure or potential loss resulting from a cyber attack or data breach

- Cyber risk encompasses damage and destruction of data, monetary loss, theft of intellectual data, productivity loss and reputational damage

Risk Assessment process

Critical component of cybersecurity risk management and follows a step-by-step methodology to evaluate threats, vulnerabilities, and potential impacts on an organization



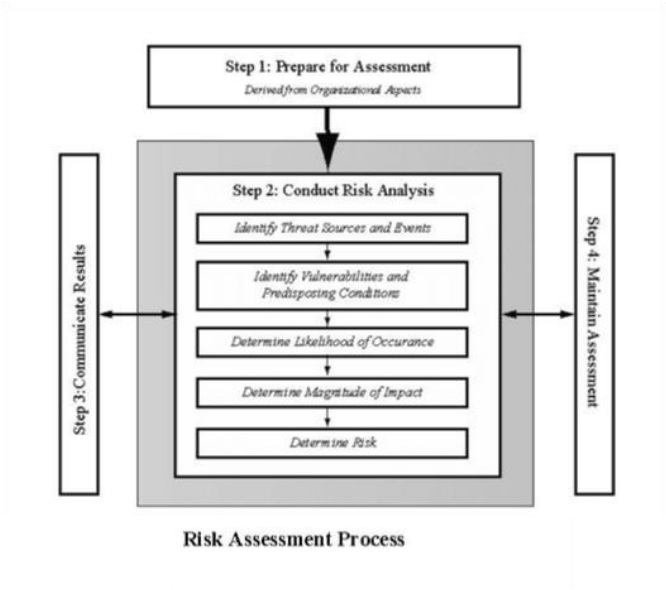
Risk Assessment Process

Step 1: Prepare for Risk assessment

- Establishes the scope, objectives, and methodology of the risk assessment
- Defines what will be assessed (e.g., systems, networks, applications)
- Identify Business goals and regulatory requirements
- Identify the assets to be examined
- Identify Existing security policies and risk tolerance levels

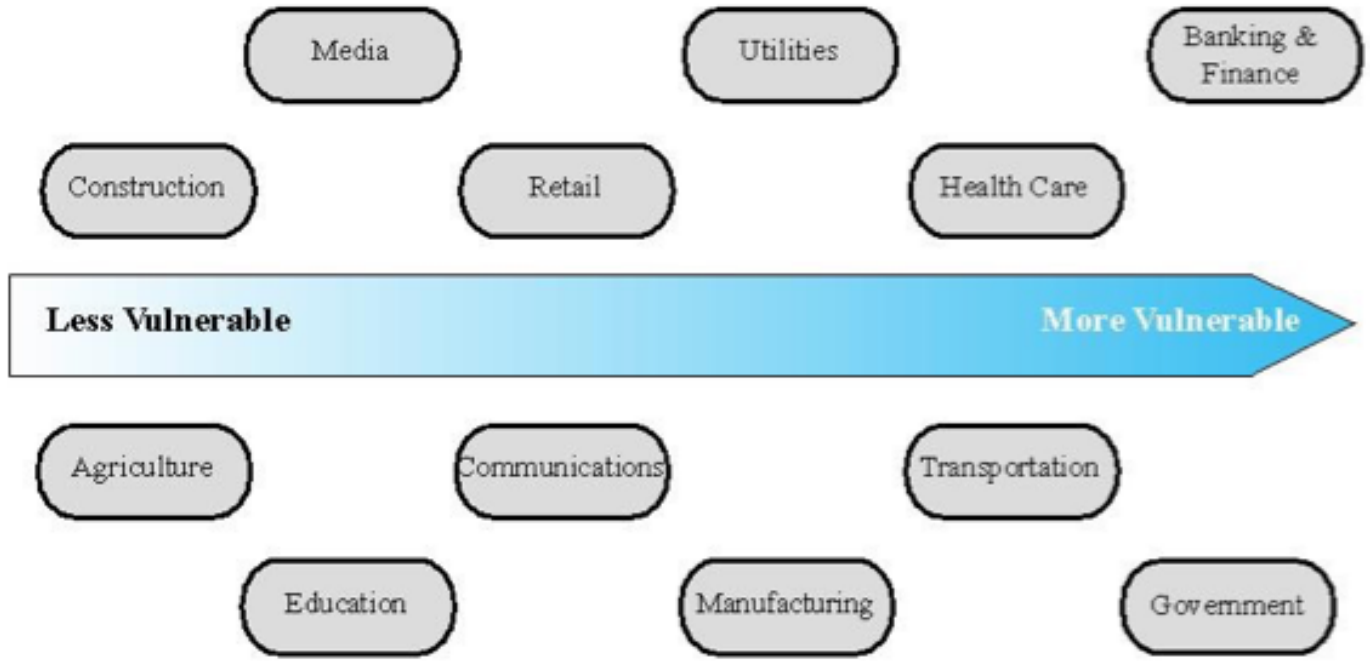
- Explores political and social environment in which the organization operates
- Explore external factor:
  - ➢Legal and regulatory constraints
  - ➢Provide baseline for organization's risk exposure

- Determine Risk appetite- level of risk the organization views as acceptable



Risk Assessment Process

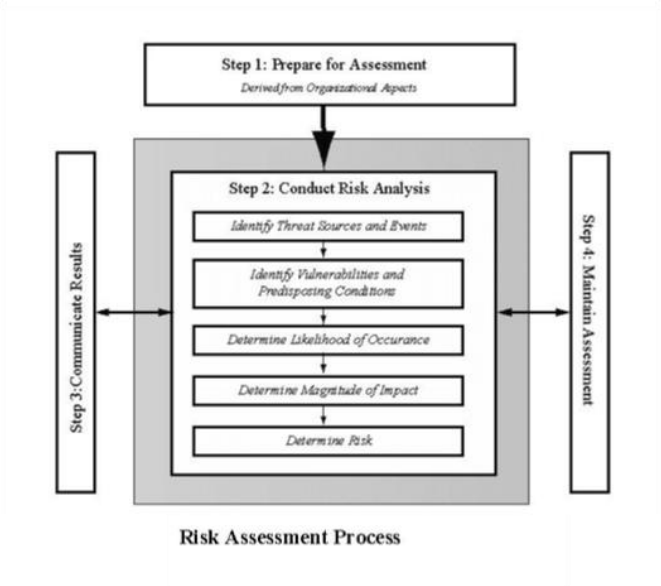
Prepare for Risk assessment: Industries Ranked by Vulnerability



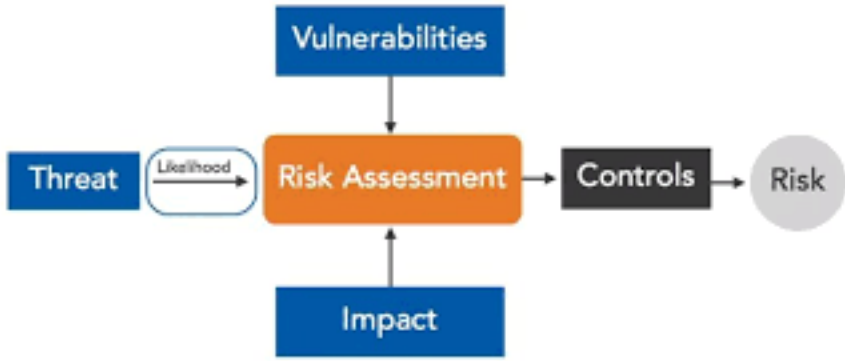
Generic Organizational Risk Context

Step 2: Risk Assessment Process

1. Identify Threat Sources and Events
   - Determine what could pose a security risk (e.g., hackers, phishing attacks, system failures).
2. Identify Vulnerabilities
   - Assess weaknesses that could be exploited (e.g., weak passwords, outdated software)
3. Determine Likelihood of Occurrence
   - Calculate the probability of a cyber event happening
4. Determine Magnitude of Impact
   - Assess how severe the consequences would be if a threat materializes
5. Determine Overall Risk
   - Use the Risk Equation [More Later]
   - Categorize risks into Low, Medium, High, and Critical



Risk Assessment Process



Assets Identification

- Identify key assets to examine
- In risk management, an asset is anything of value to an organization that needs protection from potential threats
- Assets can be tangible (physical) or intangible (non-physical) and are classified based on their importance, sensitivity, and impact if compromised

- Examples:
  - Tangible (Physical): Servers, laptops, IoT devices, network infrastructure.
  - Intangible (Non-physical): Customer data, emails, financial records, intellectual property.
  - Critical assets: Bank accounts, employee records, vendor access credentials, CCTV security footage

Risk Identification

- Risk identification process requires identifying the threats and vulnerabilities that exist in an operating environment

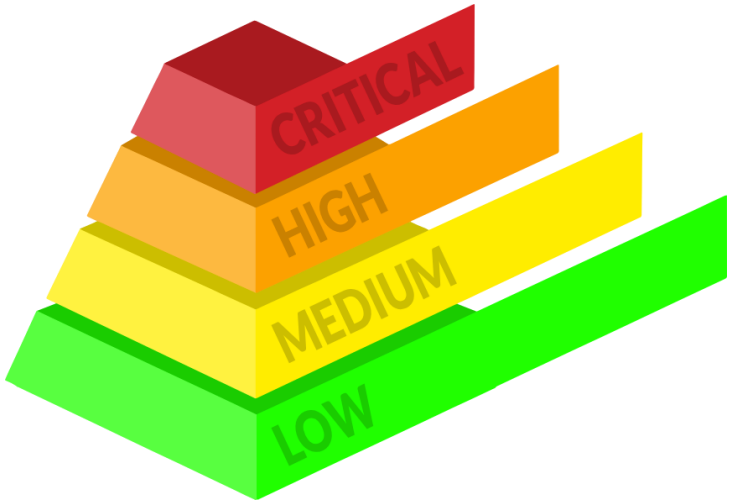
- Risk categories:
  - **External risk** is a risk originating from a source outside the organization
    - Ex: Cybersecurity adversaries, malicious code, malware, and natural disasters
  - **Internal risk** is a risk originating from within the organization
    - Ex: Malicious insiders, mistakes made by authorized users, equipment failures
  - **Multiparty risk** is a risk impacting more than one organization
    - Ex: A power outage in a city, Cloud service provider outage, compromise of a SaaS provider's database- affecting the information of many different customers
  - **Legacy systems risk** is a risk from outdated systems
    - Outdated systems often do not get security updates and cybersecurity professionals must take extraordinary measures to protect the systems against unpatchable vulnerabilities

Risk Level

The risk levels are categorized based on three key factors in risk assessment:

1. Likelihood (Probability of Occurrence) – How likely it is that the risk event will happen
2. Impact (Consequence if Exploited) – The severity of damage if the risk materializes
3. Mitigation Capability – The ability to control, prevent, or minimize the risk

- Critical
- High
- Medium
- Low
- No Risk



Critical Risk

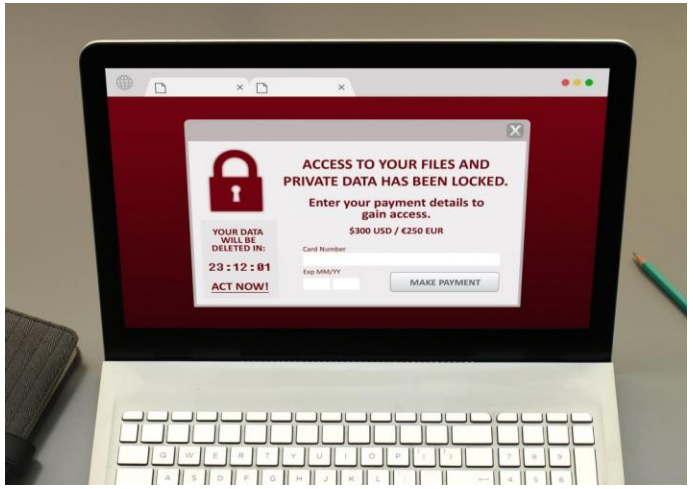
- A critical risk status indicates that a system has a severe and immediate risk of destructive events
- High probability of occurring, severe impact

- A critical risk event could include:
  - ➢Complete network failure or shutdown
  - ➢Essential application failure
  - ➢Compromise resulting in the loss of system or administrative controls
  - ➢Compromise resulting in the loss of data vital to the organization

Example: A zero-day vulnerability in financial software allowing hackers to steal customer data

High Risk

- High probability, slightly lower impact than critical risks
- Causes major disruptions but may not be catastrophic
- Needs urgent action to prevent escalation



High-risk events may include:

- Multiple virus attacks causing significant damage or disruption
- Unreliable systems and equipment
- Cyberattack resulting in the loss of administrative authority
- A major weakness resulting in high vulnerability

Example:

- A ransomware attack locking employees out of systems but not affecting customer data
- A misconfigured cloud storage bucket exposing millions of customer records

Medium Risk

- Medium-to-low probability of occurring
- Moderate damage if exploited, manageable impact
- Should be mitigated but may not be an immediate priority

Medium risk events may include:

- A cyberattack that has created a moderate impact on systems—things are not shut down, but productivity has been impacted
- A security compromise of non-sensitive information
- A security compromise may be reported, but damages are not yet detected
- A virus detected with the potential to spread

Example:

- An employee using weak passwords that could be brute-forced but is protected by MFA
- A third-party plugin with outdated security measures that could be exploited if not patched

Low Risk

- Low probability of occurring (unlikely to happen)
- At a low-risk status, your network activity is deemed normal
- low impact- Minimal damage if exploited
- Requires monitoring but may not need urgent mitigation

Low-risk events may include

- A small virus that is quickly contained and/or causes little damage
- Phishing emails identified and isolated by proper software
- Delayed minor software updates or minor maintenance patches

Example:

- A minor software bug causing display errors in a non-critical application
- Non-critical service running an outdated SSL certificate that does not impact functionality

No Risk?

