Cyber Resilience : Enterprise Security Process Aspect

Submitted by:
Abhishek Pasi
Sairaj Patil
Mudit Rathore

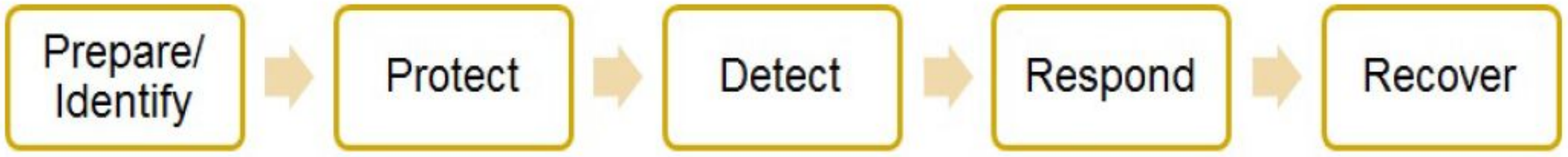
Objectives

- Cyber Resilience & its phases.
- Resilience & its features.
- Cyber Resilience Assessment of an organisation.
    - Our Proposed Parameters
    - Flowcharts
    - Our proposed Scoring Mechanism
    - Parameters Description
- Cyber Resilience Process improvement.

Cyber Resilience

Cyber resilience is about managing security with a multi-layered approach that encompasses people, processes, and technology(Product).

Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack. Resilience is more than just preventing or responding to an attack—it also takes into account the ability to operate during, and to adapt and recover, from such an event.



Prepare/ Identify

Protect

Detect

Respond

Recover

Cyber Resilience

Cyber Resilience is not defined by a series of checklists, but through evaluations based on the current threat environment and the acceptable risk level for the organization.

Managing people and processes is key. A recent Ponemon Institute study found that **35 percent** of the root causes for data breaches involved **human factors**, such as negligent employees or contractors. The same report attributed **29 percent** of breaches to system glitches, which includes IT and business **process failures**.

Prepare/Identify

- To successfully face and overcome an attack, you must thoroughly understand your cyber risk posture through assessments and simulations.
- Infrastructure and information assessment that includes all known security vulnerabilities.
- Spotting and addressing the most urgent issues first will make your organization a less appealing target for attackers.
- Improving visibility and understanding your information and systems.

Protect

- Once you have a good handle on what's out there, where it lives, its level of sensitivity, how vulnerable it is, and your risk tolerance, you can begin to take the necessary steps to protect it.
- This is all about developing and implementing safeguards for critical infrastructure and services in order to limit or contain the impact of an attack.
- Securing business-critical systems from cyber threats.
- Protecting the organization’s endpoints and gateways from targeted attacks and advanced threats.

Detect

- Detect focuses on developing and implementing the appropriate activities to rapidly identify an attack, assess the systems that maybe affected, and ensure a timely response.
- One of the most significant consequences of this lack of preparation is that it cripples the organization's ability to effectively respond to the breach. As response time, and time to resolution increase, cyber criminals have more time to exploit and damage the business
- According to the 2014 Verizon Data Breach Investigations Report, **85 percent of point-of-sale intrusions took weeks to discover, and 43 percent of web application attacks took months to discover.**

Respond

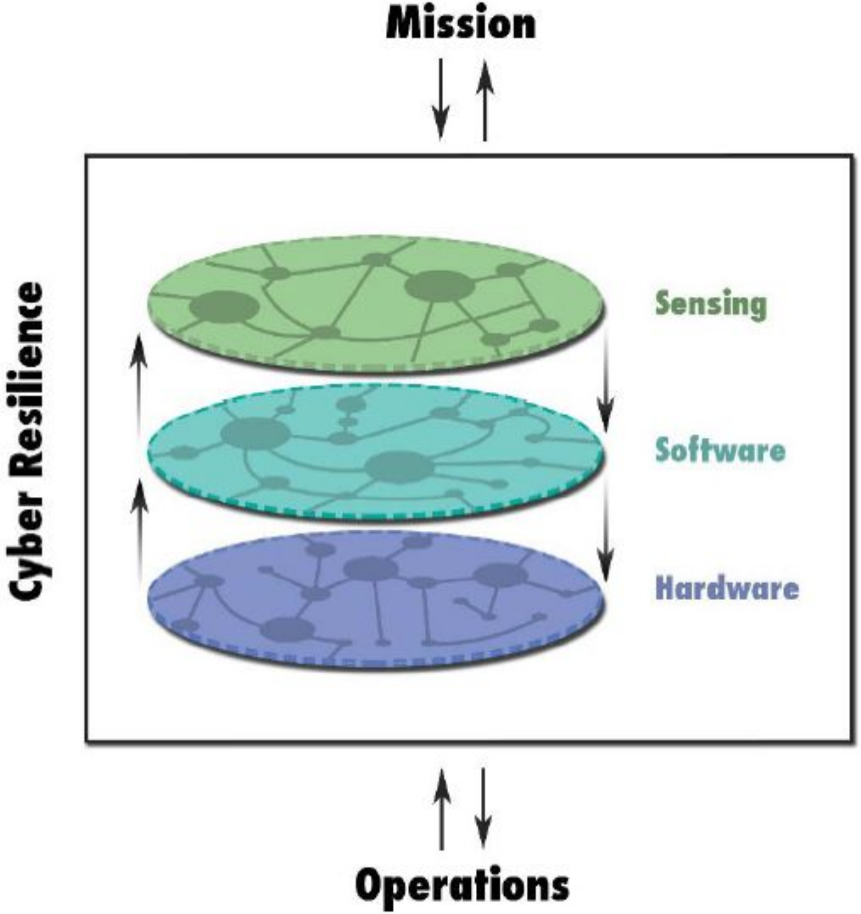
- The respond pillar provides guidance on the types of activities that can accelerate time to remediation and contain the impact of the attack once it’s detected.
- Managing risk by measuring and tracking your cyber resilience, including how well systems were protected during an attack.
- Devising a system whereby lessons learned are incorporated into future response activities.

Recover

- This stage involves developing and implementing the appropriate systems and plans to restore any data and services that may have been impacted during a cyber attack.
- As much as we prepare and protect our organizations, we may not be able to avoid certain types of attacks. Even if you respond quickly to a cyber breach, an attack may have consequences.
- As with response plans, recovery plans need to be re-evaluated and updated regularly to meet all of the risk-related aspects of a disaster that an organization might face.

Cyber Resilience

Cyber Resilience ensures that system recovery occurs by considering interconnected hardware, software and sensing components of cyber infrastructure . It thus constitutes a bridge between sustaining operations of the system while ensuring mission execution.



The cyber resilience domains comprise sensing, hardware, and software comp
which collectively contribute to sustaining system operations. .

What is Resilience?

