Why Should You Care about Cyber Security?

Sandeep K. Shukla
C3i Hub
IIT Kanpur

Outline

- Threat Landscape
- Modus Operandi of Attackers
- Best Practices
  - Cyber Security Governance
  - Cyber Security Policy Enforcement
  - Risk Assessment
  - Risk Driven Control for Risk Mitigation
    - Configuration and Control Management
  - Asset Management
  - Vulnerability Management
  - Patch Management
  - Monitoring and Response
  - Regular Audit and Compliance
  - Awareness and Training

Cyber Threat Landscape

ETPrime

India sees sharp increase in cyberattacks in Q1 2023: report

ETtech • Last Updated: May 09, 2023, 02:09 PM IST

SHARE FONT SIZE SAVE

Synopsis

India has seen a sharp increase in the number of cyberattacks in the first three months of 2023, as per a report. Over 500 million cyberattacks were blocked in Q1 2023 out of a billion attacks globally, as per the State of Application Security Report' by Indusface.

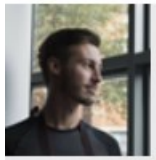
C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

$265 billion

Ransomware will cost its victims around $265 billion (USD) annually by 2031.

14 OCT 2022 NEWS

Education Sector Experienced 44% Increase in Cyber-Attacks Over Last Year

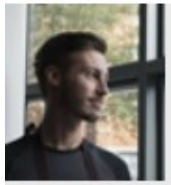


Alessandro Mascellino Freelance Journalist
Email Alessandro Follow @a_mascellino

The education sector experienced a 44% increase in cyber-attacks when compared to 2021, with an average of 2297 attacks against organizations every week, according to Check Point's *2022 Mid-*

14 SEP 2022 NEWS

SparklingGoblin APT Targeted Hong Kong University With New Linux Backdoor



Alessandro Mascellino Freelance Journalist
Email Alessandro Follow @a_mascellino

A Linux variant of the SideWalk backdoor was used by the SparklingGoblin advanced persistent

Indian education sector biggest target of cyber threats, remote learning among key triggers: Report

PTI / Updated: May 1, 2022, 16:26 IST

SHARE AA

YOU'RE READING

Indian education sector biggest target of cyber threats, remote learning...

Education · 1 Min Read

India tops global cyber attacks on education sector: CheckPoint Research

In India, schools, universities and research centers make for attractive targets to cy criminals because they are often under-resourced from a security perspective

A cancer centre is the latest victim of cyber attacks. Why health data hacks keep happening