- A scenario where a system, asset, or process has no identified vulnerabilities, threats, or impact
- Zero Likelihood, No impact
- Example:
  - A fully air-gapped system with no external network connections and no attack vectors
  - A patched and monitored system with multi-layered security, showing no active threats

- Absolute "No Risk" is rare—risks evolve over time
  - Every system, process, or asset has some degree of risk due to evolving threats, human error, or unforeseen vulnerabilities

- Continuous monitoring and proactive security are needed

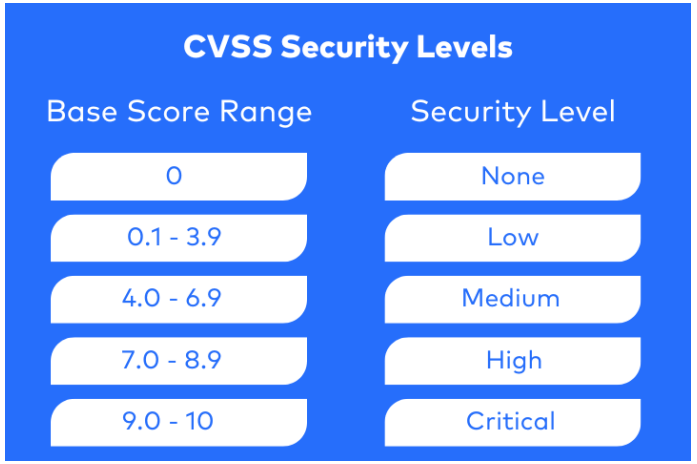
Risk Level Score

- CIS and NIST cybersecurity frameworks recognize various levels of cybersecurity risk

- A **CVSS (Common Vulnerability Scoring System)** score is calculated based on the potential damage level and the likelihood of an attack on that vulnerability

- Scores range from 0 to 10: A higher score indicates a more severe vulnerability
- Used by companies, governments, and industries to assess risks and develop action plans
- CVSS helps IT teams decide which vulnerabilities to fix first

CVE (Common Vulnerabilities and Exposures) is just an identifier for tracking security vulnerabilities (e.g., CVE-2021-44228 for Log4Shell)



SOURCE: https://www.getastra.com/blog/security-audit/cvss/

CVSS versions

- CVSS v2 (2007)
  - Introduced the first structured vulnerability scoring system but lacked granularity and cross-boundary risk assessment
  - If working with legacy systems, you may still see CVSS v2 scores

- CVSS v3.0/3.1 (2015/2019)
  - Improved scoring with Privileges Required, Scope metric, and refined impact ratings but still lacks exploitability details
  - CVSS v3.1 remains widely used and is supported by NIST's National Vulnerability Database (NVD)

- CVSS v4.0 (2023)
  - Added Automated Exploitability, Passive vs. Active User Interaction, and better risk granularity for IoT and cloud security
  - CVSS v4.0 is the most accurate and detailed, ideal for modern threats, but adoption is ongoing

a. Base Metrics

- Base metrics represent the core characteristics of a vulnerability and do not change over time
- Provides a starting point for understanding the inherent risk of a vulnerability

Key base metrics include:

- **Exploitability**: Measures how easy or difficult it is to exploit the vulnerability
  - Factors like attack vector (how the attack can be launched), attack complexity (how complicated the attack is), and privileges required (level of access needed) contribute to this metric
- **Scope**: Indicates whether the vulnerability affects just one system or can propagate to other systems
- **Impact**: Evaluates the consequences of a successful exploit on confidentiality, integrity, and availability

b. Temporal Metrics

- Temporal metrics consider changes over time, such as the availability of patches or exploit code
- This score can fluctuate as new information becomes available

Key temporal metrics include:

- **Exploit Code Maturity**: Measures the development and spread of an exploit that takes advantage of the system weakness
- **Remediation Level**: Indicates whether a patch or fix is available or not
- **Report Confidence**: Reflects the level of certainty that the vulnerability exists and can be exploited

c. Environmental Metrics

- Environmental metrics allow organizations to adjust the Base score based on their specific infrastructure and security requirements
- Helps tailor the score to the organization’s unique risk profile

Key environmental metrics include:

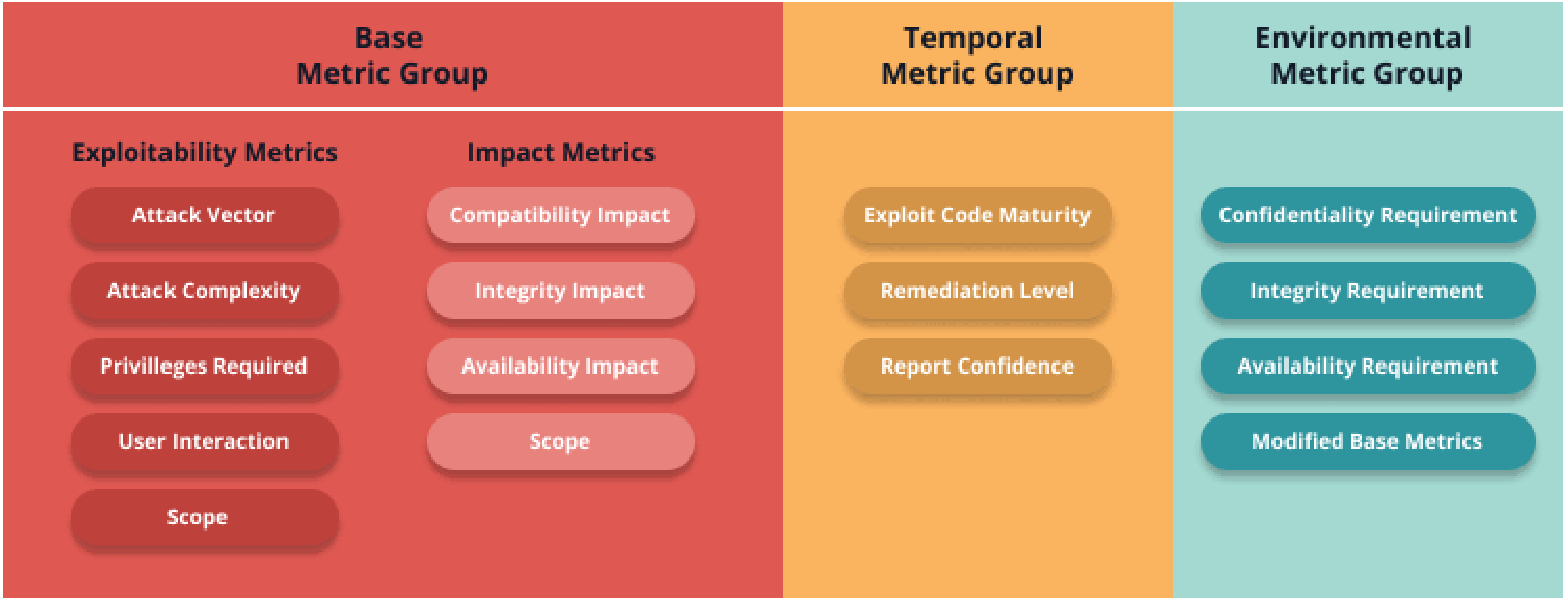
- **Security Requirements**: Assesses the criticality of the system affected by the vulnerability

- **Modified Base Metrics**: Allows adjustments to Base metrics depending on existing mitigation measures

SECURITYIUM

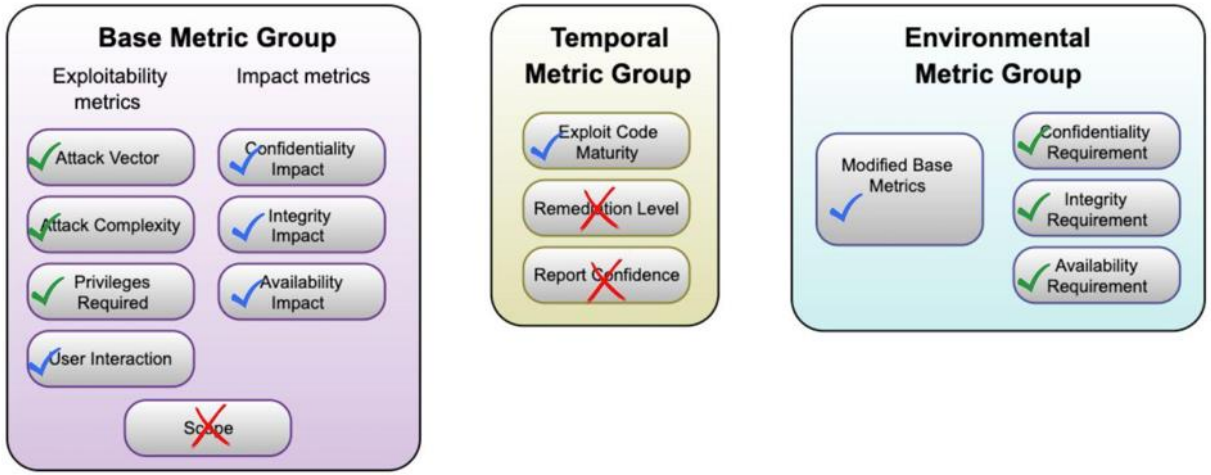
CVSS Score Metrics

A CVSS score is composed of three sets of metrics (**Base**, **Temporal**, **Environmental**), each of which have an underlying scoring component.

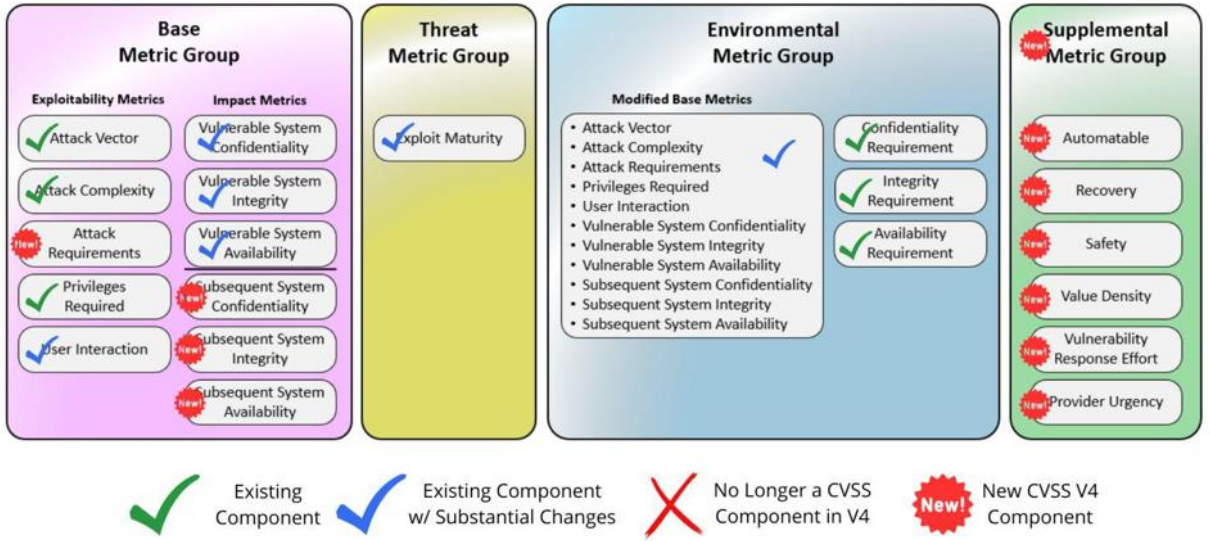


Source: https://www.securityium.com/understanding-the-common-vulnerability-scoring-system-cvss-a-complete-guide/