Resilience defined by the National Academies of Science (NAS) as “The ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events”

The common resilience features include critical functions (services), thresholds, cross-scale (both space and time) interactions, and memory and adaptive management

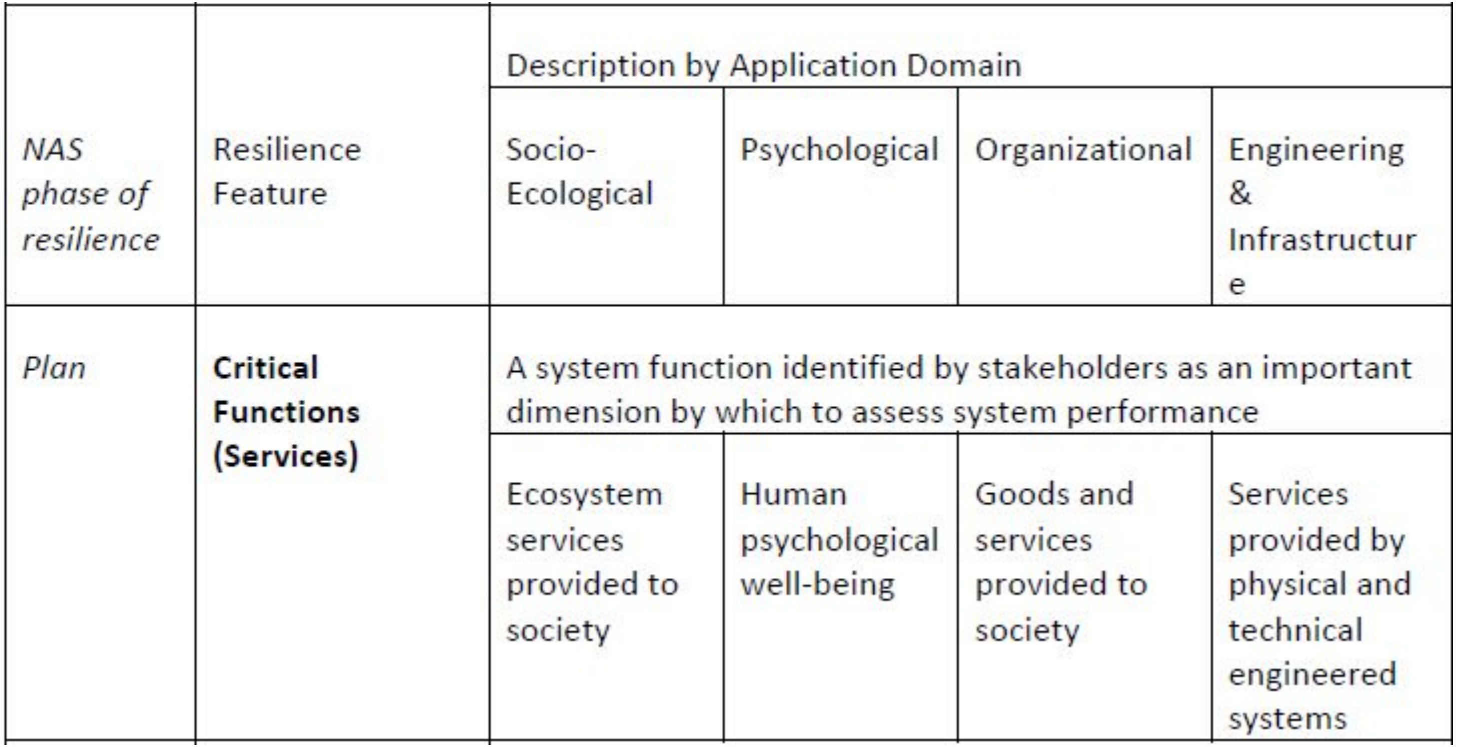
Resilience Cont.

Resilience has roots in many disciplines and integrates ecological, social, psychological, organizational, and engineering perspectives and definitions.

- **Resilience engineering**: “The ability of systems to anticipate and adapt to the potential for surprise and failure**”.**
- **Ecological resilience**: The ability of the system to absorb and withstand shocks.

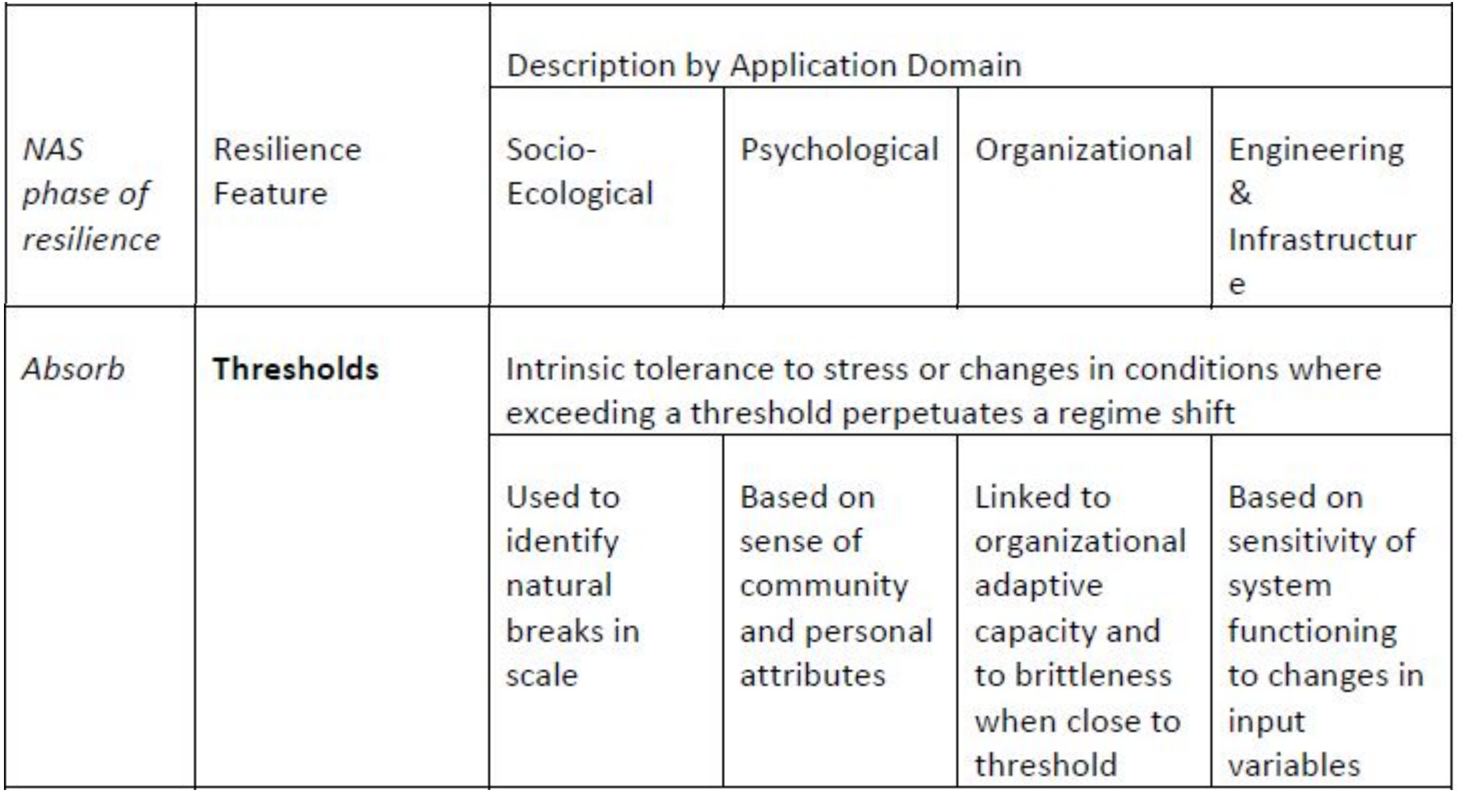
Resilience is used as a metaphor to describe how systems react to stressors, and to bridge the gap in understandings between fields.