Published: May 8, 2023 2.40am BST

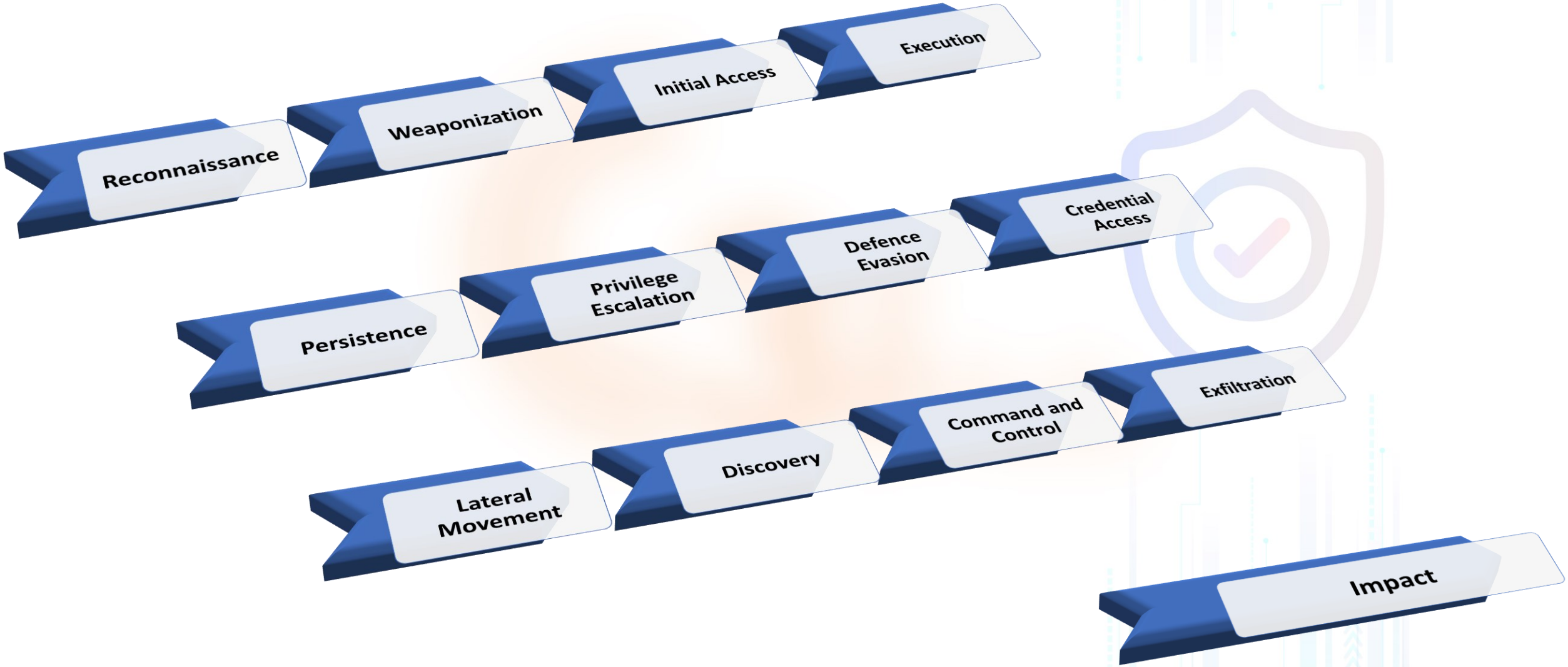
Shutterstock

It seems hardly a day goes by without another report of a cyber crime incident. With Medibank still fresh in our minds, the latest attack is on a Sydney-based cancer treatment facility, Crown Princess Mary Cancer Centre in Westmead Hospital.

Authors

Moh
Senic
Secu

Modus Operandi


Reconnaissance
Weaponization
Initial Access
Execution
Persistence
Privilege Escalation
Defence Evasion
Credential Access
Lateral Movement
Discovery
Command and Control
Exfiltration
Impact