Common Vulnerability Scoring System v3.1



Common Vulnerability Scoring System v4



Source (Read this): https://tuxcare.com/blog/the-transition-to-cvss-v4-0-what-you-need-to-know/

Example: CVSS

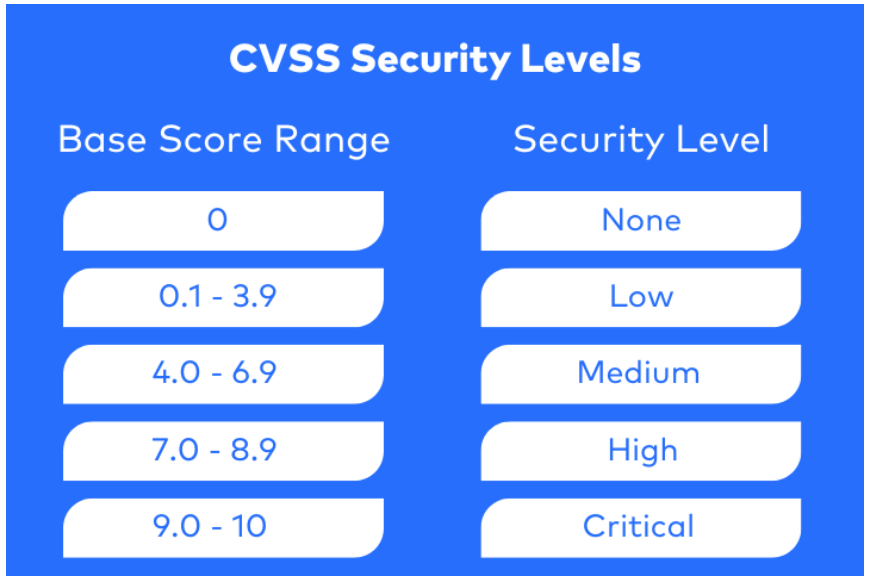
- Let’s say a vulnerability allows unauthorized access to confidential data on a web application

1. Base score might be high because it’s easy to exploit remotely, and the impact on confidentiality is severe
2. If a patch has been released, the Temporal score would lower the overall risk
3. If the organization has strong internal controls, the Environmental score could further reduce the vulnerability’s final risk level

Exercise: Can you categorize the following CVE based on score?

Search NVD: https://nvd.nist.gov/vuln/search

- **CVE-2021-34527**
- CVE-2021-26855
- CVE-2021-21985
- CVE-2021-22986
- **CVE-2024-29099**

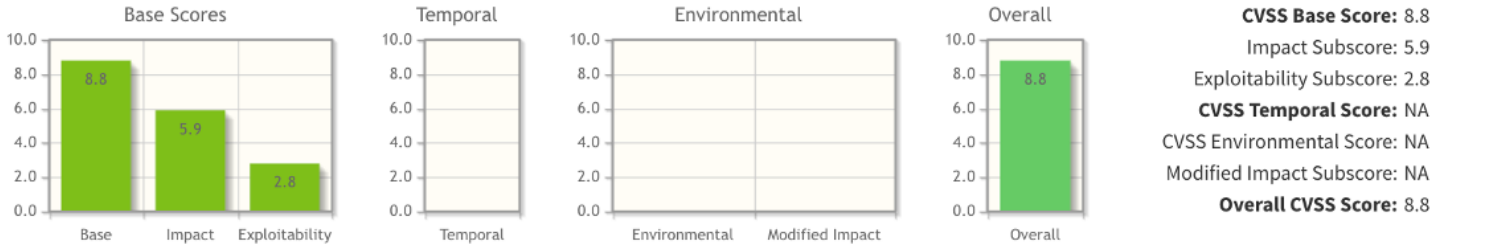


https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Common Vulnerability Scoring System Calculator

Source: NIST

This page shows the components of a CVSS assessment and allows you to refine the resulting CVSS score with additional or different metric values. Please read the CVSS standards guide to fully understand how to assess vulnerabilities using CVSS and to interpret the resulting scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

* All base metrics are required to generate a base score

Activity: Common Vulnerability Scoring System Calculator

- A Heap Buffer Overflow in Google Chrome refers to a memory corruption vulnerability where an application writes more data to a dynamically allocated memory buffer (heap) than it can hold, leading to crashes or potential arbitrary code execution
- Allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page

Can you calculate CVSS base score for this?

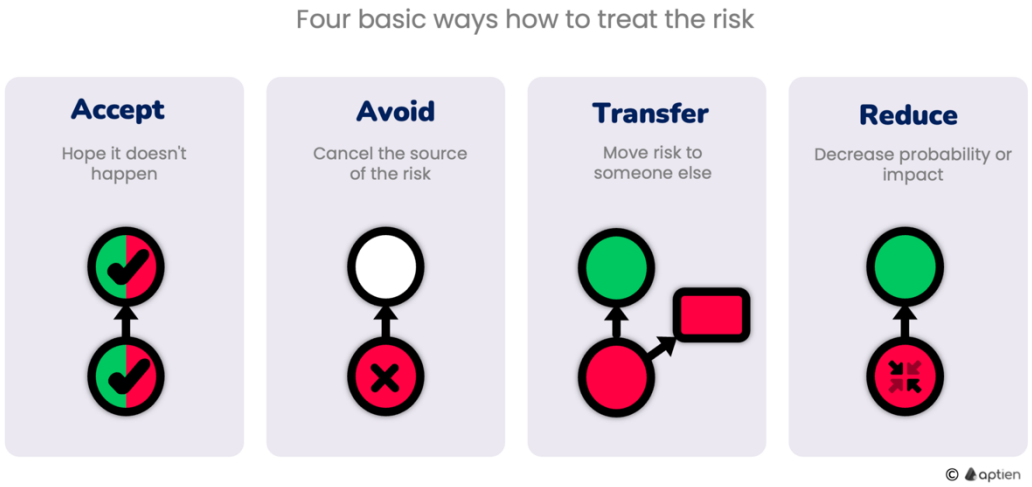
Who uses CVSS?

- Cybersecurity Professionals: Analysts, Incident Responders, Pen Testers
- IT & Network Administrators: Prioritize patching & risk management
- Security Vendors & Researchers: Rate vulnerabilities, threat intelligence
- Government & Regulatory Bodies: NIST, CISA, compliance enforcement
- Software Developers & DevOps: Secure coding & patching
- Cyber Insurance Providers: Risk assessment & policy pricing
- Managed Security Service Providers (MSSPs): Client security management

Once you have identified and assessed a risk, the next step is deciding how to respond to it

How Do We Handle Risk?

- Managing risks effectively ensures business continuity, data protection, and compliance with security standards
- Since no system is 100% secure, organizations must decide how to respond to different levels of risk
- There are four fundamental strategies organizations use to treat risks based on their severity and impact
- These strategies help determine how to minimize risks in a cost-effective way



What: The Four Ways of Treating Risk

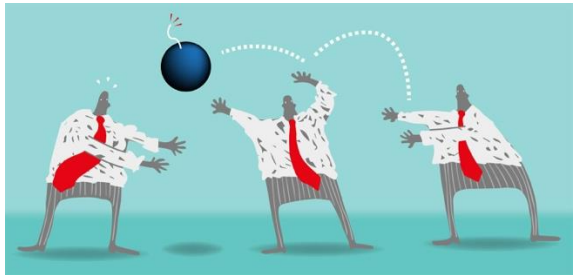
Avoid is a risk management strategy where an organization changes the business practices to completely eliminate the potential that a risk will materialize

- Identify as many threats or vulnerabilities as possible and implement strategies to mitigate those threats, reducing the impact of an attack
- Can be achieved through training and education, and implementing technical security controls and safeguards
- Include measures such as refraining from using vulnerable software or discontinuing certain activities that pose significant cybersecurity risks

Examples: Avoid Risk

- A healthcare provider stops using cloud storage to prevent potential data leaks
- A company removes USB ports from all computers to prevent malware infections
- A financial institution bans employees from using personal email on work devices
- A government agency blocks access to all social media sites on corporate networks
- A software firm stops supporting a risky third-party plugin to avoid vulnerabilities.

What: The Four Ways of Treating Risk



Transfer shifts some of the risk's impact from the organization experiencing the risk to another entity

- Transfer to third-party vendors or external service providers who have specialized expertise in managing cybersecurity risks
- Typically an insurance company
- Enables businesses to offset the financial burden of potential cyber-attacks or security breaches and ensures they have the necessary resources to recover and mitigate any damages

- Examples:
  - A company purchases cyber insurance to cover potential data breaches
  - A hospital contracts a cybersecurity firm to handle network security monitoring
  - A business signs an agreement with a cloud provider to handle data protection

What: The Four Ways of Treating Risk

Accept is choosing to take no other risk management strategy and to simply continue operations as normal despite the risk

- May occur when the risks are deemed to be acceptable or when the cost of mitigation outweighs the potential impact of the risk

- Examples:
  - A company continues using an old operating system despite minor security flaws
  - A small business does not invest in cybersecurity training due to limited resources
  - A university allows students to use weak passwords but monitors login attempts
  - A startup does not implement strict data encryption for non-sensitive files
  - A retailer does not upgrade its security cameras due to low perceived threat

What: The Four Ways of Treating Risk

Reduction/Mitigation is the process of applying security controls to reduce the probability and/or magnitude of a risk

- Risk mitigation strategies include disaster recovery plans, incident response plans, and business continuity plans
- Measures such as encryption, firewalls, and stronger passwords

Examples:

- A company enforces multi-factor authentication (MFA) for all employee logins
- A retailer encrypts all customer payment transactions to prevent fraud
- A university regularly updates and patches its software to prevent vulnerabilities
- A hospital implements strict access controls to limit unauthorized patient record access
- A corporate office installs firewalls and intrusion detection systems to monitor threats

What: The Four Ways of Treating Risk

Residual risk: there is always some remaining risk!!

- Remaining level of risk following the development and implementation of the control mechanisms

- Even after implementing firewalls and antivirus software, there is still a risk of zero-day attacks
- Encrypting data reduces the risk of breaches, but insider threats or misconfigurations can still expose data
- A company uses multi-factor authentication (MFA), but phishing attacks can still trick users into giving credentials

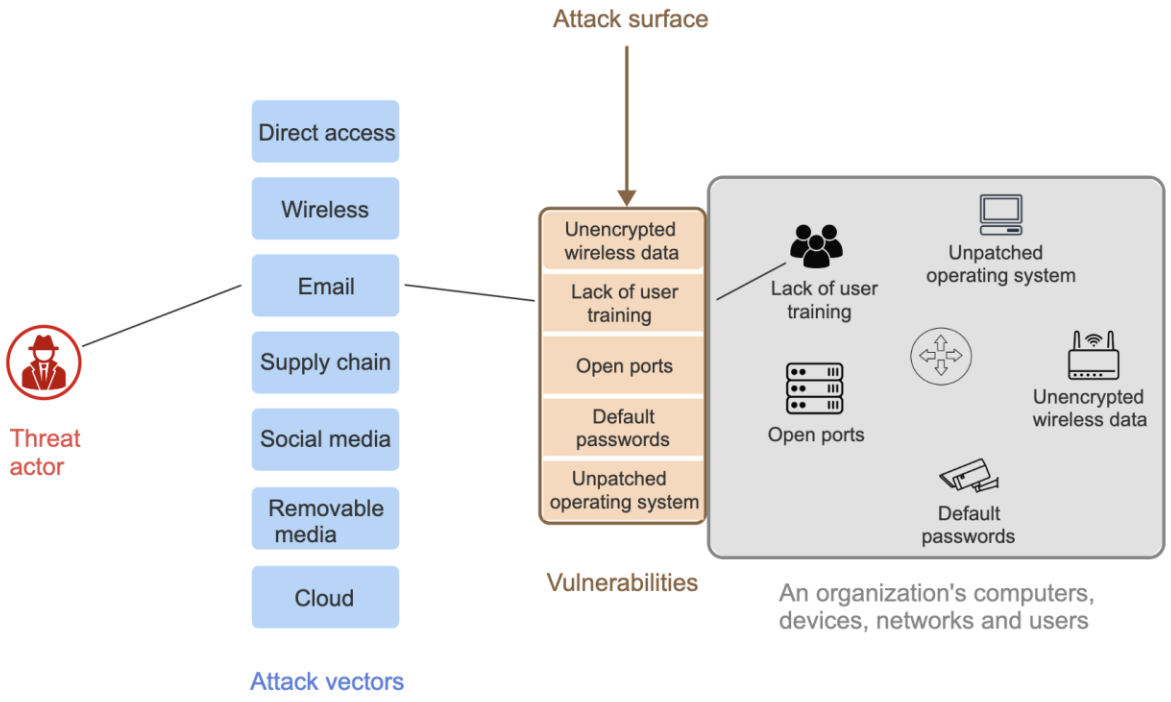
- Watch this video. Which of the four ways is being used?