Resilience Features: Critical Functions



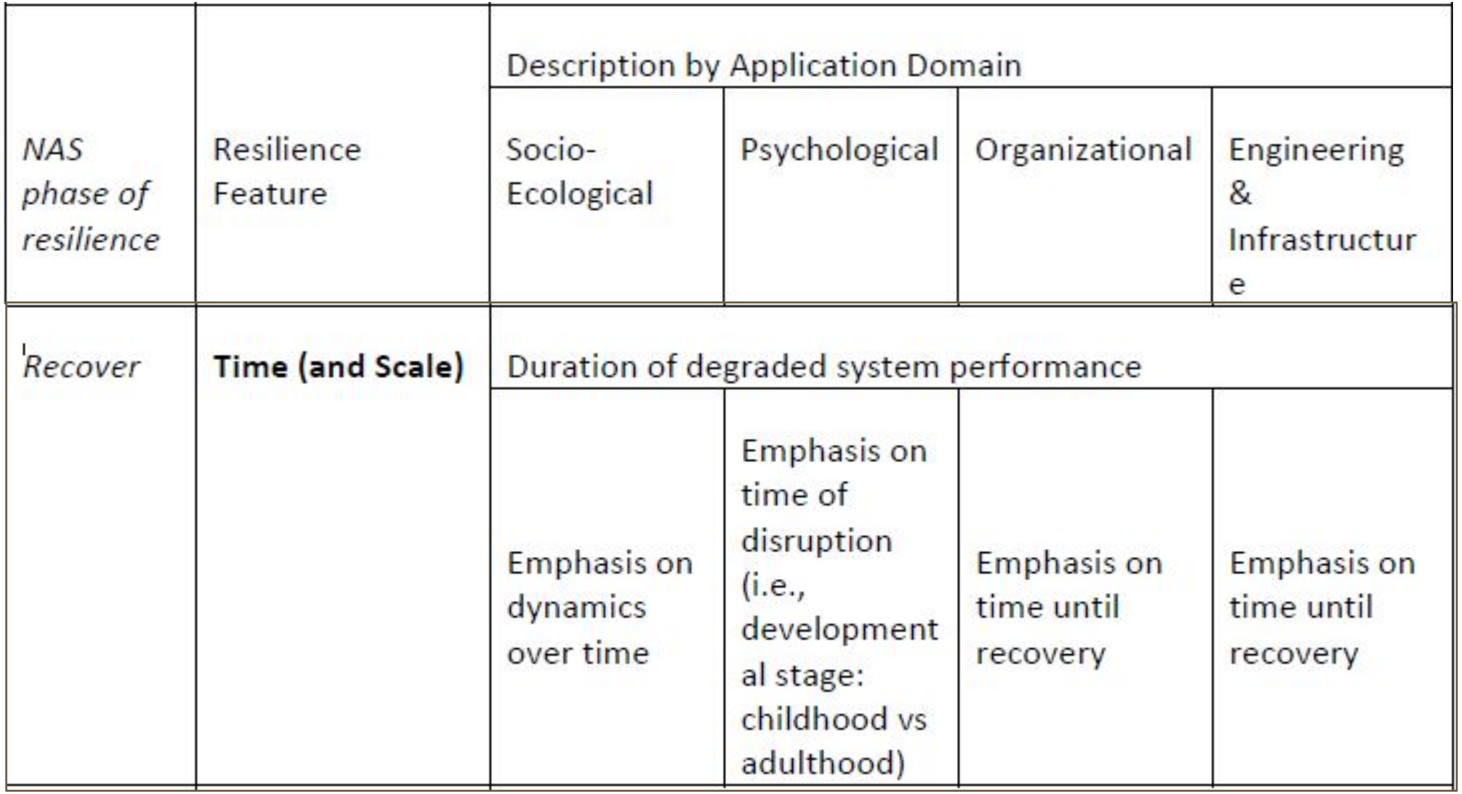
NAS phase of resilience	Resilience Feature	Description by Application Domain			
		Socio-Ecological	Psychological	Organizational	Engineering & Infrastructure
Plan	**Critical Functions (Services)**	A system function identified by stakeholders as an important dimension by which to assess system performance			
		Ecosystem services provided to society	Human psychological well-being	Goods and services provided to society	Services provided by physical and technical engineered systems

Resilience Features: Thresholds



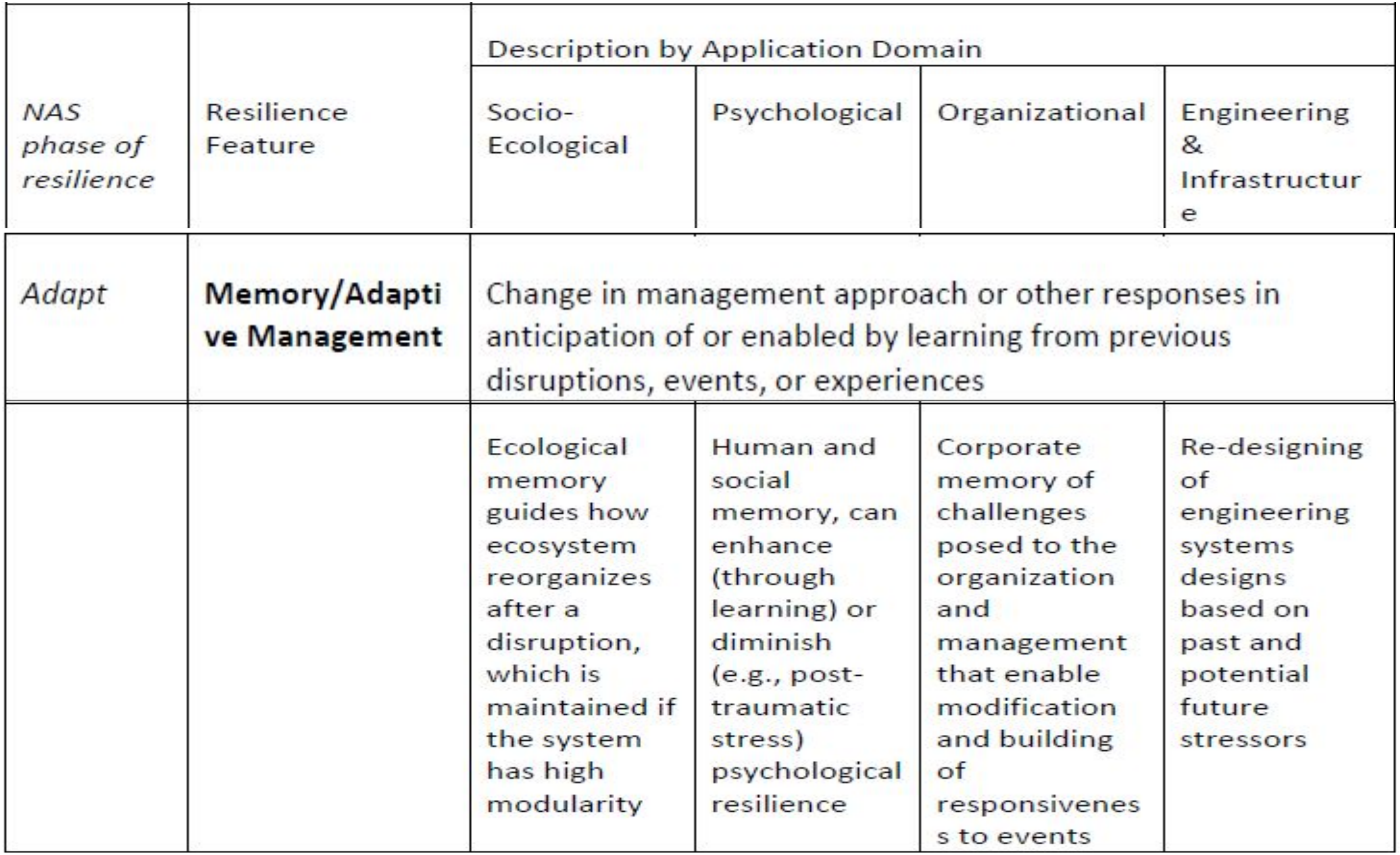
NAS phase of resilience	Resilience Feature	Description by Application Domain			
		Socio-Ecological	Psychological	Organizational	Engineering & Infrastructure
Absorb	**Thresholds**	Intrinsic tolerance to stress or changes in conditions where exceeding a threshold perpetuates a regime shift			
		Used to identify natural breaks in scale	Based on sense of community and personal attributes	Linked to organizational adaptive capacity and to brittleness when close to threshold	Based on sensitivity of system functioning to changes in input variables