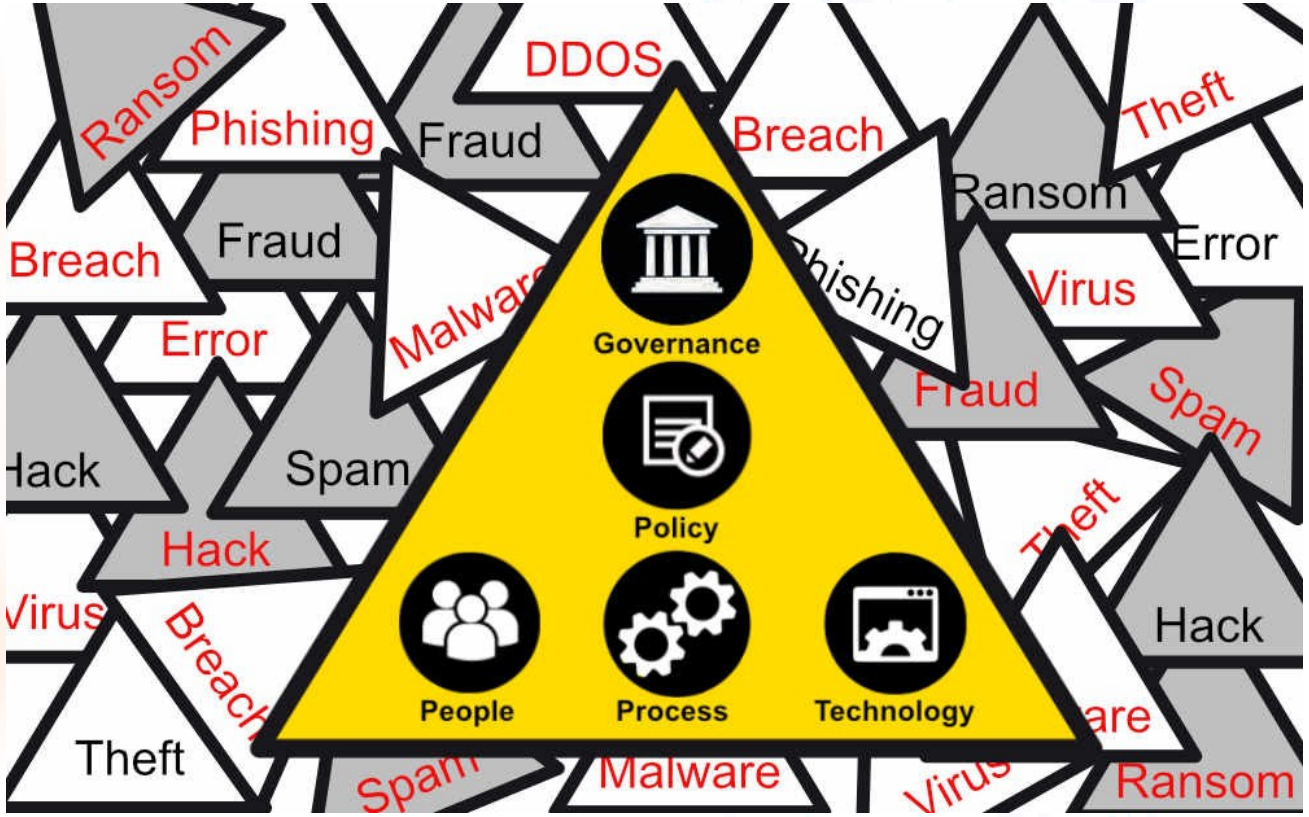
Best Practices

Cyber Security Governance

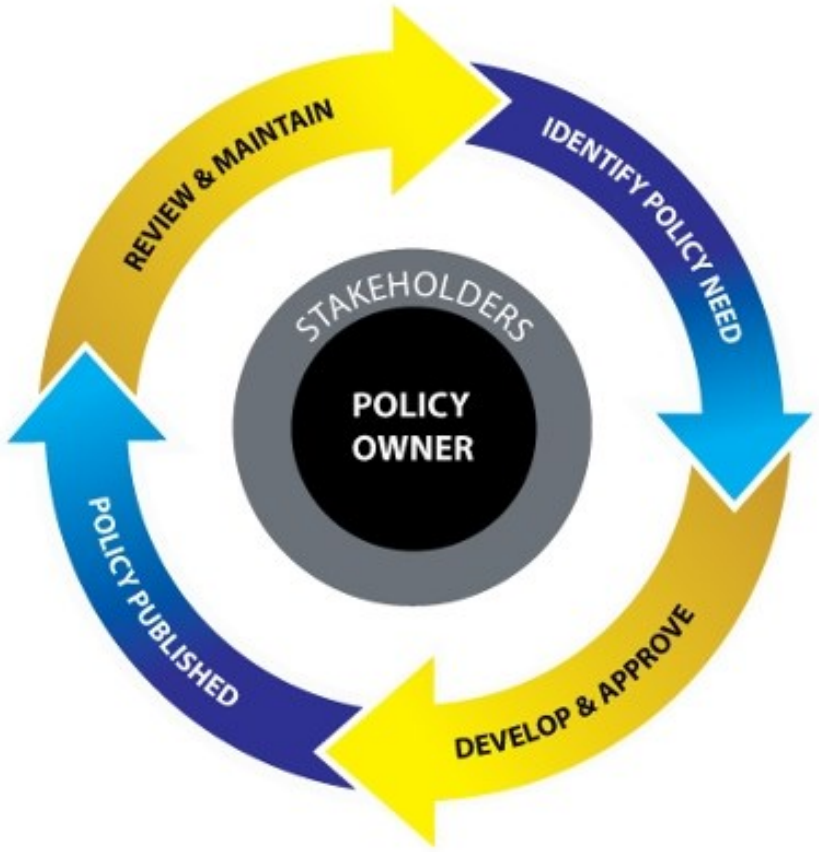
Cyber Security is not just about technology

Governance involves

- Board of Directors
- C-Suite Executives
- Legal
- IT and OT Management
- Culture and Processes



Cyber Security Policy



- Adoption of an elaborate cyber security policy
- Board Level Buy in
- Wide dissemination among employees and stake holders
- Implementing and Enforcing the adopted Policy
- Carrot and Stick approach in Enforcing
- Repeated Awareness Training