Understanding Threats

- Threat needs threat actor and opportunity
- Chained up pit bull is not a threat
- You need to understand who might attack your organization (threat actors)
  - Nation states
  - Disgruntled employees
  - Competitors
  - Hackers
  - Very few individual attackers these days

What is an Attack Surface?

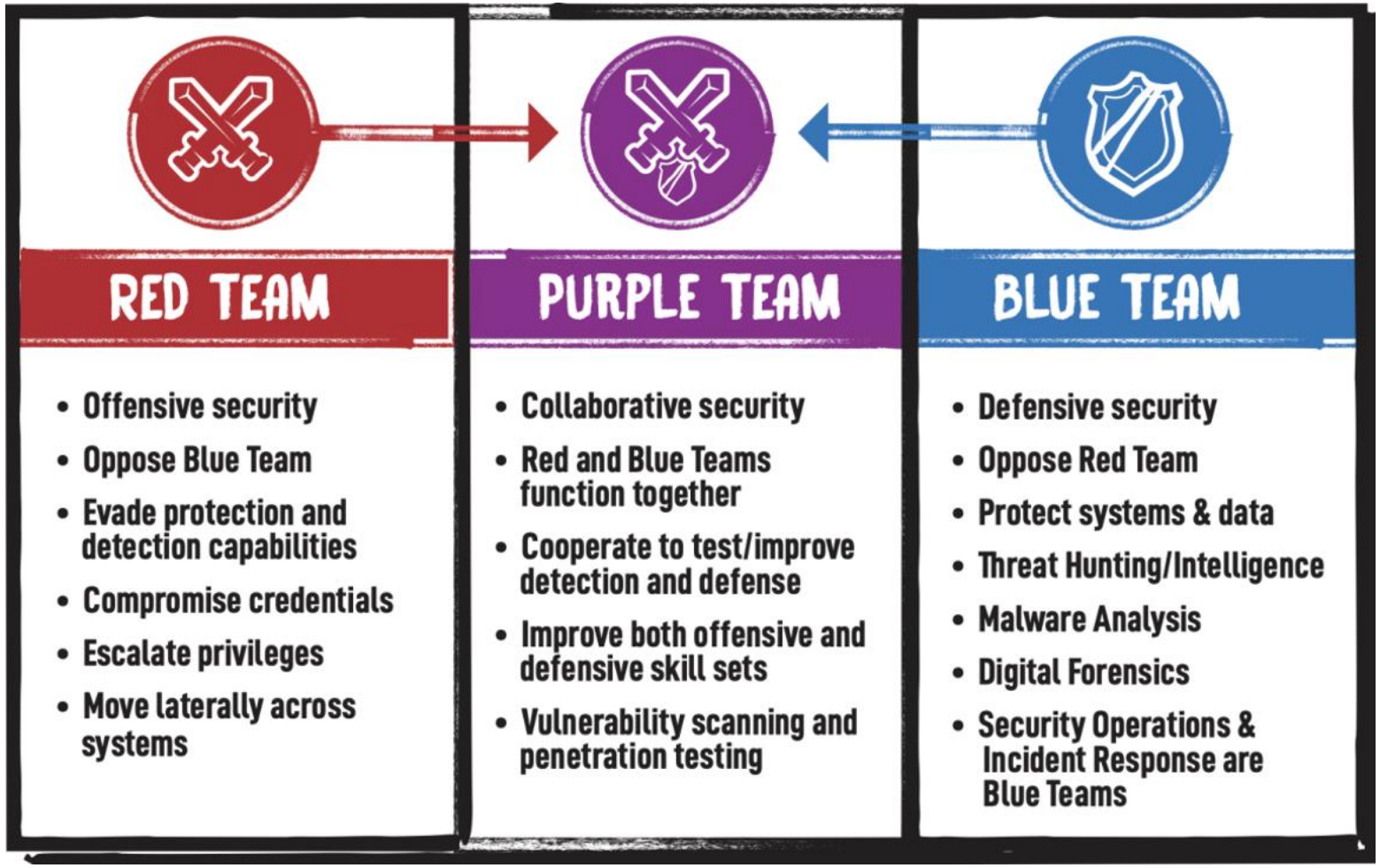
- “Set of entry ways a threat actor could use”
- Example: open ports



Understanding Vulnerabilities

- Application vulnerabilities, OS vulnerabilities
- Coding errors
- Missing patches
  - Organizations don’t patch fast enough
  - PCI says critical patches within 30 days
- Faulty configurations
- OWASP has categorized the “top 10” most common application vulnerabilities that are seen in practice
- https://owasp.org/www-project-top-ten/

Who Finds Vulnerabilities?



https://pentestmag.com/red-teaming-10000-feet/

We Are Protecting Data

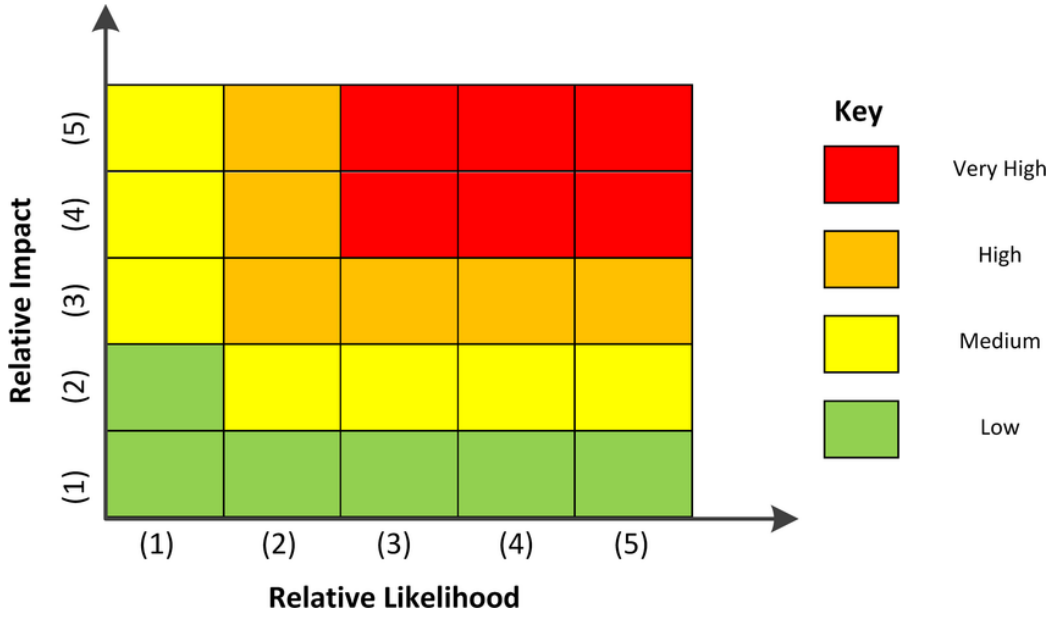
- "It's all about the information"
- **Protecting Data**, not servers, networks or applications
- Valuing data assets: average cost of breach = $11.7m (Accenture Report)
  - Internal costs
    - Detection, investigation, containment
    - Recovery
  - External costs
    - Information loss
    - Business disruption
    - Revenue loss

Key Definitions in Risk Management

- **Threat** – Any potential event or actor that could cause harm to an asset
  - Examples: Hackers, malware, insider threats, natural disasters, phishing attacks
- **Vulnerability** – A weakness in a system or process that a threat can exploit
  - Examples: Unpatched software, weak passwords, misconfigured security settings
- **Risk** – The probability and impact of a threat exploiting a vulnerability to harm an asset
  - Example: If a company stores unencrypted customer data (vulnerability) and phishing attacks (threat) increase, the risk of a data breach is high

Understanding the Risk Equation

- What is the risk equation?
- How do we determine impact?



The Risk Equation

- Risk is defined as the probability of a loss event (likelihood) multiplied by the magnitude of loss resulting from that loss event (impact)

  Risk = Likelihood (Probability of Event) x Impact

  Likelihood = Threat x Vulnerability

  Risk = (Threat x Vulnerability) x Impact

- Three ways of using this: Quantitative, Ordinal scale (ranking, 1 to n), Qualitative (low, medium, high)

- **Key point**: unless you have a threat AND vulnerability AND impact, you have NO risk!
- If Impact is represented in dollars, Risk is in Dollars

Back to the Risk Equation

- Risk = Likelihood x Impact
  - If Likelihood = 10% per year and Impact = $1M, Risk = $100,000 per year
- Likelihood = Threat x Vulnerability
  - Could be qualitative, qualitative, or ordinal

- Threat includes: threat actor and threat action
- Threat actors are a lot like mice
- Mouse video
- Mouse avoiding traps. Trap = “control”

Quantitative Scale

- A quantitative scale is used when risks can be measured numerically, often in monetary terms
- Relies on actual data, historical records, and statistical probabilities to calculate the expected risk impact

- Define the Risk Factors
  - Threat (T): probability (likelihood) of an event occurring, expressed as a **percentage**
  - Vulnerability (V): extent to which an asset is susceptible, represented as a value between **0 and 1**
  - Impact (I): financial or operational consequence if the risk materializes, usually in **dollars**

- Calculate and Interpret the Risk Score
  - A higher risk value suggests significant financial exposure and requires immediate mitigation
  - A moderate risk value may warrant additional monitoring and controls
  - A low risk value might not need immediate action

Quantitative Example

Suppose you're evaluating the risk of a project delay in a construction project

- **Threat** (likelihood of a delay occurring): 30%
- **Vulnerability** (how susceptible the project is to delays)= 0.7 (on a scale of 0 to 1, where 1 means extremely susceptible)
- **Impact** (consequences of a delay): $100,000

Calculate the risk:

Risk = (Threat x Vulnerability) x Impact
Risk = (0.3 x 0.7) x $100,000
Risk = $21,000

In this quantitative example, the calculated risk is $21,000. This means that, based on the given values, the projected cost associated with the risk of a project delay is $21,000

Ordinal Scale

- An ordinal scale is used in risk assessment when risks cannot be precisely quantified in monetary terms but can be ranked relative to each other based on likelihood, or impact
- Define the Risk Factors: Threat (T), Vulnerability (V), Impact (I) (**each rated 1 to 10)**
  - ➢Each factor is assigned a numerical value based on qualitative judgment:

Factor	Low (1-3)	Medium (4-7)	High (8-10)
Threat (T)	Rare occurrence	Occasional occurrence	Frequent occurrence
Vulnerability (V)	Strong defenses, unlikely to be exploited	Moderate risk, some weaknesses	Highly vulnerable, easy to exploit
Impact (I)	Minimal effect	Some disruption	Catastrophic loss

- Interpret the Risk Score
  - ➢A higher score (e.g., 400–1000) indicates a critical risk requiring immediate mitigation
  - ➢A medium score (e.g., 100–400) suggests moderate attention is needed
  - ➢A low score (e.g., below 100) may not require immediate action

Example: Ordinal Scale

Let's say you're assessing the risk of a potential data breach for a small online retailer

- **Threat**: You might identify the threat of a hacker attempting to breach your website. On a scale of 1 to 10, you rate the likelihood of this threat as 8

- **Vulnerability**: You've determined that your website has some security vulnerabilities, which you rate as a 6 on a scale of 1 to 10

- **Impact**: If a breach occurs, it could lead to the loss of customer data and damage to the company's reputation. You rate the potential impact as 9 on a scale of 1 to 10

- Risk = (Threat x Vulnerability) x Impact

  Risk = (8 x 6) x 9 = 432

This score can help you prioritize security measures and allocate resources to mitigate the risk

Qualitative Scale

- A **qualitative scale** in risk assessment is used when numerical data is unavailable or when risks are better expressed in descriptive categories
- Relies on expert judgment, historical trends, and subjective assessments rather than precise calculation
- You use descriptive categories (low, medium, high) to categorize each risk
  - HIGH RISK = severe or catastrophic effect on operation
  - MEDIUM RISK = serious adverse effect on operation
  - LOW RISK = limited adverse effect on operation

Interpret the Results

- Low Risk: Acceptable, monitor periodically
- Medium Risk: Requires mitigation strategies
- High Risk: Requires immediate attention

Example: Qualitative Scale

- If **Threat**: Medium, **Vulnerability**: Medium, **Impact**: High
- To calculate the overall risk, you can simply combine these assessments
- There's no specific numerical value associated with these categories, so the calculation is done qualitatively
- In this case, the overall risk would be considered “Medium to High”

Example: A small business evaluates the risk of a phishing attack.