Resilience Features: Time and scale



NAS phase of resilience	Resilience Feature	Description by Application Domain			
		Socio-Ecological	Psychological	Organizational	Engineering & Infrastructure
Recover	**Time (and Scale)**	Duration of degraded system performance			
		Emphasis on dynamics over time	Emphasis on time of disruption (i.e., developmental stage: childhood vs adulthood)	Emphasis on time until recovery	Emphasis on time until recovery

Resilience Features: Memory/Adaptive Management



NAS phase of resilience	Resilience Feature	Description by Application Domain			
		Socio-Ecological	Psychological	Organizational	Engineering & Infrastructure
Adapt	**Memory/Adaptive Management**	Change in management approach or other responses in anticipation of or enabled by learning from previous disruptions, events, or experiences			
		Ecological memory guides how ecosystem reorganizes after a disruption, which is maintained if the system has high modularity	Human and social memory, can enhance (through learning) or diminish (e.g., post-traumatic stress) psychological resilience	Corporate memory of challenges posed to the organization and management that enable modification and building of responsiveness to events	Re-designing of engineering systems designs based on past and potential future stressors

Resilience

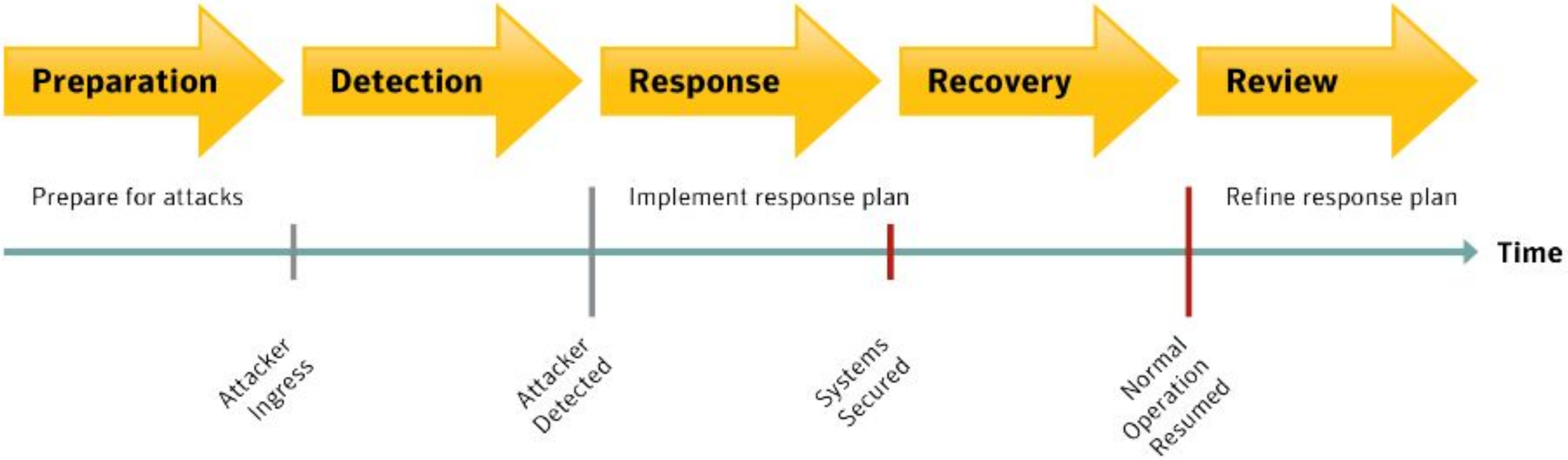
Resilience is often confused or conflated with several other related but different concepts. These include risk, robustness, and security.

- **Risk** : “A situation involving exposure to danger [threat].”
- **Security** : “The state of being free from danger or threat.”
- **Robustness :** “The ability to withstand or overcome adverse conditions or rigorous testing.”