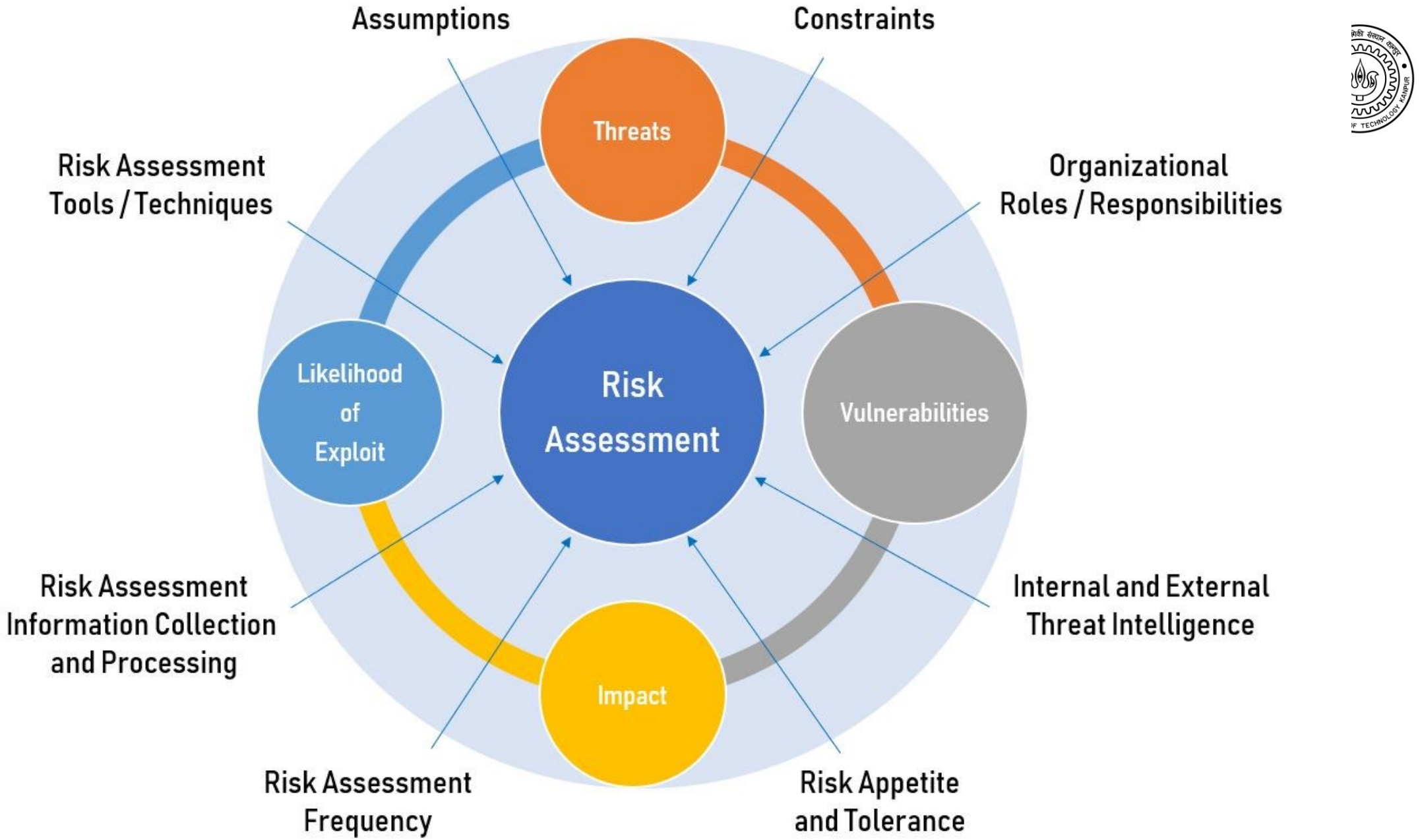