- Likelihood: ”High" – The business receives frequent phishing emails
- Impact: ”High" – If a phishing attack succeeds, it could expose customer data
- Risk Level = High

Benefits of Calculating Risk

1.Proactive Defense

Identify threats before they're exploited

2.Resource Efficiency

Allocate cybersecurity resources effectively

3.Cost Savings

Avoid financial losses from cyber attacks

4.Prioritization

Focus on high-risk assets and systems

5.Compliance and Regulation

Meet regulatory requirements to avoid penalties and legal issues.

Calculating risk empowers decision-makers to better understand potential challenges, allocate resources wisely, and plan for the future, ultimately leading to more resilient and successful outcomes

Other Benefits Beyond the strategic benefits

Calculating cyber risk helps security teams:

- Communicate cyber risk to senior executives, board members and business risk owners in a common language that everyone understands – monetary terms, like dollars
- Demonstrate the value of their cybersecurity program and provide the ROI for future security investments
- Work with senior executives to determine acceptable levels of risk
- Prioritize the mitigation of cyber security risks based on their potential business impact

Creating a Risk Register

- What is the risk register?
- Define our system—and context
- What are the threats
- What are the vulnerabilities
- Mitigations
- Residual risks

What is Risk Register

- A risk register is a document that lists and manages risks to a project or organization
- Key component of Risk Management
- Used to document each risk, assess its level, track mitigation strategies, and monitor any residual risk after mitigation
- Risk register shows all risks on one sheet of paper and facilitates prioritization
- How much risk is the organization willing to tolerate, after remediation??

Components of Risk Register

- **Risk ID** – unique identifier for each risk
- **Risk Description** – brief explanation of the risk, including how it could affect the organization
- **Risk Category** – type of risk (e.g., malware, insider threat, cloud misconfiguration, phishing)
- **Likelihood** – probability of the risk occurring (e.g., Low, Medium, High)
- **Impact** –potential consequences if the risk materializes (e.g., financial loss, data breach, reputational damage)

ID	Risk description	Risk category	Risk assessment			Risk response type	Risk response description	Risk response cost	Risk owner	Status
			Likelihood	Impact	Exposure rating					
R.1	[Web application] is using a deprecated and unsecure protocol. If exploited, this vulnerability could allow a hacker to decrypt web app traffic.	System and Information Integrity	Moderate	Moderate	Moderate	Mitigate	Upgrade [web application]'s authentication protocol. Have all the tools necessary to perform this upgrade.	$0	[Engineer]	Open

More Components

- **Risk Score** – calculated score based on likelihood and impact (e.g., Risk = Likelihood × Impact)
- **Mitigation Measures** – Actions to reduce or eliminate the risk (e.g., implementing firewalls, security awareness training, patch management)
- **Risk Owner** – person or team responsible for managing the risk
- **Current Status** – status of risk mitigation efforts (e.g., Open, In Progress, Mitigated)
- **Review Date** – scheduled date for reassessing the risk

ID	Risk description	Risk category	Risk assessment			Risk response type	Risk response description	Risk response cost	Risk owner	Status
			Likelihood	Impact	Exposure rating					
R.1	[Web application] is using a deprecated and unsecure protocol. If exploited, this vulnerability could allow a hacker to decrypt web app traffic.	System and Information Integrity	Moderate	Moderate	Moderate	Mitigate	Upgrade [web application]'s authentication protocol. Have all the tools necessary to perform this upgrade.	$0	[Engineer]	Open

Steps for Creating Risk Register

1. Define Scope and System
2. Prepare for assessment
3. Identify Assets
4. Identify Threats & Vulnerabilities
5. Define Risk assessment methodology
6. Build Risk Register
7. Improve and Make Changes

Step 1: Scope and Define System

Define scope – What systems, data, or operations will be assessed?

Example Scenario:

- Let's consider my personal computer, which contains confidential information necessary for my work, like preparing class materials
- It also holds other confidential and personal information, including emails, stored passwords, financial documents, and personal files
- I am currently travelling to a conference with my colleagues via Train/Bus

My personal PC

The goal here is to identify:

- What needs to be protected — in this case, the sensitive information on my computer
- Potential vulnerabilities and threats due to factors like mobility and the confidential nature of the data

Step 2: Prepare for Risk Assessment

Identify objectives

- Why is the assessment being conducted?
- What assets, systems, or data are you protecting?
- What business processes depend on these assets?
- What compliance or regulatory requirements must be met (e.g., FERPA, HIPAA, PCI-DSS, NIST 800-53)?
- What threats and vulnerabilities are of concern (e.g., malware, insider threats, unauthorized access)?

- Example: A financial institution conducts a risk assessment to protect customer transactions and comply with PCI-DSS regulations

Step 3 Identify Assets

- Hardware (Tangible Asset)
  - Personal Computer (PC) , Hard drive (HDD/SSD), Peripheral Device
- Data (Intangible Asset)
  - Confidential Information – Includes class materials, research data, personal work files
  - Other sensitive information stored on the PC- Stored Passwords & Credentials, Emails & Communication Logs, Company or Institutional Data
- Software & Access Credentials
  - Any software used for work-related tasks (e.g., email, document editors, security software)
  - Stored credentials or saved passwords that could be compromised

Step 4 Identify Threats

What could be threat to my personal computer while travelling?

- Loss or Theft of the Laptop
- Unauthorized Access
- Public Wi-Fi Security Threats
- Malware Attacks
- Phishing Attacks
- Hard Drive Failure
- Shoulder Surfing

Step 5 Define risk assessment methodology

- Define risk assessment methodology – How will risks be measured?
  - Quantitative/Qualitative/Ordinal

- Develop a risk ranking scale for your system (Table I-3 in NIST 800-30: Guide for Conducting Risk Assessments)

We will use 3 level(qualitative) for simplifying things:

- HIGH RISK = severe or catastrophic effect on operation
- MODERATE RISK = serious adverse effect on operation
- LOW RISK = limited adverse effect on operation

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Step 6 Building Out A Risk Register

- NIST 800-30 (one of many government cybersecurity standards at nist.gov)
- Use QUALITATIVE scores for vulnerabilities and risk

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

https://doi.org/10.6028/NIST.SP.800-30r1

Building Out A Risk Register

- Let's use simplified risk register (from Appendix TABLE I-5)
- Use QUALITATIVE scores for vulnerabilities and risk

Threat*	Threat Source	Likelihood	Vulnerability	Impact	Risk	Treatment	Type	Residual
Password Guessing	Coworker	Low	Weak password	High	Low	Require strong passwords	Mitigation	Low

Add in First Threat

Building Out A Risk Register

Threat	Threat Source	Likelihood	Vulnerability	Impact	Risk	Treatment	Type	Residual
Password Guessing	Coworker	Low	Weak password	High	Low	Require strong passwords	Mitigation	Low

Add in A Second Threat

Building Out A Risk Register

Threat	Threat Source	Likelihood	Vulnerability	Impact	Risk	Treatment	Type	Residual
Password Guessing	Coworker	Low	Weak password	High	Low	Require strong passwords	Mitigation	Low
Loss at airport	Travel	High	Confusion at TSA	Medium	Medium	Insurance	Transfer	Medium

A Third Threat

Building Out A Risk Register

Threat	Threat Source	Likelihood	Vulnerability	Impact	Risk	Treatment	Type	Residual
Password Guessing	Coworker	Low	Weak password	High	Low	Require strong passwords	Mitigation	Low
Loss at airport	Travel	High	Confusion at TSA	Medium	Medium	Insurance	Transfer	Medium
Hard drive failure	Internal	Low	Single drive	High	Low	Have second PC	Mitigate	Low

Building Out A Risk Register

Threat	Threat Source	Likelihood	Vulnerability	Impact	Risk	Treatment	Type	Residual
Password Guessing	Coworker	Low	Weak password	High	Low	strong passwords/ MFA	Mitigation	Low
Loss at airport	Travel	High	Confusion at TSA	Medium	Medium	Insurance	Transfer	Medium
Hard drive failure	Internal	Low	Single drive	High	Low	Have backup PC and cloud storage	Mitigate	Low
Malware	Downloads	Medium	Antivirus weaknesses	High	Medium	Use EDR, Strong Antivirus	Mitigate	Low
Phishing Attack	Email	High	Lack of awareness	High	High	Training, email filtering	Mitigation	Low
Shoulder Surfing	Public Spaces	Medium	No Screen Privacy/Filter	Medium	Medium	Privacy Screen	Mitigation	Low

Step 7: Communicate and Maintain

- Communicate Results
  - ➢Provide risk findings to stakeholders (management, security teams, or clients)
  - ➢Helps in making informed decisions and implementing necessary risk mitigation strategies

- Maintain the Assessment
  - ➢Includes monitoring new threats, reassessing existing risks, and adjusting security measures accordingly

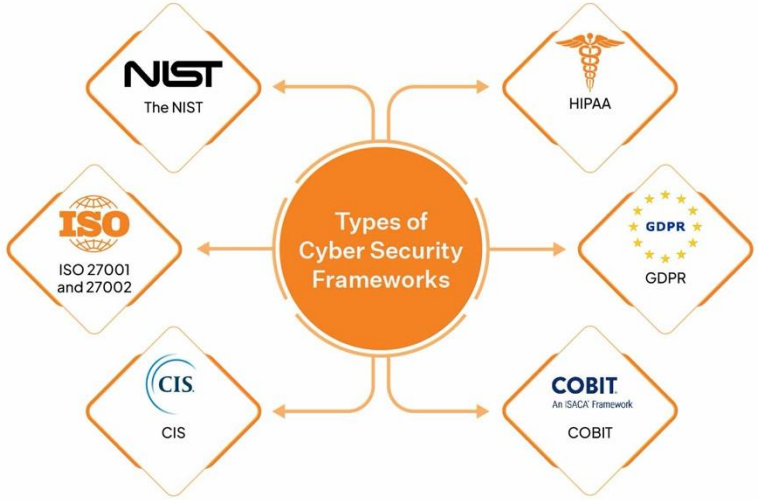
This final step ensures continuous improvement, adaptation, and preparedness in managing risks

If you were hired today as a security analyst, where would you start?

Cybersecurity Framework: they help us not start from scratch

Cybersecurity Framework

- CSF is a system of standards, guidelines, and best practices to manage risks that arise in the digital world
- Mandatory, or at least strongly encouraged, for companies that want to comply with state, industry, and international cybersecurity regulation
- Helps organizations *identify and manage risks, detect and respond to cyber threats, and recover from cybersecurity incidents*
- Helps businesses to build trust with their customers, partners, and stakeholders by demonstrating a commitment to cybersecurity and protecting sensitive information.



Cybersecurity Frameworks

https://www.pcisecuritystandards.org/

- **Payment Card Industry Data Security Standard (PCI DSS):**
  - ➢A set of requirements designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment
  - ➢Protect cardholders against misuse of their personal information
  - ➢Grouped into 6 broad objectives:

Objective	Examples
Build and maintain a secure network	Use firewalls, change default passwords
Protect cardholder data	Encrypt transmission and storage
Maintain a vulnerability management program	Install antivirus, patch systems
Implement strong access control	Restrict data access by need
Monitor and test networks	Log access, test security systems
Maintain an information security policy	Create and enforce policies

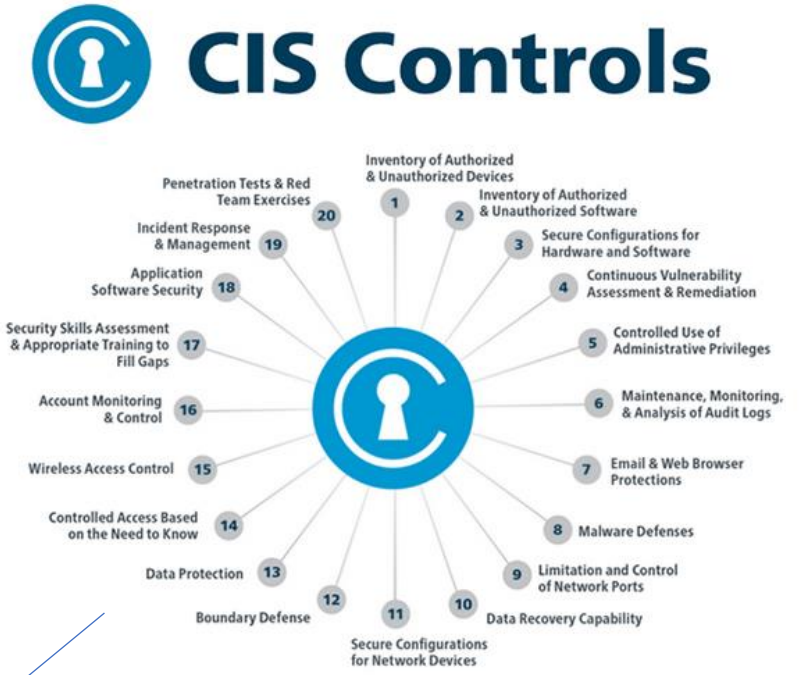
Any organization that handles payment card data must comply