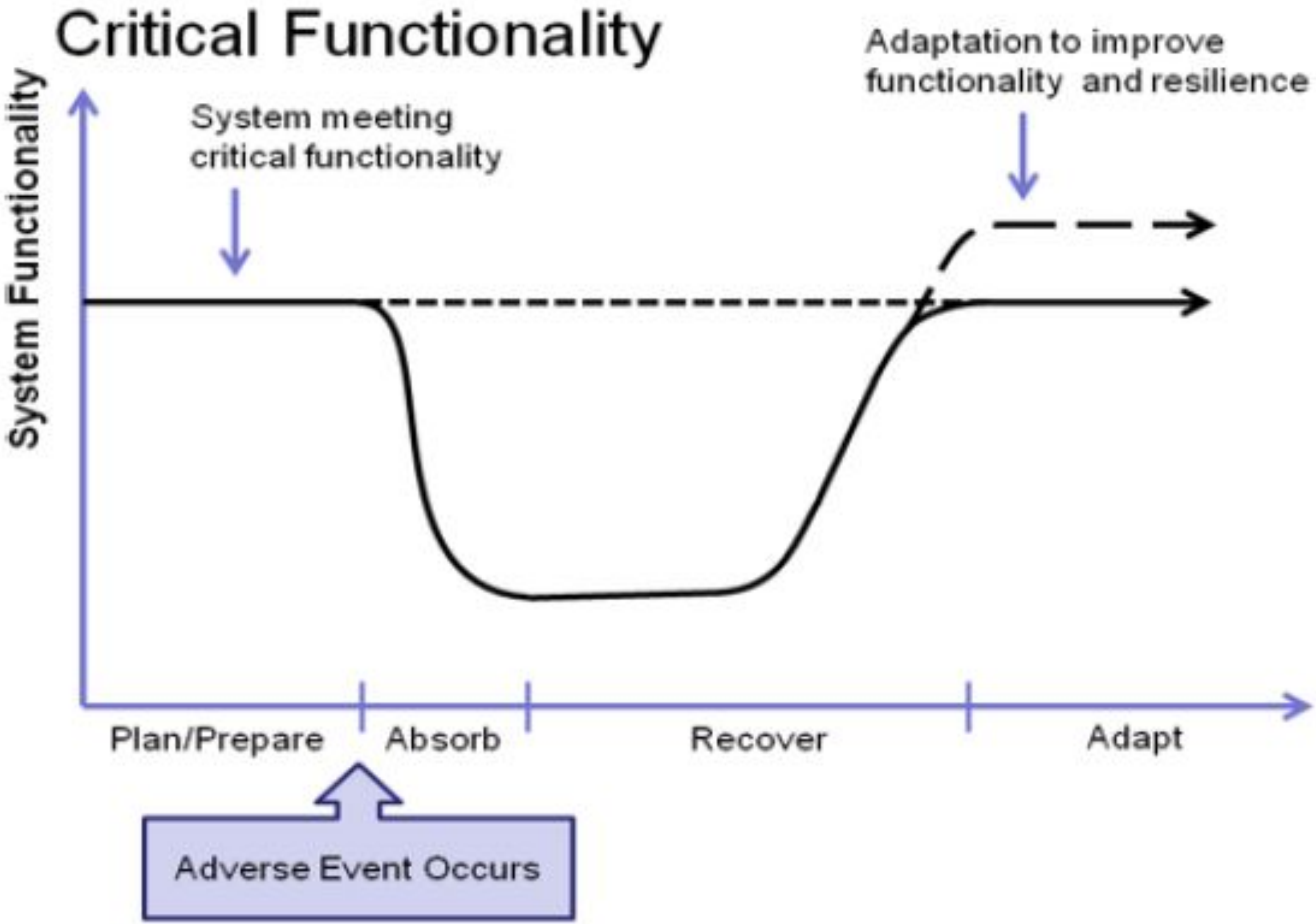
Security, Robustness and **Risks** are connected, they are focused on preventing system from degrading and keeping functionality within acceptable level before and after the adverse event.

Resilience is a very different concept. Oxford defines it as “the capacity to recover quickly from difficulties.”

Cyber Resiliency refers to the system's ability to recover or regenerate its performance after a cyber attack produces a degradation of its performance



Critical Functionality


System Functionality
System meeting critical functionality
Adaptation to improve functionality and resilience
Plan/Prepare
Absorb
Recover
Adapt
Adverse Event Occurs

What is IT Risk or Cyber Risk?

ISO’s definition of IT risk is similar: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.

NIST's defines : "Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system."

Resilience assessment

Resilience assessment, starts with the assumption that system is affected, functionality is impaired and is focused on evaluation of recovery speed.

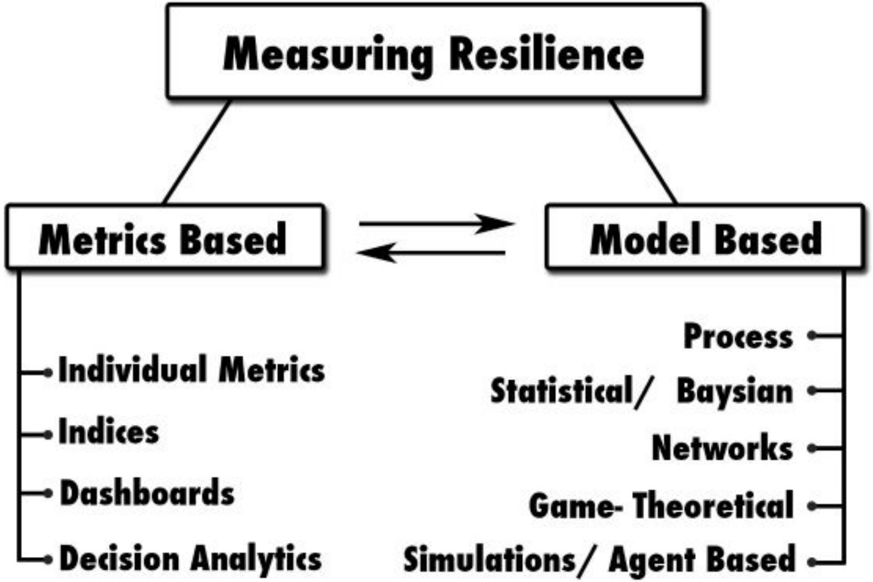
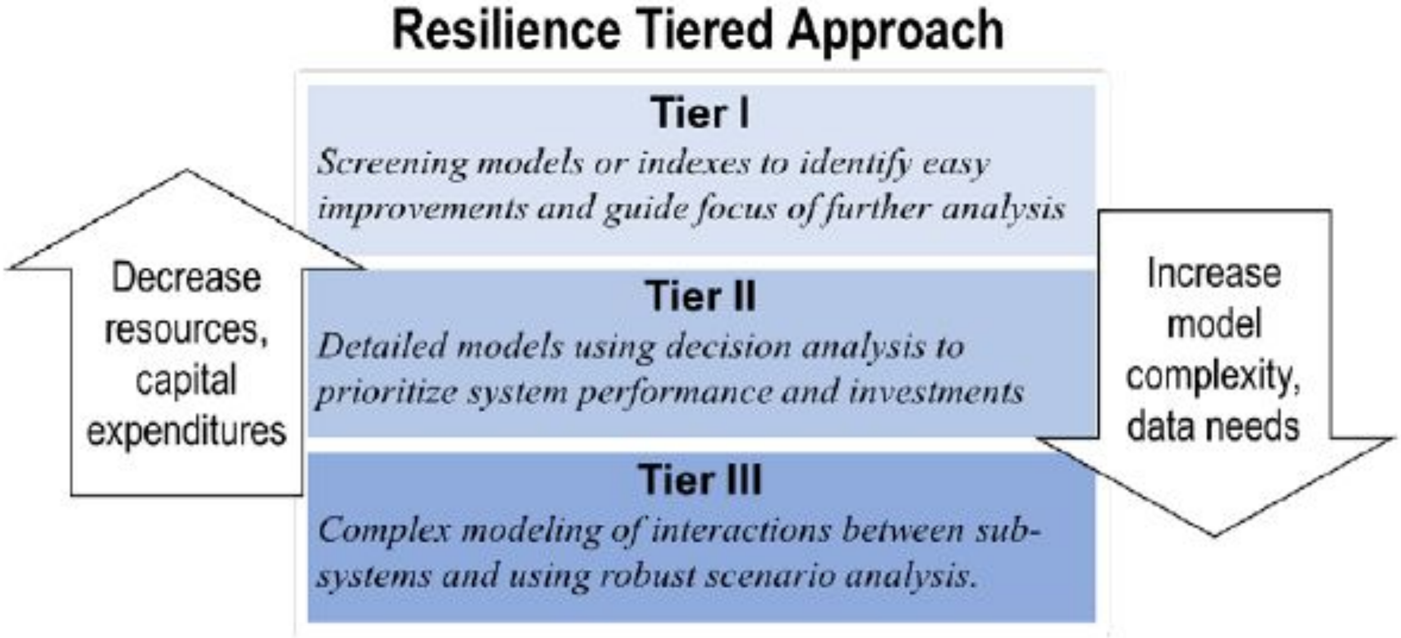


Figure 2.Metric-based and model-based approaches for Resilience Assessment. Multiple tools have been developed to address resilience in systems in both methodological groups.



Resilience Tiered Approach

Tier I

Screening models or indexes to identify easy improvements and guide focus of further analysis

Tier II

Detailed models using decision analysis to prioritize system performance and investments

Tier III

Complex modeling of interactions between sub-systems and using robust scenario analysis.

Decrease resources, capital expenditures

Increase model complexity, data needs

Figure 3. Overview of tiered approach to resilience assessment

Proposed Parameters for Assessing Cyber Resilience

We have chosen appropriate parameters for the evaluation of Cyber Resilience and have classified the various parameters into the different stages of the Cyber Resilience as follows.

Plan/Prepare:

1. Asset management
2. Infrastructure and Information assessment
3. Governance structure and processes
4. Information security and policy deployment
5. Configuration Management
6. Controls Management
7. Vulnerability assessment and management
    a. Black Box Testing
    b. Grey Box Testing
    c. White Box Testing
8. Malware Protection Deployed
9. Training and awareness

Detection:

1. Intrusion Detection & Prevention
2. Incident management
3. External dependencies management
4. Situational awareness
5. Risk management

Respond/Recover:

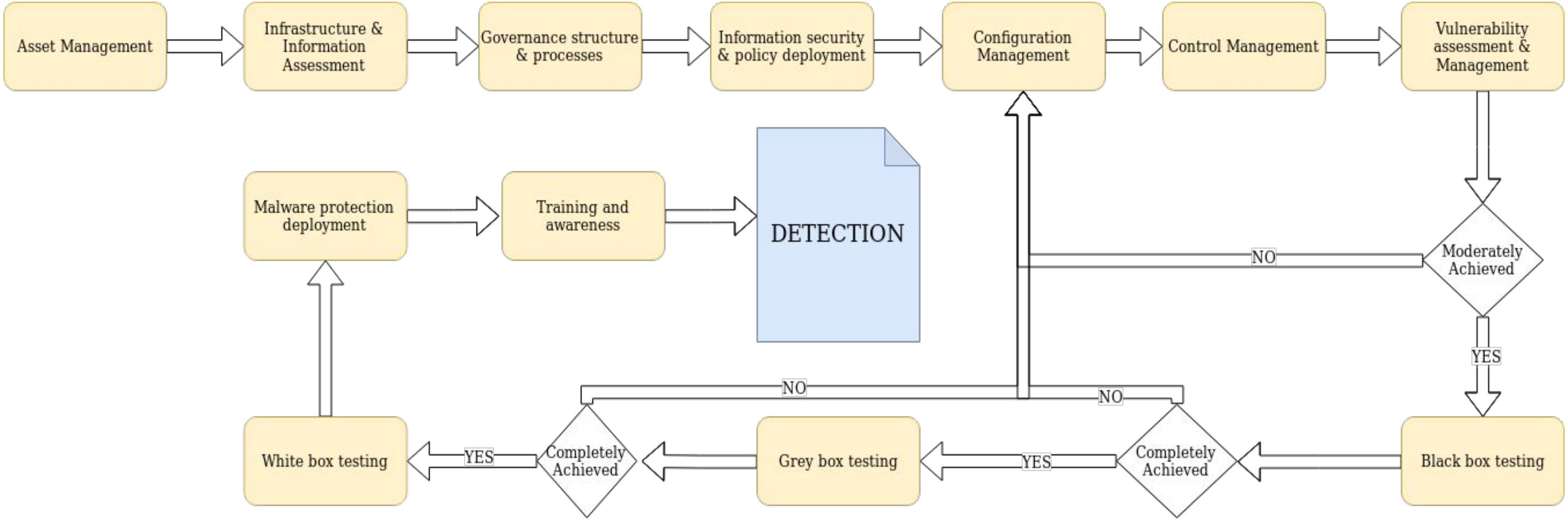
1. Information sharing and collaboration
2. Incident response management
3. Service continuity management

Adapt:

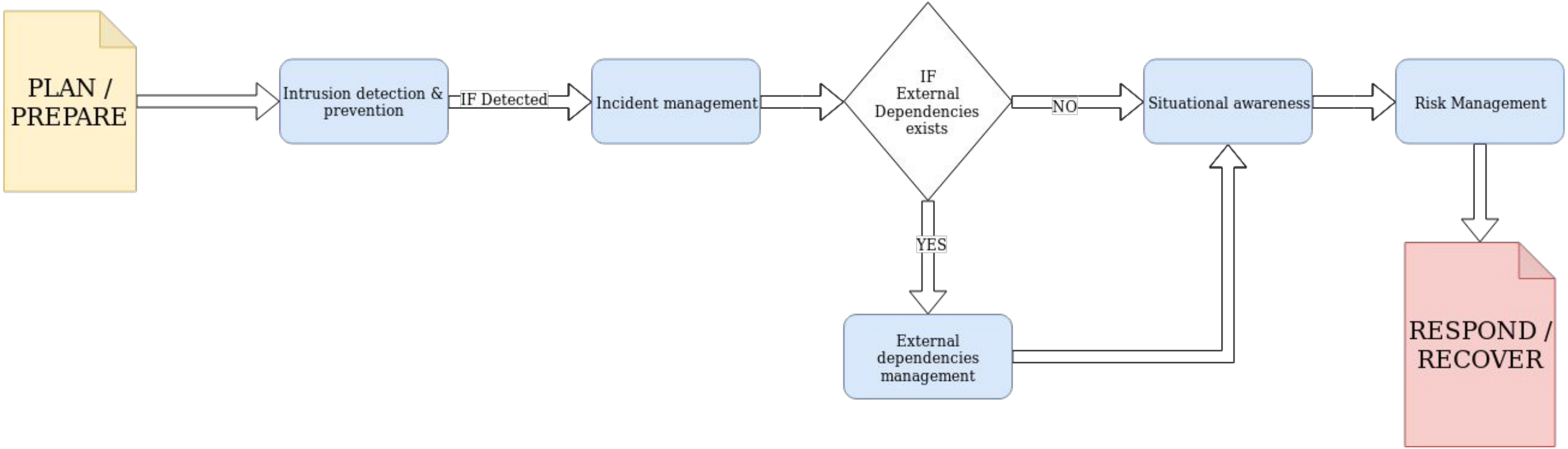
1. Recent Security Breaches
2. Comprehensive risk management programme
3. Internal audit
4. Change management
5. Continual improvement process
6. Information and security policies updation
7. Asset infrastructure updation
8. Board-level commitment and involvement
9. External certification/validation

Flowcharts

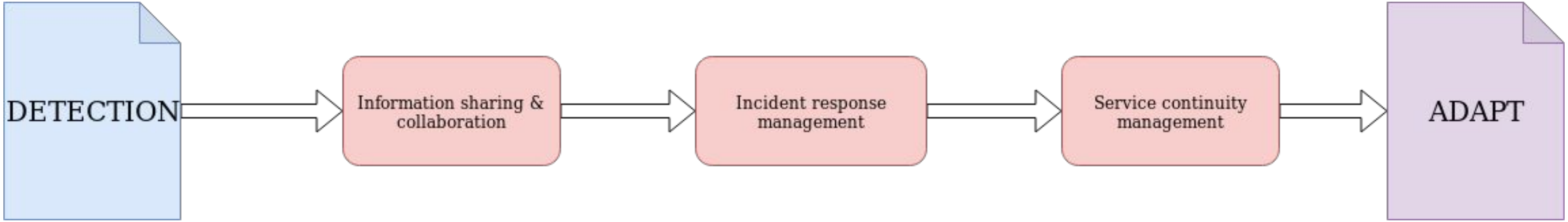
PLAN / PREPARE



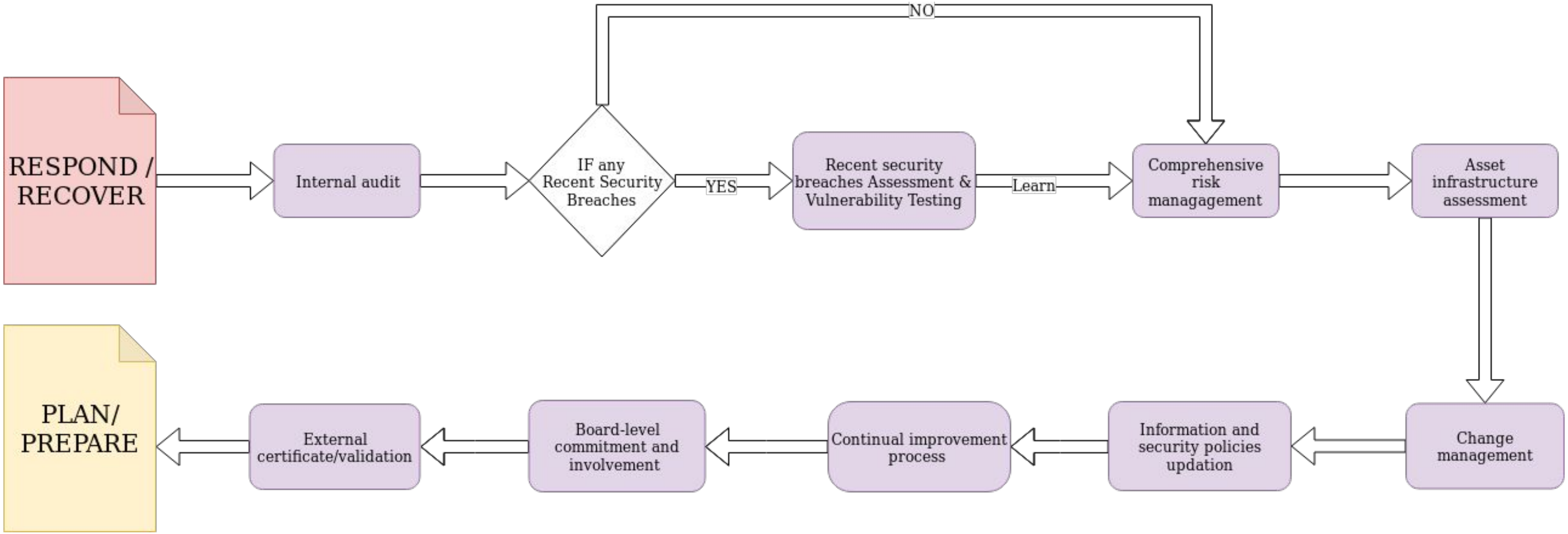
DETECT


PLAN / PREPARE
Intrusion detection & prevention
IF Detected
Incident management
IF External Dependencies exists
NO
Situational awareness
Risk Management
YES
External dependencies management
RESPOND / RECOVER

RESPOND / RECOVER


DETECTION
Information sharing & collaboration
Incident response management
Service continuity management
ADAPT

ADAPT


RESPOND / RECOVER
Internal audit
IF any Recent Security Breaches
NO
YES
Recent security breaches Assessment & Vulnerability Testing
Learn
Comprehensive risk managagement
Asset infrastructure assessment
Change management
Information and security policies updation
Continual improvement process
Board-level commitment and involvement
External certificate/validation
PLAN/ PREPARE

Scoring Mechanism

- Each of the parameters are judged by the organisation itself or some external organisation and then given a score from 0-10 as follows:
    - Not Achieved -> 0
    - Partially Achieved -> 2
    - Moderately Achieved -> 4
    - Mostly Achieved -> 6
    - Completely Achieved -> 8
    - Well Defined -> 10
- After this, all the different stages of Cyber Resilience is given score based on the average of the scores in the corresponding parameters that comes under that stage.
- Finally, the Overall Cyber Resilience score for an organisation is calculated by the average of the scores in all the stages of Cyber Resilience.

Parameters Description

PLAN/PREPARE parameters

Asset management:

Identify, document, and manage assets during their lifecycle to ensure sustained productivity to support critical services.

Infrastructure and Information assessment:

Regardless of recent improvements in network performance and capacity, it is essential for any organization to periodically assess the reliability of IT Infrastructure and its ability to address business requirements. Assessment of infrastructure and information to find security vulnerabilities and finding gaps in the existing defenses are one of the most important assessment.

Governance structure and processes:

Governance is the set of responsibilities and practices exercised by those responsible for an enterprise (e.g., the board and executive management in a corporation, the agency head for a Federal agency) with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

PLAN/PREPARE parameters

Information and security policies:

Set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority.

Configuration Management:

The Configuration Management domain addresses an organization can implement processes and procedures that manage assets and ensure that changes made to those assets are minimally disruptive to the organization.

Controls Management:

The Controls Management domain represents a way for the organization to identify control objectives and establish controls to meet those objectives.

PLAN/PREPARE parameters

Vulnerability assessment and management:

Vulnerability assessment and management consists of identify, analyze, and manage vulnerabilities in a critical service's operating environment

- **Black Box Testing:**

  Black box security testing mimics the actions of a hacker, attacking the application from the outside, with zero knowledge of the inner workings of the application. In doing so, it tests the functionality of the application.

- **Grey Box Testing:**

  Grey box security testing is a combination of white box and black box testing, where the hacker has some limited knowledge of the internal workings of the application.

PLAN/PREPARE parameters

- **White Box Testing:**

White box testing mimics the actions of a hacker having all knowledge of the application, testing the application's internal workings.

Malware Protection Deployed:

It deals with the level of the protection deployed for Malwares.

Training and awareness:

Training and awareness focuses on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization's operational cyber resilience requirements and goals are known and met.

DETECTION parameters

Intrusion detection & Prevention:

Intrusion-detection is capability of detecting break-ins, penetrations, and other forms of computer abuse is described.

Intrusion-prevention is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

Incident management:

The Incident Management domain examines an organization's capability to recognize potential disruptions, analyze them, and determine how and when to respond.

External dependencies management:

External Dependency Management focuses on external entities that provide, sustain, or operate Information and Communications Technology (ICT) to support the organization.

DETECTION parameters

Situational awareness:

Situational awareness revolves around actively discovering and analyzing information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.

Risk management:

Risk Management involves of identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.

RESPOND/RECOVER parameters

Information sharing and collaboration:

Information sharing and collaboration enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors.

Incident response management:

An incident response management deals with collection of procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery.

Service continuity management:

Service continuity management ensures the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other event.

ADAPT parameters

Recent Security Breaches:

Analyzing the previous security breaches and threats that occured on the organisation and adapting to them to better handle those threats in future.

Comprehensive risk management programme:

The forecasting and comprehensive evaluation of security risks together with the identification of procedures to avoid or minimize their impact.

Internal audit:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

ADAPT parameters

Change management:

Change management processes ensures the integrity of assets, using change control and change control audits.

Continual improvement process:

An incremental effort to improve products, services, or processes.

Information and security policies updation:

The updation of Information and security policies after analyzing the happened attacks and adapting to them.

ADAPT parameters

Asset infrastructure updation:

Asset infrastructure updation includes creation,updation and maintenance of asset register.

Board-level commitment and involvement:

Any strategic key decision cannot be taken without the approval from the Board of director, thus for high level operational needs. Thus involvement of Board-level commitment is important and is essential for running the business.

External certification/validation:

Whether the organisation have some external certifications or have their validation done by some external agency.

Cyber Resilience Process improvement:

The Cyber Resilience Assessment provides us the current state of our enterprise cyber resiliency and also identifies specific gaps in the various domains of cybersecurity.

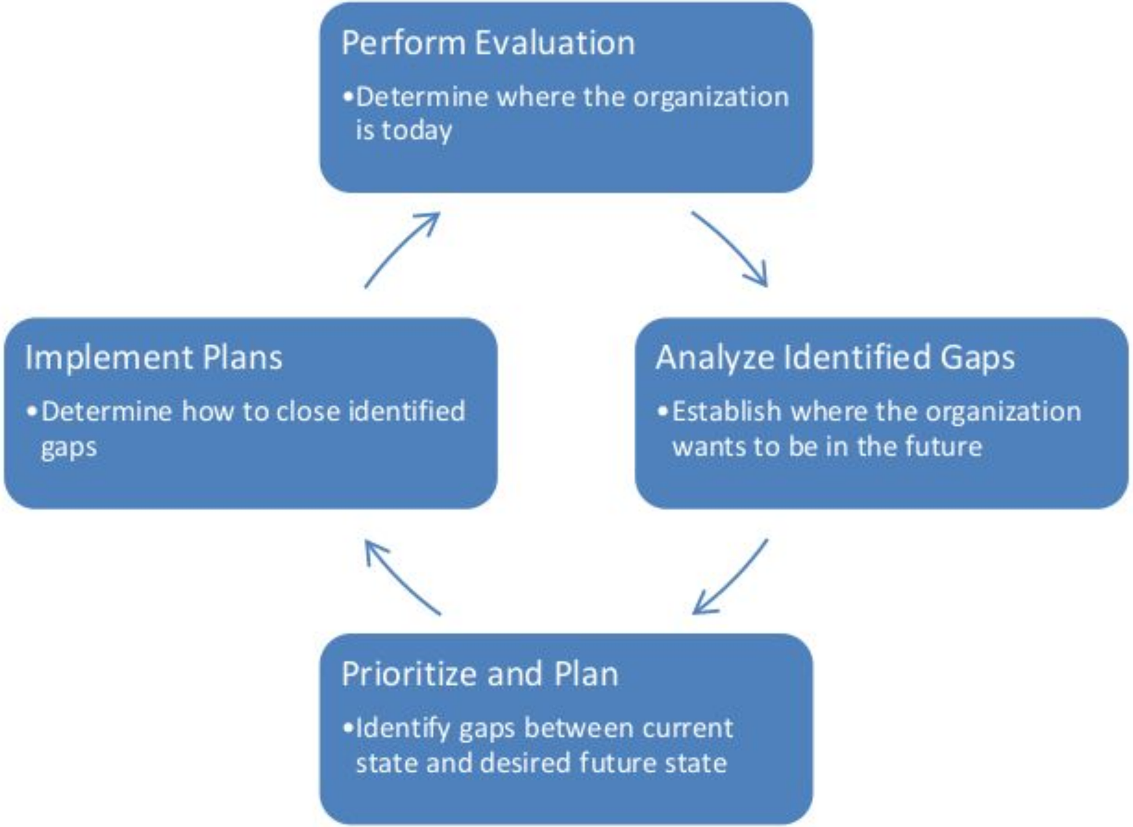
The next step that remains is to analyze those gaps and improve the overall cyber resiliency of our enterprise.

Making improvements:

The Cyber Resilience Assessment provides an organization with information on its current level of cybersecurity capabilities in each of the four stages of Cyber Resilience, but it does not prescribe that organizations should reach specific score in any particular stage or parameter.

The organization must determine the appropriate plan of action for improvement based on organizational objectives and risk environment.

But the CR(Cyber Resilience) Assessment can be used as a baseline for initiating a process improvement project, as depicted:



Perform Evaluation

- Determine where the organization is today

Analyze Identified Gaps

- Establish where the organization wants to be in the future

Prioritize and Plan

- Identify gaps between current state and desired future state

Implement Plans

- Determine how to close identified gaps

Figure 17: Steps in a Typical Process Improvement Activity

Let us now focus on the three phases of a process improvement project that remain after the self-assessment is performed:

- Analyze Identified Gaps
- Prioritize and Plan
- Implement Plans

Analyze Identified Gaps:

It generally is not optimal for an organization to strive to achieve the highest score in all domains.

The organization should instead determine the level of practice performance and score achievement for each domain that best enable it to meet its business objectives and cybersecurity strategy.

This collection of desired capabilities is the organization’s target state of practice performance and score achievement.

Following approach can be used for identifying a target state:

The organization begins by walking through its scores in each parameter of the CR Assessment and performing the following steps:

1. Identify all of the practices that have a low score.

2. For each practice that has a low score, review the practice and determine whether the practice needs to be performed to meet the organization’s business and cybersecurity objectives.

3. If the practice needs to be performed, then document that practice.

4. If the practice does not need to be performed, then move on to the next practice for which there was a low score.

5. Repeat steps 1 through 4 for all practices in that stage of the Cyber Resilience.

6. Repeat for all the stages of the Cyber Resilience.

The generated list of practices that need to be performed also serves as the list of gaps to be addressed. This list of gaps gives the organization a starting point for prioritizing and planning.

Prioritize and Plan:

The prioritization should be done using criteria such as:

- how gaps affect organizational objectives and critical infrastructure
- the criticality of the business objective supported by the domain
- the cost of implementing the necessary practices
- the availability of resources to implement the practices.

A cost-benefit analysis for gaps and activities can inform the prioritization of the actions needed.

Next, the organization should develop a plan to address the selected gaps. An organizational sponsor would ideally be the owner of the plan, though responsibility for implementation might be assigned to a person designated by the sponsor.

Implement Plans:

For the plan to succeed, organizations must provide adequate resources, including people with the necessary skills to accomplish the planned tasks and an adequate budget. In addition, the organization must continue supporting the execution of the plan by tracking progress and recognizing accomplishments.

After plans have been developed and implemented to address selected gaps, the organization should periodically reevaluate its business objectives and the risks to determine if changes to desired capability are needed.

Periodic reassessment using our proposed CR Assessment method can track progress toward the organization’s desired capability profile.

Thank you