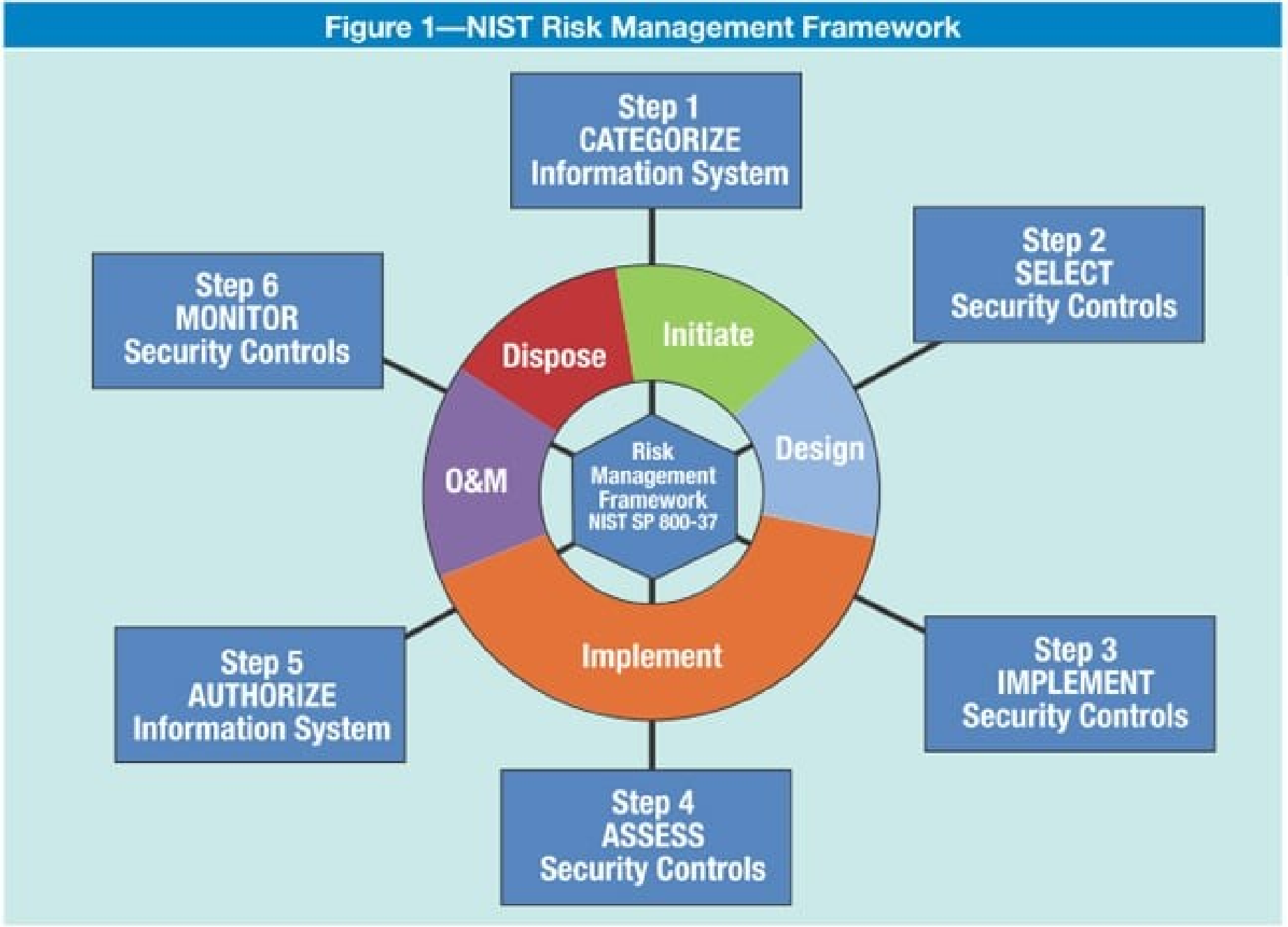
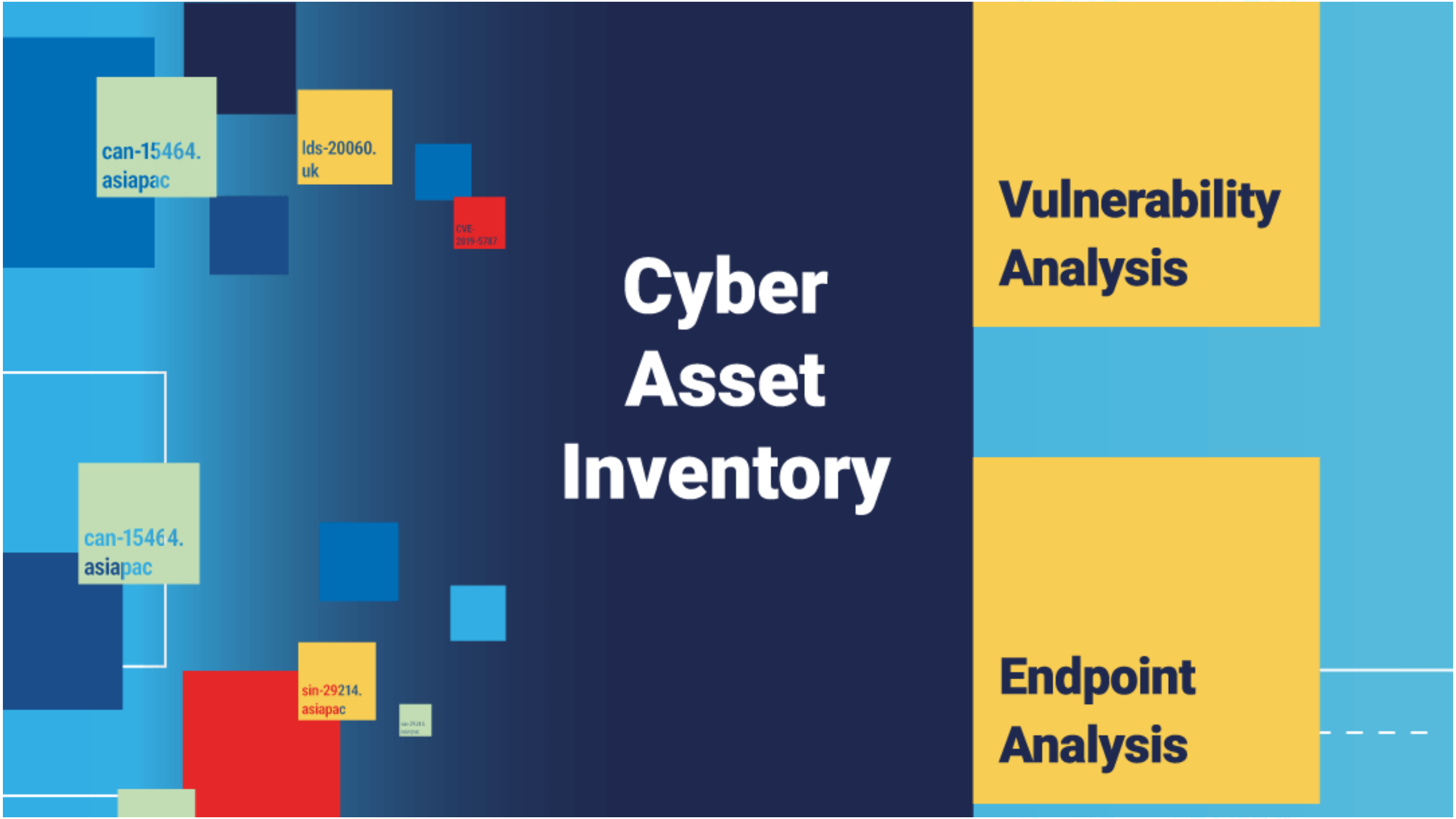

Assumptions
Constraints
Threats
Risk Assessment Tools / Techniques
Organizational Roles / Responsibilities
Likelihood of Exploit
Risk Assessment
Vulnerabilities
Risk Assessment Information Collection and Processing
Internal and External Threat Intelligence
Impact
Risk Assessment Frequency
Risk Appetite and Tolerance

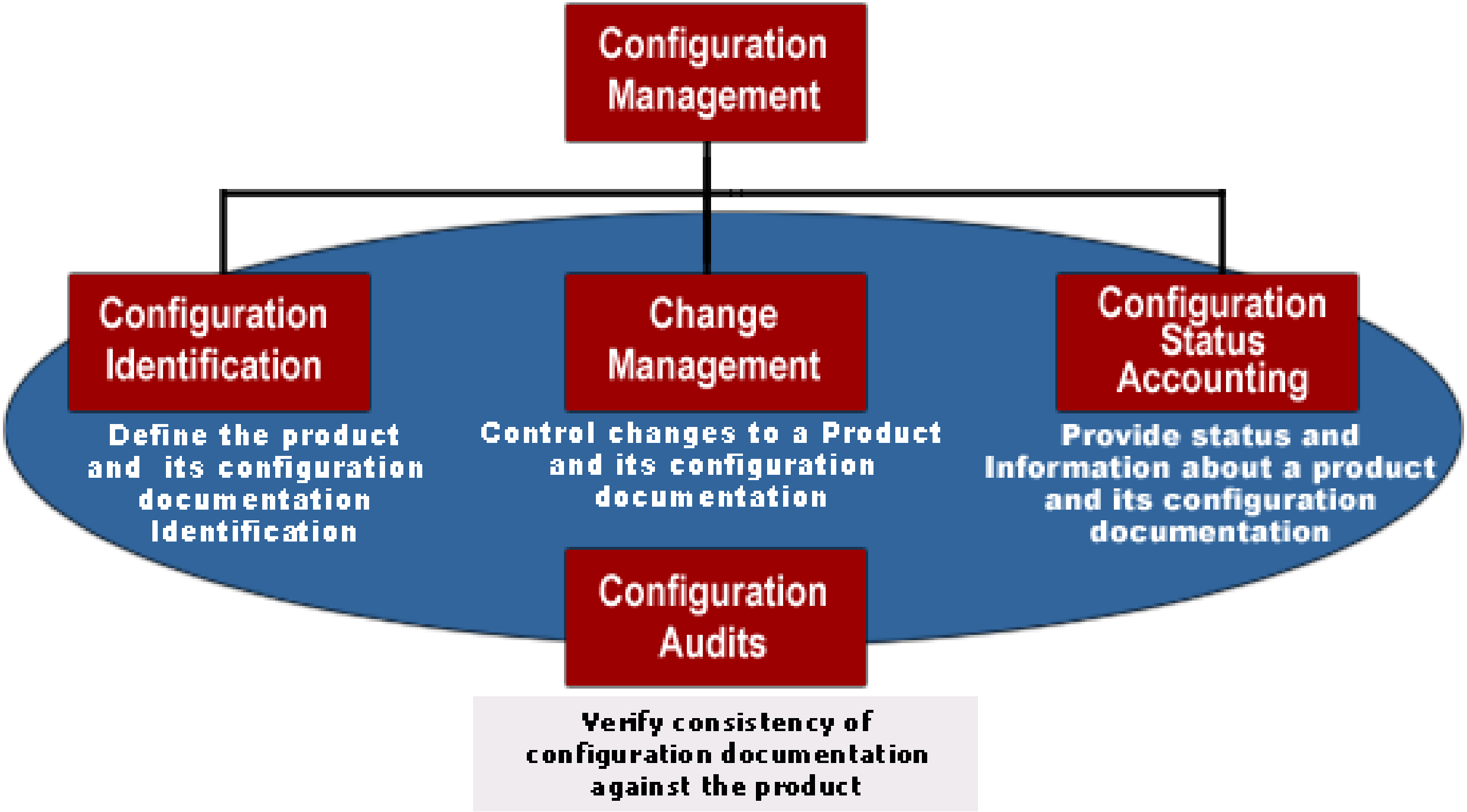
Figure 1—NIST Risk Management Framework



Source: National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST Special Publication 800-37, Revision 1, February 2010, figure 2-2. Reprinted with permission.


can-15464.
asiapac
lds-20060.
uk
CVE-
2019-5787
Cyber
Asset
Inventory
Vulnerability
Analysis
can-15464.
asiapac
sin-29214.
asiapac
Endpoint
Analysis


7
STEPS OF A PATCH MANAGEMENT PROCESS
DISCOVER MISSING PATCHES
01
DOWNLOAD PATCHES FROM VENDOR SITES
02
PRIORITIZE THE PATCHES
03
TEST THE PATCHES
04
DEPLOY THE PATCHES ON ENDPOINTS
05
PERFORM A PATCH AUDIT
06
UPDATE THE PATCH JOB REPORT
07


Configuration Management
Configuration Identification
Define the product and its configuration documentation Identification
Change Management
Control changes to a Product and its configuration documentation
Configuration Status Accounting
Provide status and Information about a product and its configuration documentation
Configuration Audits
Verify consistency of configuration documentation against the product


Vulnerability
Management

Cyber Security Monitoring & SoC

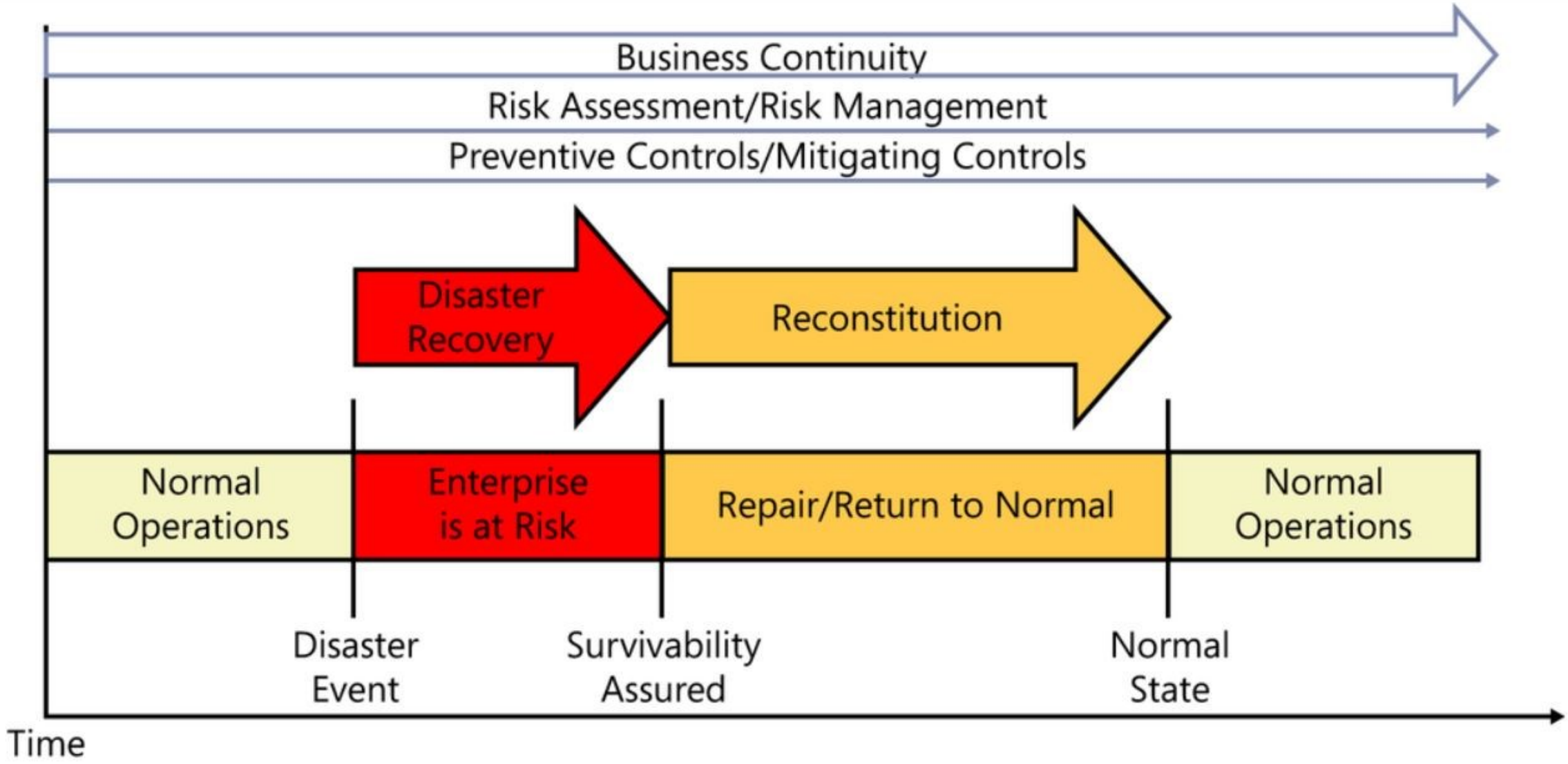


Figure 8-1. The timeline of disaster recovery and business continuity


COMPLIANCE
STANDARDS
POLICIES
RULES
REGULATIONS

Cyber Security Awareness Training

DCENCOMPASS

Educating staff on the importance of Cyber Security Awareness

The staff induction process is an ideal time to train new employees about the importance of cyber security.

Why is it so important?

Under the Notifiable Data Breaches (NDB) scheme, Australian organisations are required to report data breaches

What's involved?

An effective cyber security awareness training course should be practical and inclusive (all staff should be able to understand the material).
The following topics are usually covered during a session:-

- The Privacy Act (outline responsibilities)
- Document handling and classification policies
- Types of threats
- Phishing attacks
- The dangers of downloading "unofficial" files
- Social engineering
- The dangers of installing "unofficial"
- Best practice password
- Public Wi-Fi hotspots (the need for VPN

Final Words

- Cyber Threats are immense
- Attacks are waiting to happen
- Identify, Protect, Detect, Respond and Recover
- Non-trivial to create a suitable cyber security posture
- In today's world – impossible to avoid
- Be Cyber Safe