Cybersecurity Frameworks

Center for Internet Security (CIS) Controls

- CIS Controls are a set of clear actions for organizations to strengthen cybersecurity
- A set of 18 security controls designed to provide specific and actionable ways to stop the most pervasive and dangerous attacks
- Designed to help orgs defend against the most common threats
- Free and open — used by gov, edu, SMBs
- https://www.cisecurity.org/controls/cis-controls-list

#	Control Name
1	Inventory and Control of Assets
2	Inventory and Control of Software
3	Data Protection
4	Secure Configuration of Hardware/Software
5	Account Management



Top 5 Controls

NIST Risk Management Framework (NIST 800-37)

- Provides a structured approach for managing cybersecurity risk in information systems through the Risk Management Framework (RMF)
- Mandatory for US federal agencies and organizations that handle federal data
- Seven step process

Prepare	Essential activities to **prepare** the organization to manage security and privacy risk
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

https://doi.org/10.6028/NIST.SP.800-37r2

NIST SP 800-30: Guide for Conducting Risk Assessments

- Provides detailed guidance on performing risk assessments for information systems
- Focuses on risk assessment methodology, rather than full system risk management
- Key Focus Areas:
  - Identifying assets, threats, vulnerabilities, and risks
  - Assessing likelihood and impact of threats exploiting vulnerabilities
  - Supporting decision-making on risk treatment (mitigation, acceptance, transfer, avoidance)
- Risk Assessment Process:
  - Prepare for the Risk Assessment – Define purpose, scope, and assumptions
  - Conduct the Risk Assessment – Identify threats, vulnerabilities, impact, and risk level
  - Communicate Results – Provide risk findings to stakeholders
  - Maintain the Assessment – Regularly update risk assessments based on evolving threats

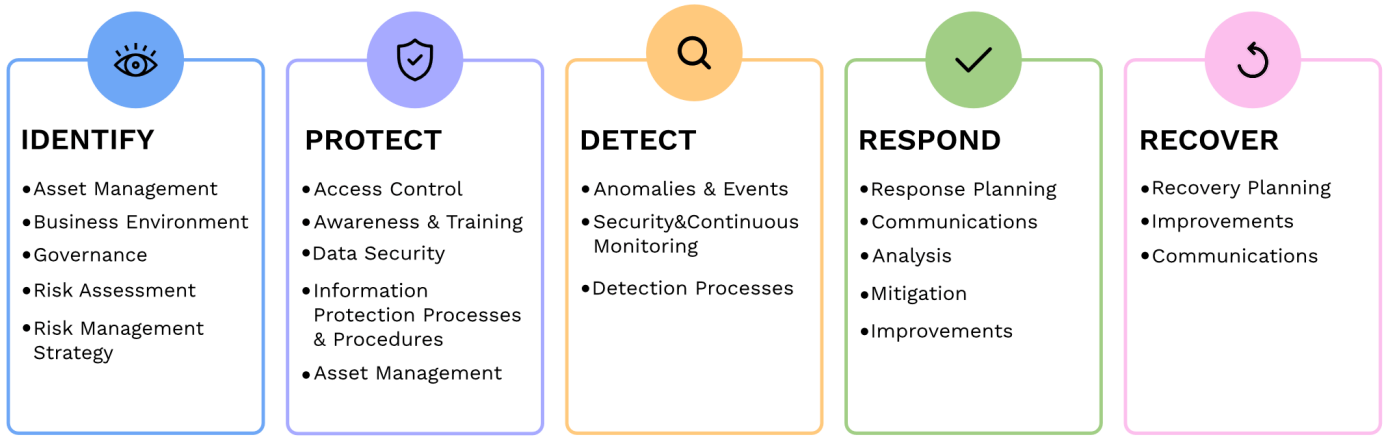
How They Work Together

- NIST 800-30 (Risk Assessment) is used within NIST 800-37 (RMF) during the Assess step to evaluate security risks
- NIST RMF (800-37) helps in managing risk across an organization, while 800-30 provides a detailed methodology for assessing specific risks

Feature	NIST 800-37 (RMF)	NIST 800-30 (Risk Assessment)
Focus	Full risk management lifecycle	Risk assessment process
Scope	Organizational/system-level risk management	Threats, vulnerabilities, and risk likelihood analysis
Process	7-step Risk Management Framework (RMF)	4-step risk assessment methodology
Outcome	Security authorization & continuous monitoring	Risk analysis for decision-making

NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

- Provides a comprehensive catalog of security and privacy controls designed to protect federal information systems and organizations from cyber threats
- It is a core component of the Risk Management Framework (RMF) (NIST 800-37) and supports compliance with FISMA (Federal Information Security Modernization Act)
- Aligns with risk-based security management as outlined in NIST 800-37
- Provides guidance for selecting, implementing, assessing, and monitoring security controls
- 5 Core Components of NIST 800-53:



Cybersecurity Frameworks

- **ISO/IEC 27002 and 27001:** A widely recognized international standard for information security management systems (ISMS)
- **ISO/IEC 27001**

- Standard for Information Security Management System

- **ISO/IEC 27002**

- Code of practice for information security controls

- **ISO/IEC 27701**

- Privacy Information Management Systems

- **ISO/IEC 31000**

- International Standards for Risk management practices

NIST Cybersecurity Framework

- NIST CSF is a voluntary set of standards, guidelines, and best practices for managing cybersecurity risk
- Outlines key principles, best practices, and guidelines that help organizations, regardless of size or sector, protect critical assets and enhance their overall cybersecurity posture

- **2013**: President Obama issued Executive Order 13636 – “Improving Critical Infrastructure Cybersecurity”
- **Goal**: Protect U.S. critical infrastructure (like energy, finance, healthcare) from increasing cyber threats
- Order tasked NIST (National Institute of Standards and Technology) with developing a **voluntary cybersecurity framework**

Year	Milestone
2014	**NIST CSF Version 1.0** released after industry collaboration
2018	**Version 1.1** introduced updates on supply chain risk, identity management
2024	**Version 2.0 (released)** expands focus beyond critical infrastructure — for *all sectors* and org sizes

NIST Cybersecurity Framework

- Why it matters:
  - Widely used in government, healthcare, finance, and more
  - Helps orgs of all sizes assess and improve their cyber posture
  - Focuses on outcomes, not just tools

Provides a continuous process for cybersecurity risk management

For organizations of any size, in any sector, whether they have a cyber risk management program already or not

Has proven useful to a variety of audiences

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Version 1.1)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (version 2.0)

Cybersecurity Framework Functions

NIST Cybersecurity Framework provides a basic and understandable language of five key functions for managing risk iteratively over time

Credit: N. Hanacek/NIST

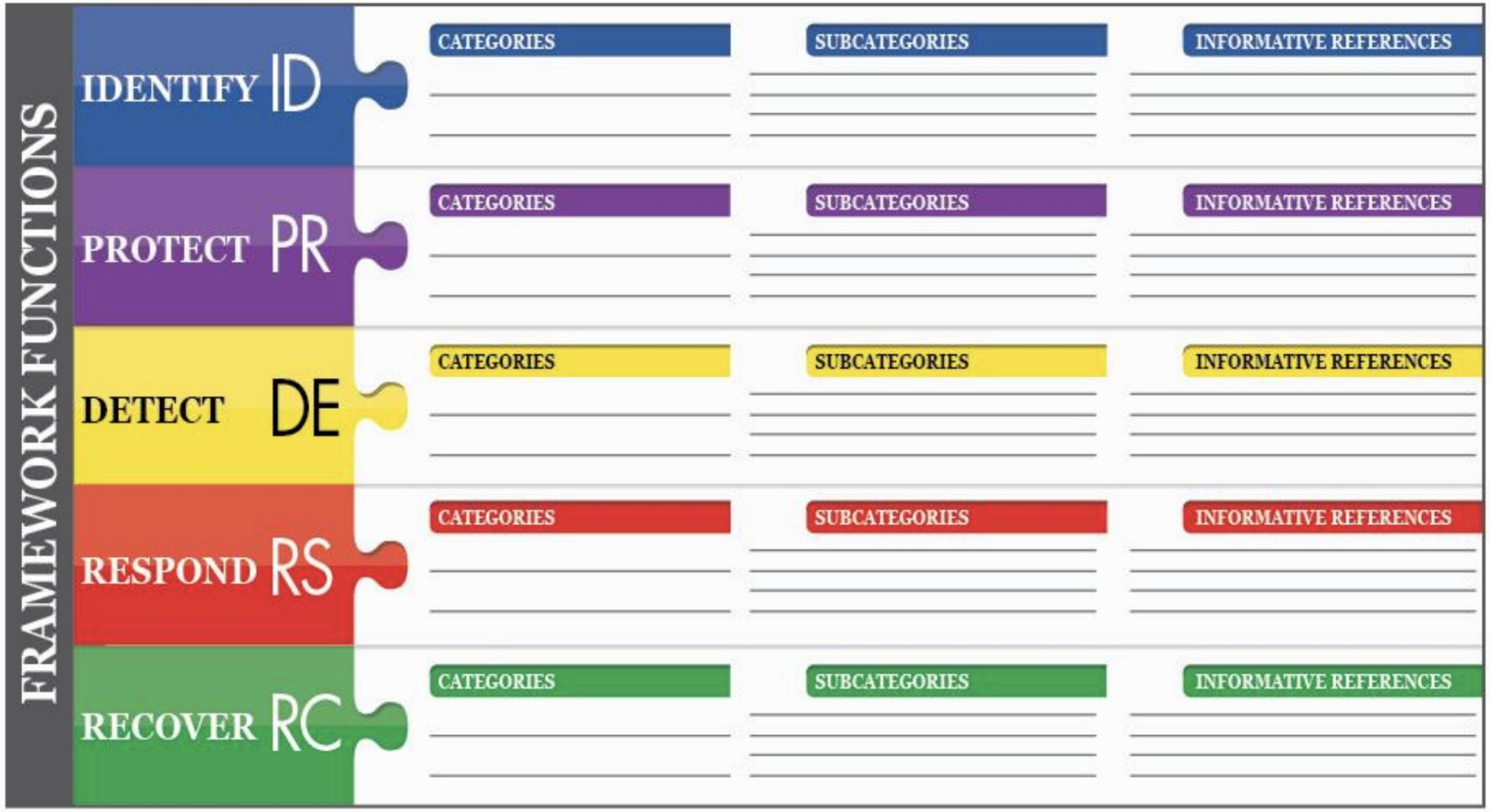


Figure 1: Framework Core Structure

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Identify

Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

- What needs to be protected?
- This could include identifying business processes, physical assets, software, or information that your business cannot survive without

Identify is about the foundational things
After all, you can't manage what you don't know

Important phase: Subsequent functions have a lot of dependencies on the Identify Function

Sample Identify Activities

- Identify critical business processes
- Document Information flows
- Establish policies for cybersecurity that includes roles and responsibilities
- Maintain hardware and software inventory
- Identify contracts with external partners
- Identify Risk Management processes

Protect

Develop and implement the appropriate safeguards to ensure delivery of services.

Look at processes such as :

- access to the workspace (who issues identity credentials and who retrieves them from those who no longer require access);
- who has a similar role for managing access to your network(s) and services;
- are you using encryption and/or dual factor authentication methods where available;
- do you have training for new hires and on a regular basis for your staff; what about your vendors and so

Activities in the Protect Function are for ensuring that the critical business processes you identified earlier continue; or that in the event of a disruption can be recovered in a timely manner.

Sample Protect Activities

- Manage access to assets and information
- Conduct regular backups
- Protect sensitive data
- Patch operating systems and applications
- Create response and recovery plans
- Protect your network
- Train your employees

Activities in the Protect Function are for ensuring that the critical business processes you identified earlier continue; or that in the event of a disruption can be recovered in a timely manner

Detect

Develop and implement the appropriate activities to **identify the occurrence of a cybersecurity event**

- Cybersecurity incidents are going to occur
- You can't prevent every attack against your businesses and networks
- You need to make sure you are able to detect when something is not quite right

Too often we think if we've installed security software and trained our teams, our work is done

Sample Detect Activities

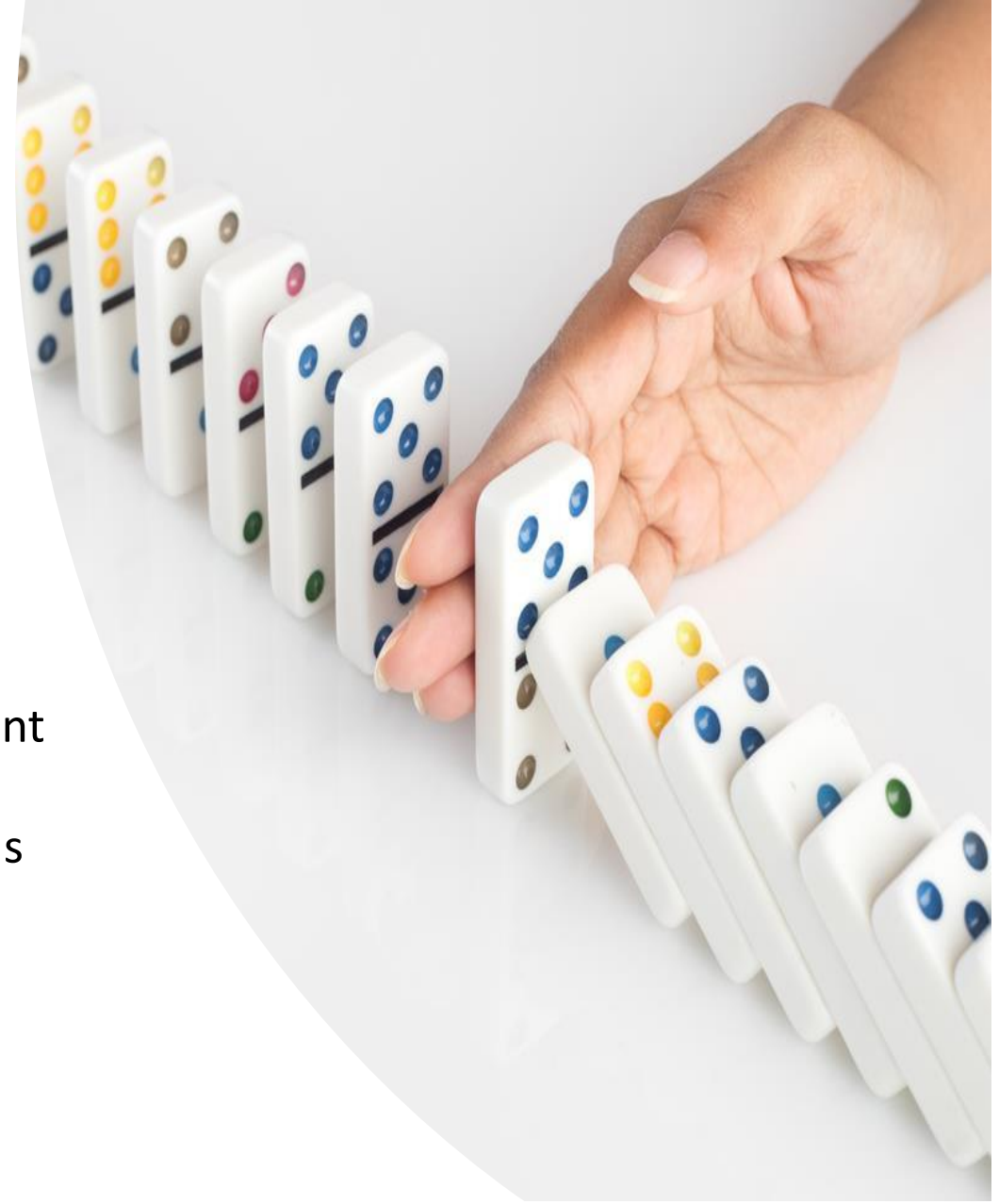
- Install and update anti-virus and other malware detection software
- Know what are expected data flows for your business
- Maintain and monitor logs

Detect function sets us up to consider what best practices will enable us to recognize harms and to react appropriately

Respond

Develop and implement the appropriate activities to **take action regarding a detected cybersecurity event**

- Need to have plans in place to respond to the incident
- Incident needs to be contained and mitigated
- You and your staff need to know what to do, who has the responsibility and how you will measure your response



Sample Respond Activities

- Coordinate with internal and external stakeholders
- Ensure response plans are tested
- Ensure response plans are updated

involves developing and implementing activities to handle detected security events effectively

Recover

Develop and implement the appropriate activities to maintain plans for **resilience and to restore any capabilities or services** that were impaired due to a cybersecurity event.

- Supports timely recovery to normal operations to reduce the impact from a cybersecurity incident
- Recovery activities help restore those business operations to normal

Sample Recover Activities

- Manage public relations and company reputation
- Communicate with internal and external stakeholders
- Ensure recovery plans are updated
- Consider cyber insurance

'Recover' function within the NIST Cybersecurity Framework is all about resilience and restoration

Framework	Issued by	Industry	Relevant Act
NIST CSF The US National Institute of Standards and Technology	NIST	Operators of critical infrastructure + general	Cybersecurity Enhancement Act of 2014
ISO/IEC 27000 family The International Organization of Standardization and the International Electrotechnical Commission	ISO 27001	General enterprise	
NIST SP 800-53 The US National Institute of Standards and Technology	NIST	Federal agencies and contractors	Federal Information Security Management Act (FISMA)
CSA CCM Cloud Security Alliance	CSA	Cloud Service Providers	
ANSI/ISA-62443 International Society for Automation (ISA) and American National Standards Institute (ANSI)	ISA ANSI	industrial automation and control systems	
CIS CSC Center for Internet Security	CIS		
HITRUST CSF Health Information Trust Alliance	HITRUST	Healthcare service providers	Health Insurance Portability & Accountability Act of 1996 (HIPAA)
NERC CIP North American Electric Reliability Corporation	NERC	Bulk Electric Systems	

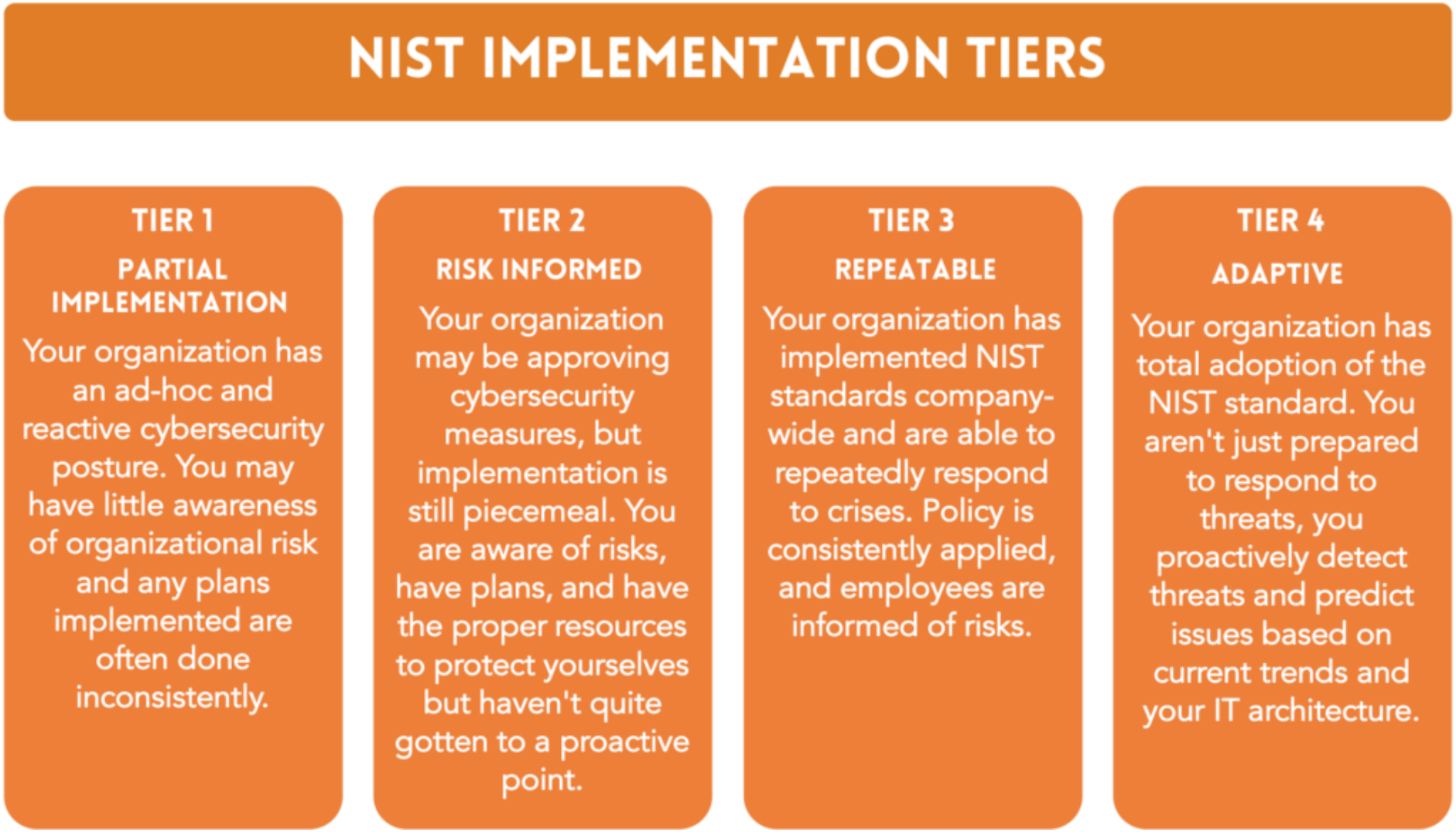
What Are NIST CSF Implementation Tiers?

- Implementation Tiers describe how well an organization manages cybersecurity risk — not how "mature" or "compliant" they are
- Purpose:
  - ➢Reflect how an organization views risk
  - ➢Show the degree of rigor and consistency in cybersecurity processes
  - ➢Help orgs decide where they are and where they want to be

Tier	Name	Description
1	Partial	Risk management is ad hoc and reactive. No formal policies..
2	Risk Informed	Some risk practices in place, but not consistently applied across the organization.
3	Repeatable	Cybersecurity practices are formalized, documented, and consistently implemented.
4	Adaptive	Organization adapts cybersecurity practices based on lessons learned and real-time risk intelligence. Continuous improvement.

Tiers = A snapshot of your cybersecurity mindset and strategy

Source: https://port53.com/blog-what-are-the-nist-cybersecurity-framework-implementation-tiers/



Quick Analogy: Securing a Bike

Tier	Behavior
Tier 1	Leave the bike unlocked outside.
Tier 2	Sometimes lock it when you remember.
Tier 3	Always lock it with a standard chain and follow routine.
Tier 4	Use GPS tracking, a smart lock, check for suspicious activity, and improve your method based on local theft reports.

Why Implementation Tiers Matter

1. It's About Risk, Not Just Tech
   - ➢Even high-tech orgs can be Tier 1 if they lack structure and process to implement controls
   - ➢Low-budget orgs can still reach Tier 3 with strong governance

2. They Guide Strategic Planning
   - ➢Helps orgs ask: “Where are we now?” “Where do we want to be?” “What gaps do we need to close?”

3. Business-Aligned Cybersecurity
   - ➢Different industries = different risk tolerance
   - ➢A bank may aim for Tier 4 and a startup may accept Tier 2 (for now)

“If you were the cybersecurity lead at a hospital, which Tier would you aim for — and why?”

It’s Monday morning. Maple Town Library’s IT manager discovers that all patron records, financial spreadsheets, and staff documents are **encrypted**, and a ransomware note demands $50,000 in Bitcoin.

The library has public computers, Wi-Fi, staff logins, and an outdated firewall. There's **no formal incident response plan**. You are the newly assembled **cyber response team**. You must quickly assess and propose an action plan — using all 5 NIST CSF functions.

Work in teams of 2 and fill out the following NIST CSF-based action plan:

Function	Your Response for Maple Town Library
Identify	
Protect	
Detect	
Respond	
Recover	

Which NIST CSF function do you think gets overlooked the most — and why?

Function	Sample Action
Identify	Create an inventory of all computers; identify critical data and who manages backups.
Protect	Apply patches; enforce MFA; separate public network from staff network.
Detect	Install endpoint detection tools; review logs weekly.
Respond	Isolate infected systems, notify stakeholders, contact cybersecurity experts.
Recover	Restore from backups, rebuild clean systems, create a recovery playbook.

Recover

“Most organizations don’t think about recovery until after something goes wrong. They may not test backups, practice recovery procedures, or even know if their data can be restored quickly.”

Why it's overlooked:

- Seen as a ‘future problem’
- Recovery planning isn’t as exciting or visible as detection tools
- Backups often exist, but aren’t tested regularly

Identify

“People focus on tools and alerts, but skip the step of understanding what needs protecting and who’s responsible. Without knowing assets and risks, everything else is just guessing.”

Why it's overlooked:

- Asset inventories are boring and time-consuming
- Risk assessments require input from across departments
- It feels abstract, but it’s foundational

Defense in Depth: Definition

- Defense in Depth is a cybersecurity strategy that uses multiple layers of defense across the technology stack to protect systems and data — so if one layer fails, others still provide protection
- Aim is to increase the time and effort required for an attacker to breach defenses, reducing the likelihood of a successful attack

Think of it like protecting a castle:

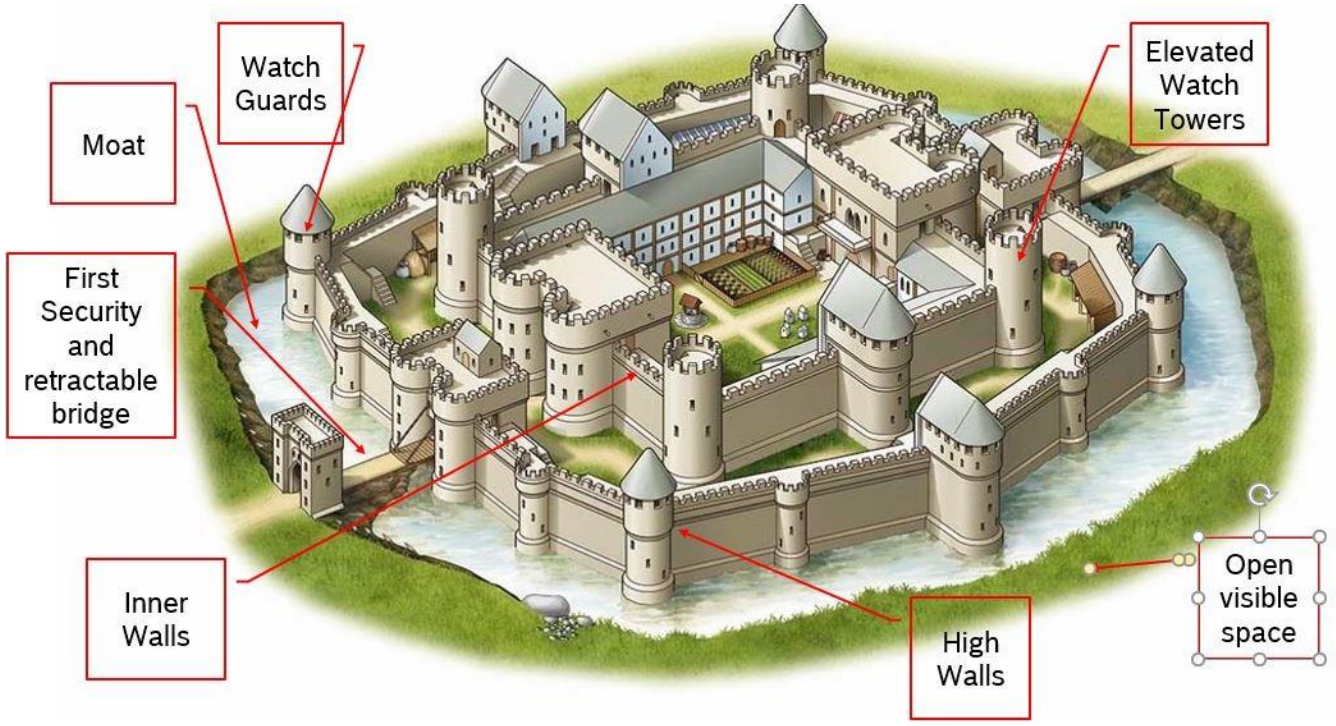
What would you do to protect a castle?

Defense in Depth: Definition

- Defense in Depth is a cybersecurity strategy that uses multiple layers of defense across the technology stack to protect systems and data — so if one layer fails, others still provide protection

Think of it like protecting a castle:

- Moat = Firewalls
- Walls = Network segmentation
- Guards = Authentication
- Locked doors = Encryption
- Alarms = IDS/monitoring
- Escape plans = Backups & recovery



6 Common Layers of Defense in Depth

1. **Physical Security-** Locked server rooms, CCTV, access badges
2. **Network Security**- Firewalls, VPNs, intrusion detection systems
3. **Endpoint Security**- Antivirus, device encryption, USB control
4. **Application Security**- Secure coding practices, input validation, patching
5. **User Security**- Training, strong passwords, MFA
6. **Data Security-** Encryption, access controls, backups

Security Architecture

Defense in Depth isn't just a standalone concept- it is woven into the Security Architecture

The Four Pillars of Security Architecture in Defense in Depth

1. **People-** Employees who are aware of cybersecurity threats and trained in safe practices
2. **Process-** Established protocols and procedures to manage security
3. **Technology-** Security tools and software that prevent, detect, and respond to attacks
4. **Partners-** Collaborating with external security firms or vendors to enhance security measures.

How Does Defense in Depth Fit In?

1. **Reduce Initial Exploits:** Defense in Depth aims to minimize the chances of successful attacks by reducing opportunities for initial exploitation.
    - Includes proactive measures like secure coding practices, vulnerability scanning, and regular security assessments

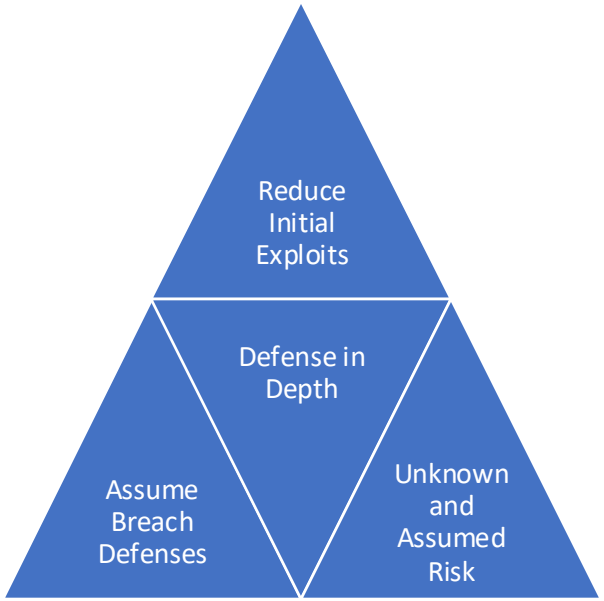
2. Assume Breach Defenses: Defense in Depth operates on the assumption that, at some point, a breach will occur

- By preparing for this scenario, organizations can implement controls that limit the damage if an attacker gains access

3. Unknown and Assumed Risk: Not all risks are known, and some may be unavoidable

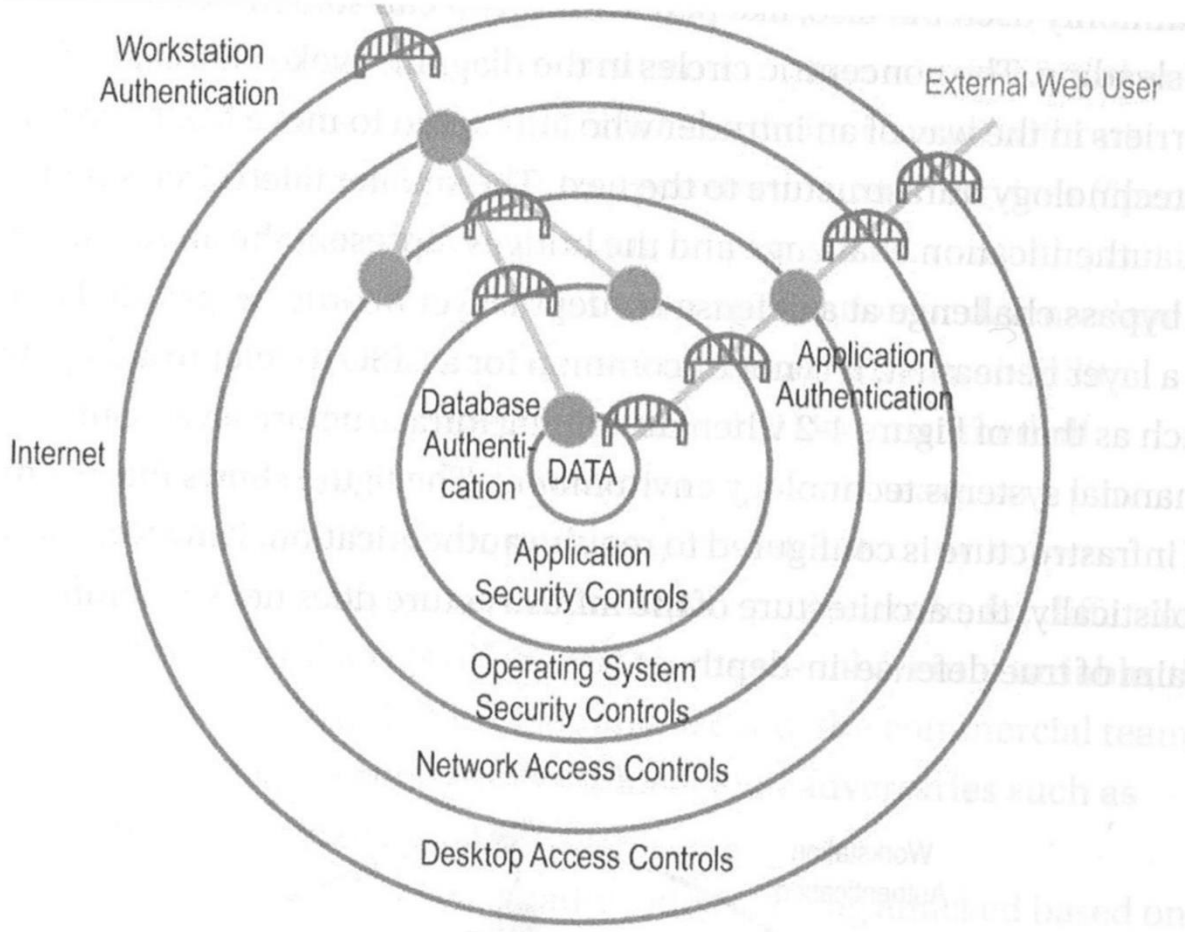
- Defense in Depth takes this into account by having multiple controls in place, each addressing different types of risks

By addressing each of these aspects, Defense in Depth makes it much harder for attackers to achieve their objectives, even if they overcome one layer of security



Access Paths

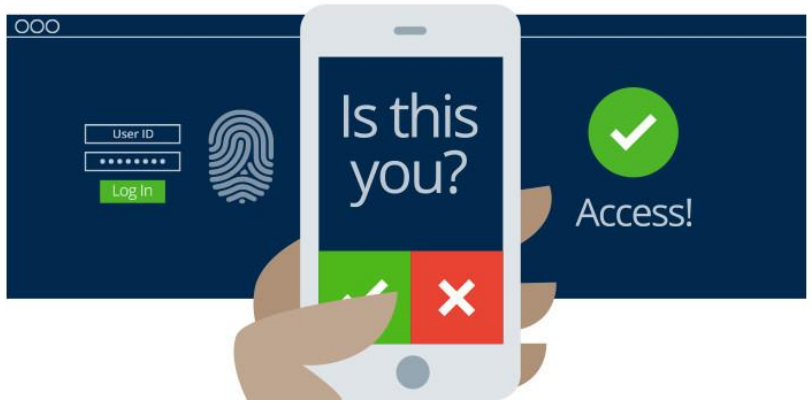
Access Paths represent the different layers of authentication and security controls that a user or system must pass through to access sensitive data. Each layer adds another level of defense, ensuring that only authorized users can reach critical resources.



Defense in Depth: Authentication

- Authentication is a critical aspect of Defense in Depth, ensuring that only verified users can access systems and data. It typically involves multiple factors to verify identity, which strengthens security by requiring users to prove who they are in different ways

- Types of Authentication Factors
  - Something you know
    - password
  - Something you have:
    - token (Yubikey)
  - Something you are:
    - biometric (finger)



References

- Financial Cybersecurity Risk Management, Paul Rohmeyer and Jennifer Bayuk, 2018.
- A Data Driven Computer Defense, Roger Grimes, 2019.
- Lecture slides prepared by Dr Lawrie Brown (UNSW@ADFA) for “Computer Security: Principles and Practice”, 1/e, by William Stallings and Lawrie Brown, Chapter 16 “IT Security Management and Risk Assessment”.

Reading

- Read NIST 800-30 “Guide for Conducting Risk Assessments”, pages 10-31, Appendix I (Required for upcoming IC activity and Lab)

- Building a heatmap using Excel:

  https://www.youtube.com/watch?v=kCuR-NfGQ6w

- Go over first two chapters of NIST 800-30, 800-37, 800-53

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf