MASTER OF SCIENCE
IN ENGINEERING

TSM_SecIndOpT

Incident Response (I)

Version: 1.1

Luca Haab | 05.05.2025 | Cours MSE

swissuniversities

Imagine a situation

Oil Transport: a fictive OT company

This Photo by Unknown Author is licensed under CC BY-SA

This image is created using the author own code

What would you

- Have done before the incident?
- Do during the incident?

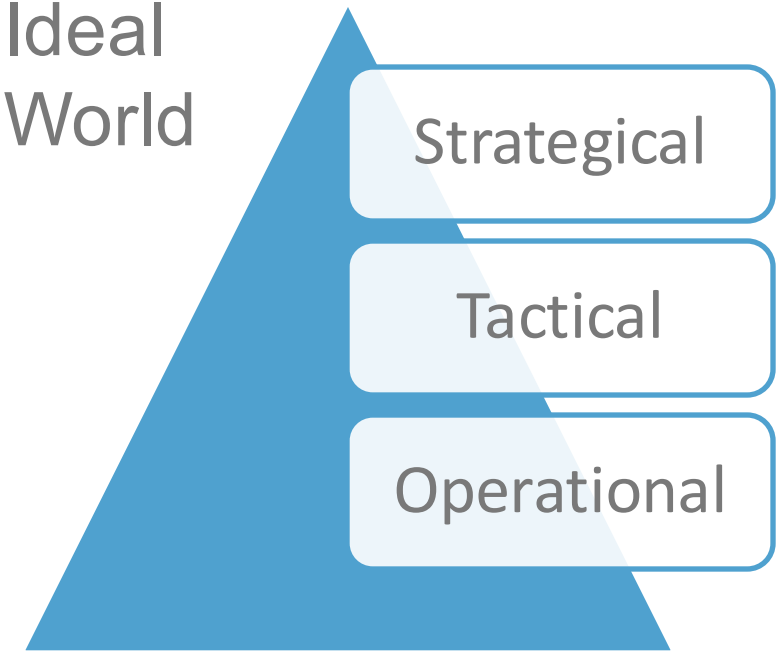
Head to

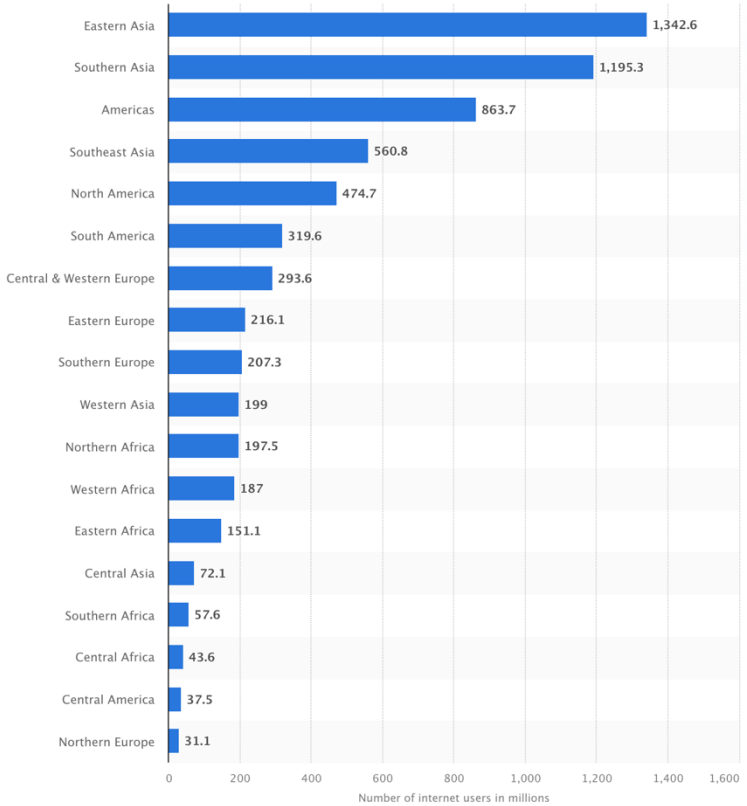
https://secindopt.github.io/homepage/exercices/incident_response/#exercice-1-a-fictive-ot-company-under-attack

This Photo by Unknown Author is licensed under CC BY-SA-NC

Context

- Business Planning Ideal World





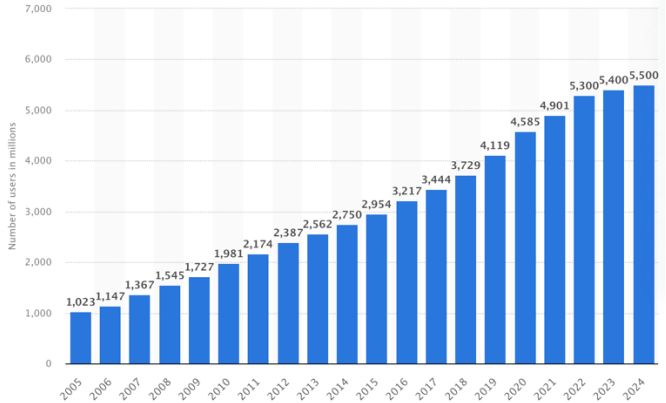
Source: https://www.statista.com/statistics/249562/number-of-worldwide-internet-users-by-region/

Abnormal Operations: Contingency

There are four types of contingency plans (CP):

- incident response planning (IR)
- disaster recovery planning (DR)
- business continuity planning (BC)
- crisis management planning (CM)

CP itself is designed to oversee the staffing and development for all of the subordinate sets of plans.

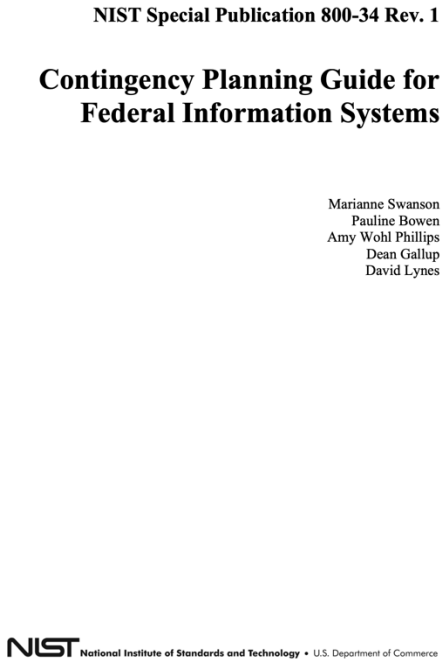


Source: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

The main goal of CP is to restore normal modes of operation with minimal cost and disruption to normal business activities after an adverse event.

Contingency Planning

"Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical [illegible] system's information


NIST Special Publication 800-34 Rev. 1

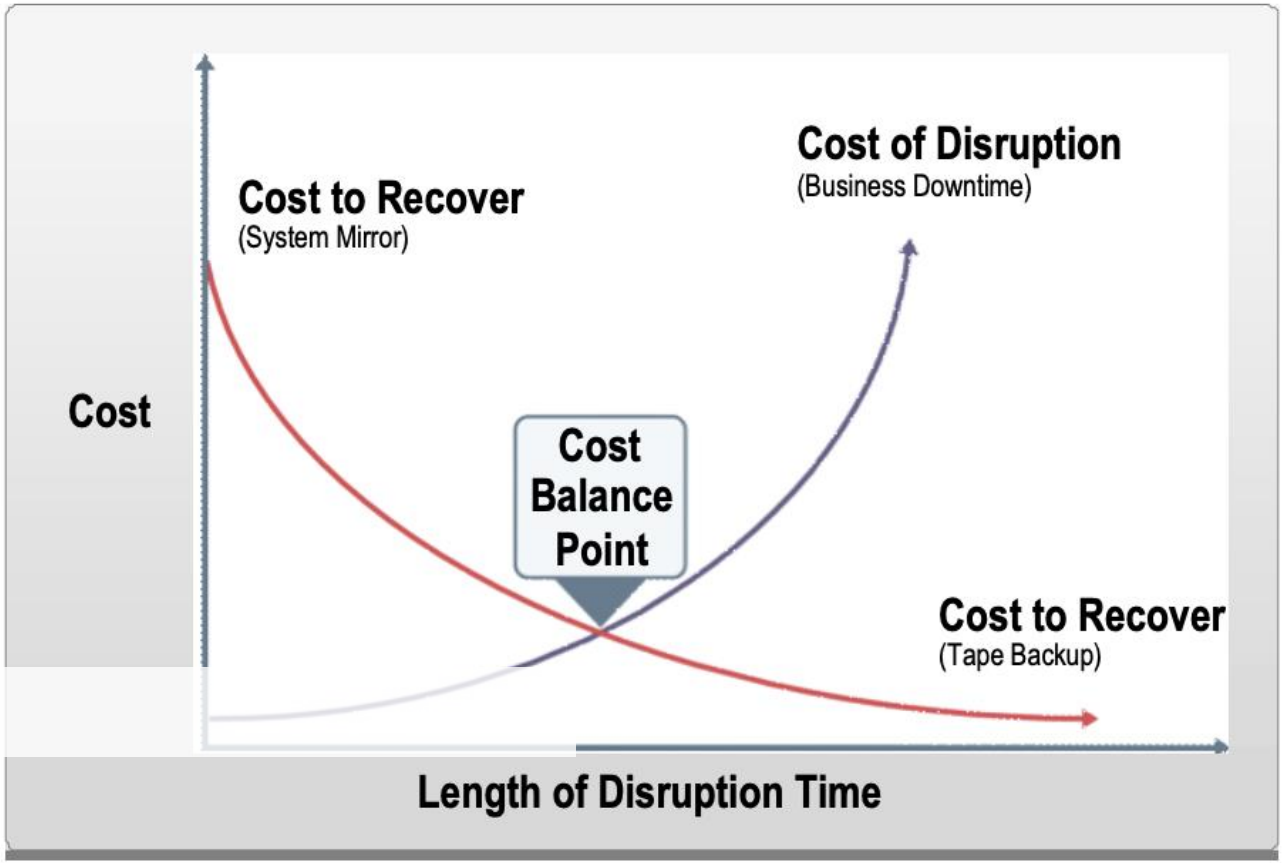
Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Be aware



Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Incident Response Plan

It entails

- Preparation for
- Detection of
- Reaction to
- Recovery from

Incidents.

Disaster Recovery Plan

Disaster Recovery

- involves preparing for and
- recovering from disasters,
- whether natural or man-made

- Recover assets that are salvageable
- Purchase or replace assets from appropriate sources
- Reestablish functional assets at the primary site (or at a new one if need be)

Business Continuity Plan

It ensures that critical business activities can continue if a disaster occurs

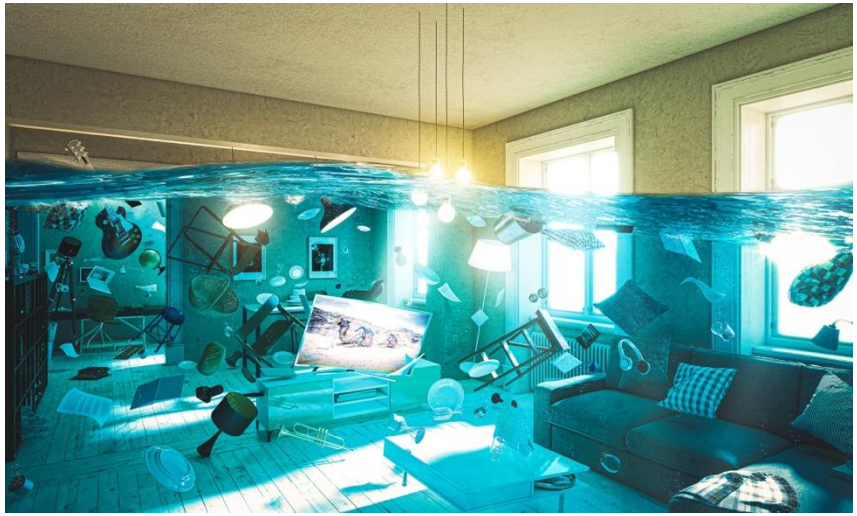
- Relocates core functions to a temporary facility
- Managed by CEO or COO
- Activated shortly after DR

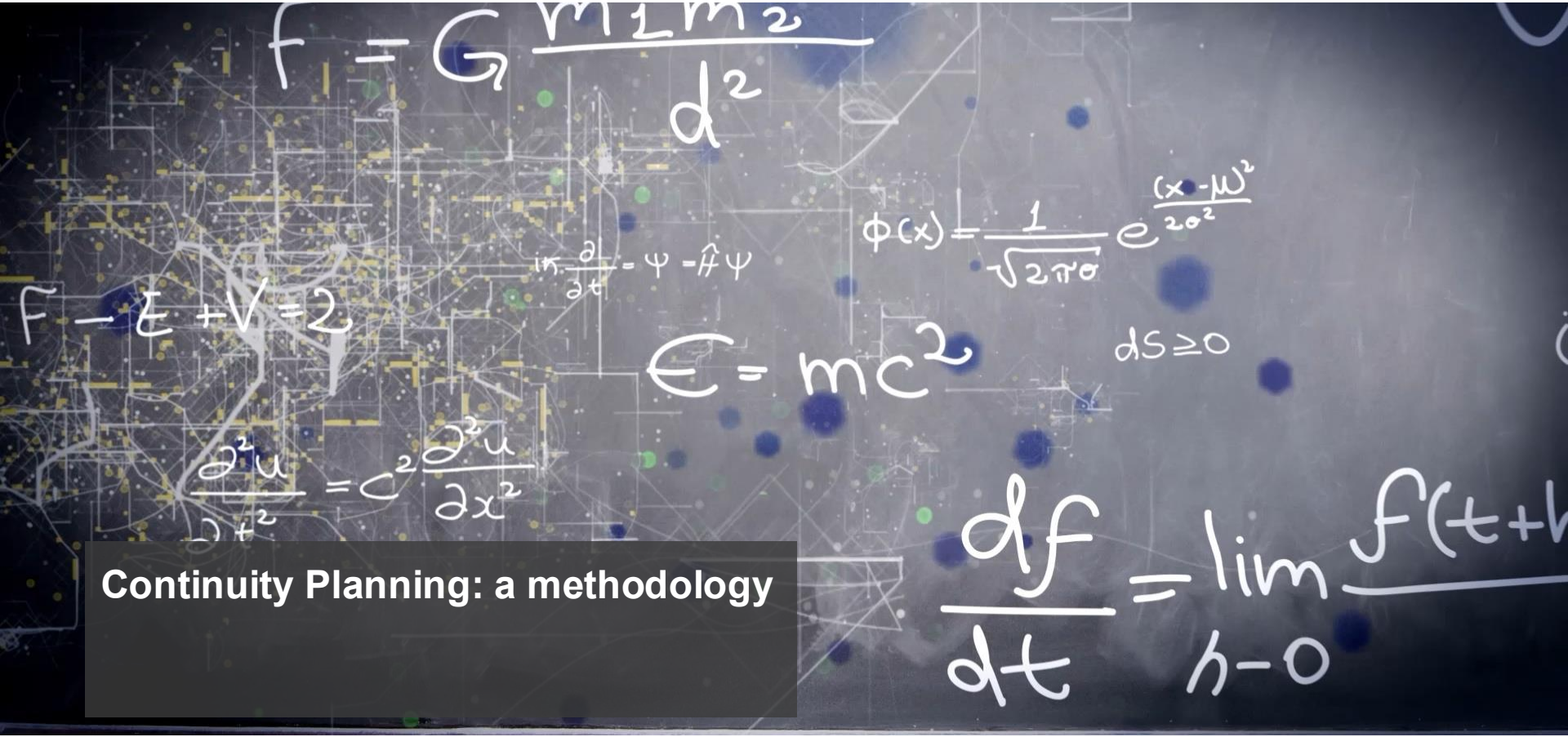
An example of a failure (in German): https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite/ or https://www.blick.ch/schweiz/ostschweiz/swisswindows-ag-macht-per-sofort-dicht-170-mitarbeiter-entlassen-hacker-angriff-versetzte-den-todesstoss-id15771321.html

Crisis Management Plan

Focuses on

- Protection of human health and welfare
- Managing the crisis
- Supporting employees and guests
- Keeping the public informed
- Communicating with major stakeholders




Continuity Planning: a methodology

CP Methodology

- Contingency Planning Management Team (CPMT)
- Policy to guide the process
- Methodology
- Business Impact Analysis (BIA)

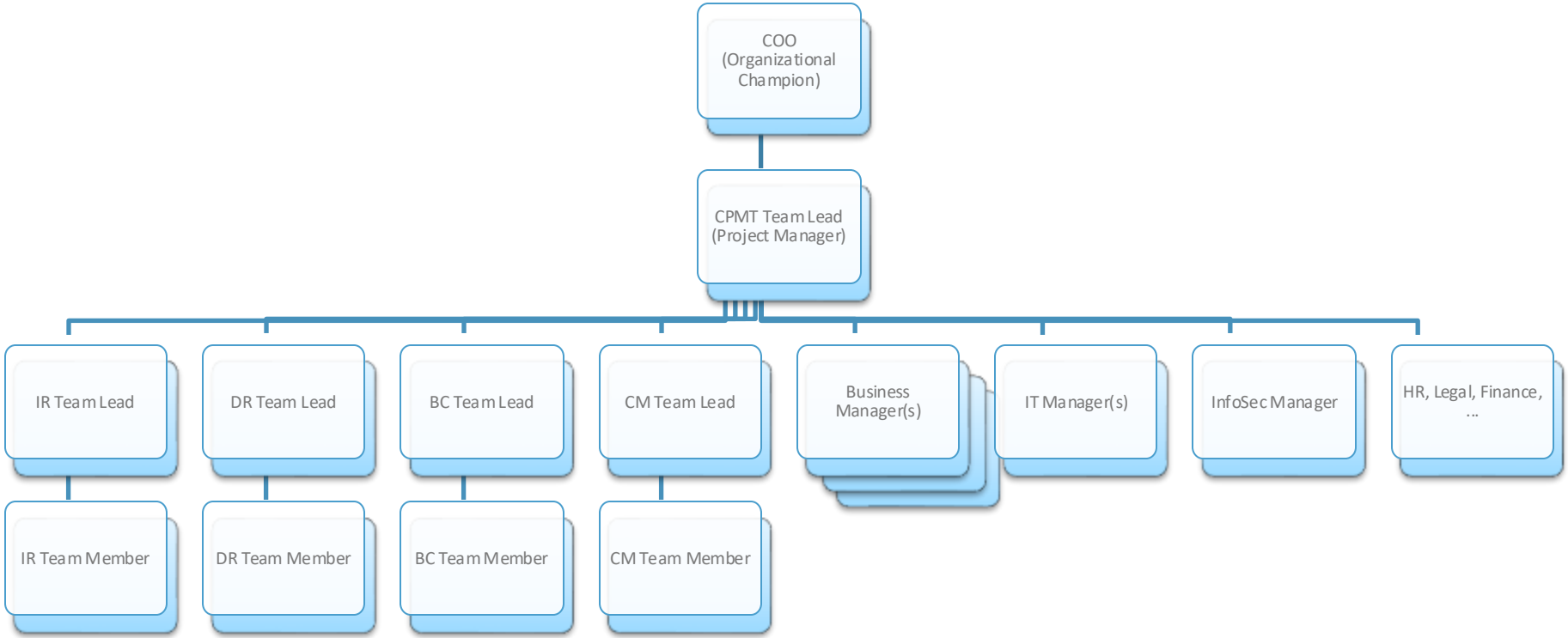
CP Methodology

1. Form the CPMT
2. Develop the CP policy
3. Conduct the Business Impact Analysis (BIA)
4. Form subordinate planning teams
5. Develop subordinate planning policies
6. Integrate the BIA
7. Identify preventive controls
8. Organize response teams
9. Create response strategies
10. Develop subordinate plans
11. Ensure testing, training and exercices

CPMT

After the definition of CP project – done in cooperation with senior management – the CPMT is responsible for:

- Obtaining commitment from senior management
- Managing and conducting the overall process
- Writing the master CP document
- Conducting the Business Impact Analysis (BIA)
- Organizing and staffing the subordinate teams – including both planning and response teams
- Providing guidance to and integrating the work of subordinate teams


COO (Organizational Champion)
CPMT Team Lead (Project Manager)
IR Team Lead
DR Team Lead
BC Team Lead
CM Team Lead
Business Manager(s)
IT Manager(s)
InfoSec Manager
HR, Legal, Finance, …
IR Team Member
DR Team Member
BC Team Member
CM Team Member

CP Policy

- Introductory statement (how important CP is)
- Statement of scope and purpose of CP
- Call for periodic risk assessment and BIA
- Definition of the major components of CP
- Identification of the key individuals responsible for CP operations and related, clear, definition of roles and responsibilities
- Call for, and guidance in, the selection of recovery options and business continuity strategies
- Requirement to train,exercice and test the various plans
- Identification of key laws, standard and regulations
- Challenge the organization

Business Impact Analysis (BIA)

It requires you to

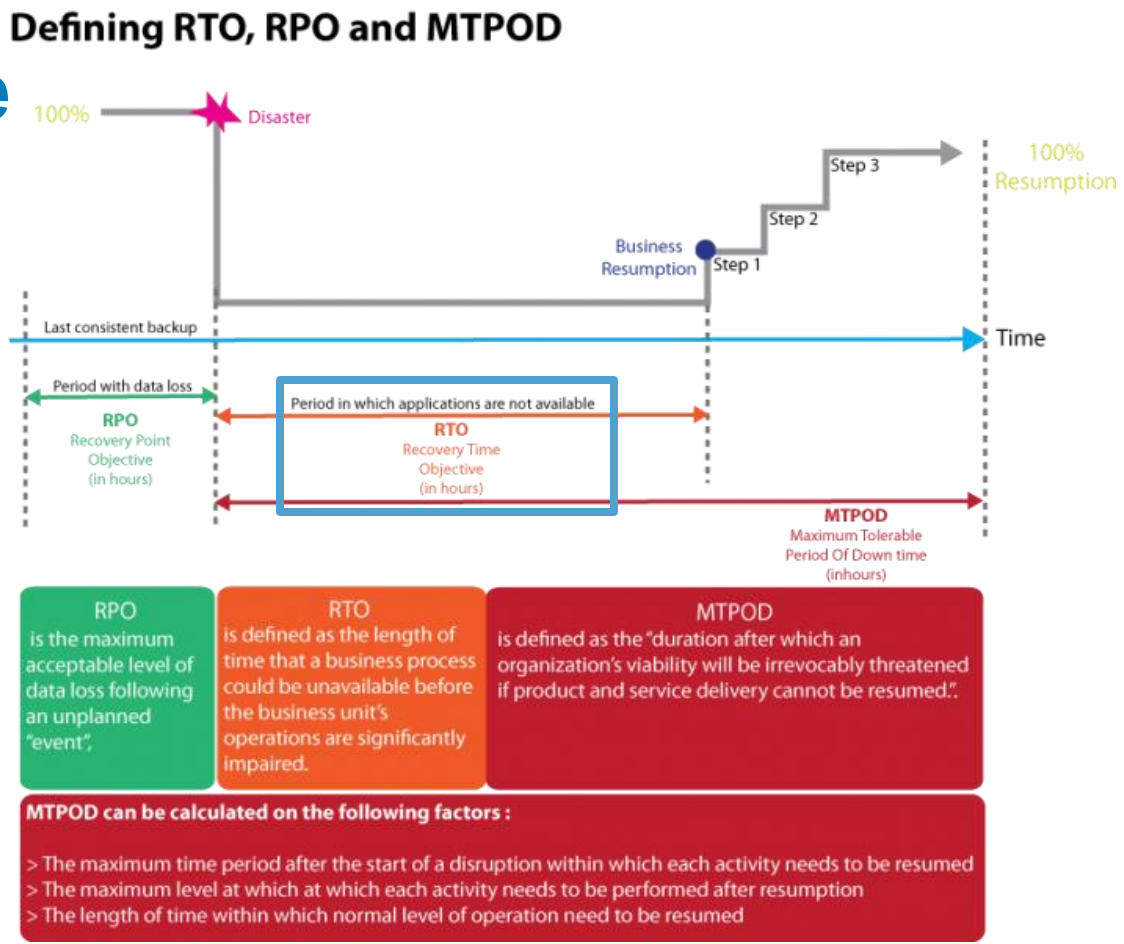
- Assess mission/business process and recovery criticality
- Identify resource requirements
- Identify recovery priorities

Template: https://csrc.nist.gov/files/pubs/sp/800/34/r1/upd1/final/docs/sp800-34-rev1_bia_template.docx

See also “Security and resilience — Business continuity management systems — Guidelines for business impact analysis”, ISO/TS 22317:2021, for more information

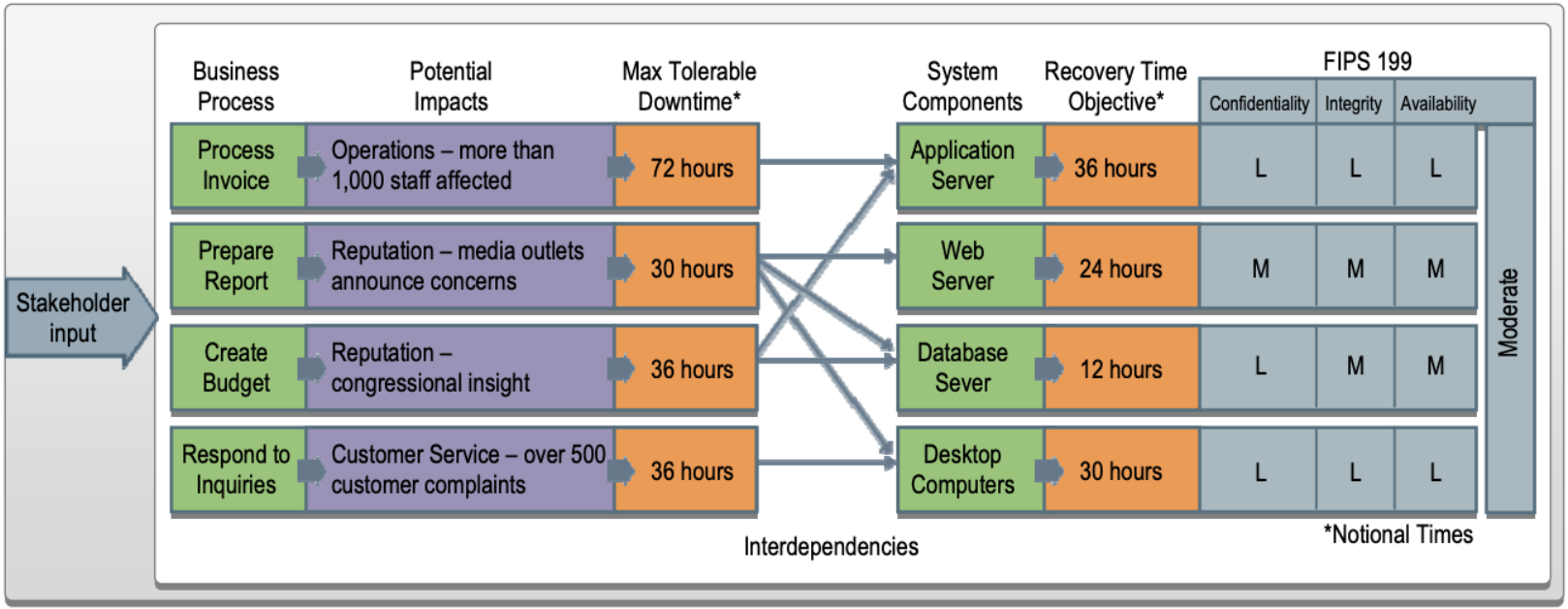
BIA: prioritize

Use time criticality of functions / processes to guide the prioritization



Source: https://www.bcmpedia.org/w/index.php?title=File:Recovery_Objectives_RTO_RPO_and_MTPD.png

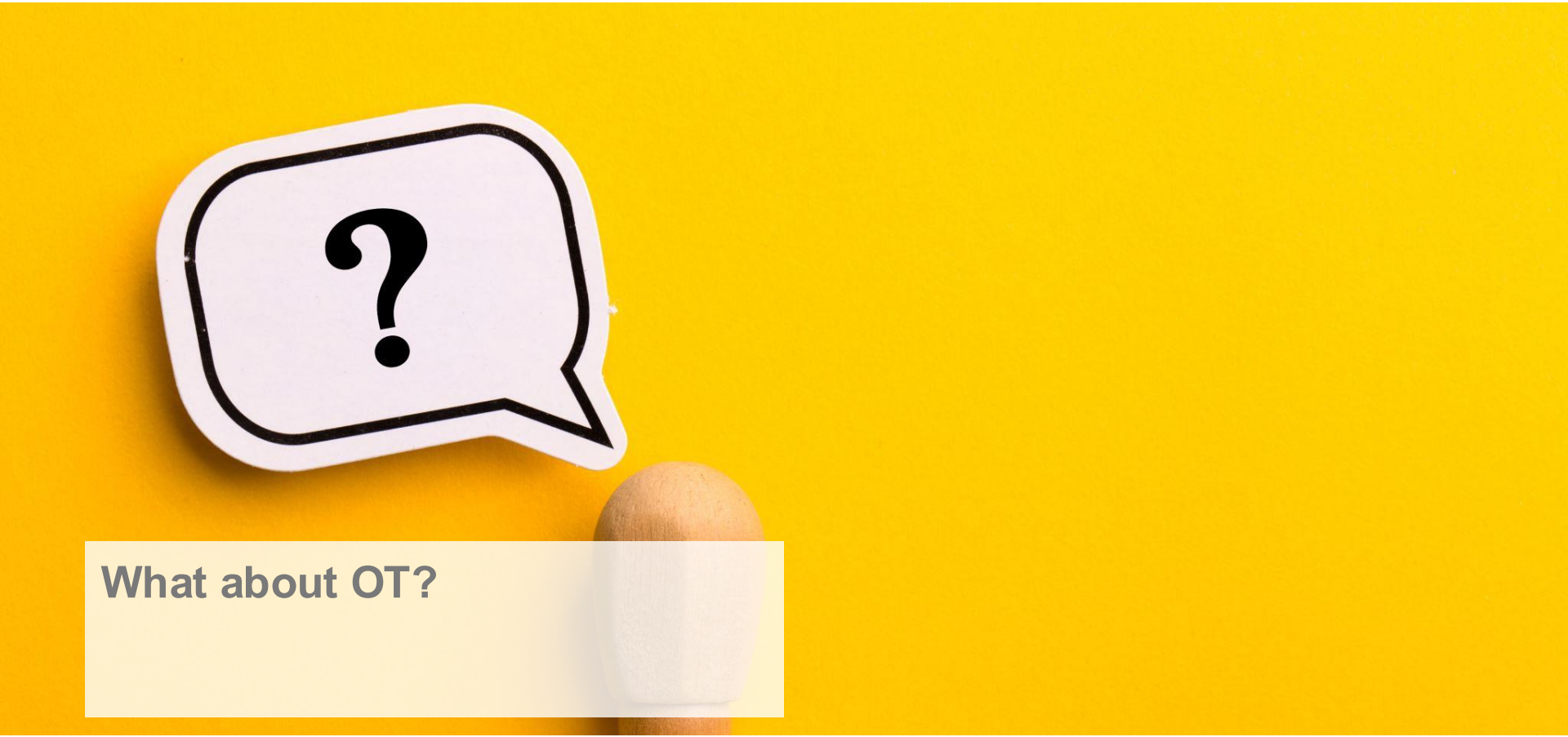
Identify resource requirements



Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Inputs to BIA Data Collection

- (Online) questionnaires
- Facilitated data-gathering sessions
- Process flows and interdependency studies
- Risk assessment(s)
- IT and OT applications & logs
- Financial reports
- Audit reports



What about OT?

BIA in OT

It fails when there is a :

- Lack of cross-functional input
  If a BIA is created without engineering, operations and OT maintenance it is doomed to fail
- Failure to capture indirect dependencies
  One may list PLC or SCADA systems but not the related dependencies
- Lack of understanding that the same time-based assumptions may not apply to OT
  In IT, Recovery Time Objectives (RTOs) of multiple hours may be acceptable. In OT, 5 minutes of downtime may have a significant impact already (the infamous "99.999%")

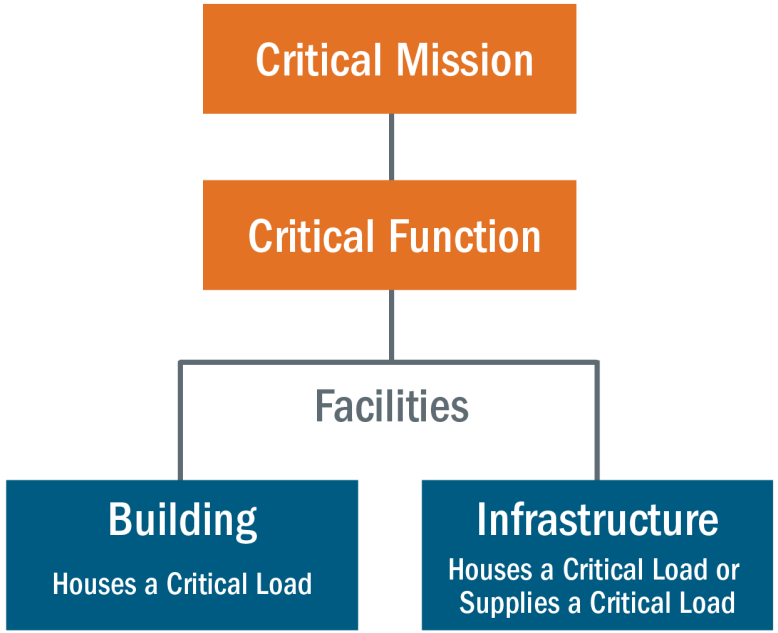
A modern BIA for Operational Technology needs to:

- Identify critical processes / functions, not just systems
- Map technical dependencies and operational tolerances
- Quantify cross-site impacts for multi-site operations
- Incorporate recovery thresholds informed by real scenarios, not just SLAs

Identifying Critical Business Functions

"Mission of such high importance that its incapacitation or destruction would have a severely degrading effect on the ability to execute the tasks or mission-essential tasks it supports in all operating environments."

Technical Resilience Navigator, U.S. Department of Energy Federal Energy Management Program, https://trn.pnnl.gov/



Examples of Critical Functions (Facility Operations)	Description
Provide proper ventilation	Ensuring that appropriate ventilation in a facility is installed and operational can protect personnel from hazardous conditions.
Provide and maintain utilities connections (DoD 2008)	Providing and maintaining utilities connections can assist in sustaining baseline site activities and protect the safety of onsite staff.
Provide and maintain electrical infrastructure	Maintaining electrical infrastructure can assist in sustaining baseline site activities, continuing research, and promoting workplace safety.
Maintain manufacturing operations	Maintaining manufacturing operations can support site activities related to the production of materials or commodities.
Upkeep training facilities	Upkeeping training facilities, such as in the military, can assist in sustaining baseline activities by preparing and educating new personnel for site operations.
Manage supplies (DoD 2008)	Managing supplies, for example by procuring and maintain contracts, controlling inventory, providing, and storing shipment information, processing order receipts, and reporting order and inventory status, can assist in sustaining baseline activities (DoD 2008).
Provide and maintain property	Providing and maintaining site property, such as buildings and other infrastructure, can assist in sustaining baseline site activities.
Provide and maintain utilities connections for related remote sites	Providing and maintaining utilities connections for remote sites, such as sites within a national park, can assist in sustaining baseline activities.

Source: https://trn.pnnl.gov/resource/TRN%20Critical%20Functions.docx

Examples of Critical Functions (Public Health & Healthcare Functions)	Description
Carry out analyses in drinking water lab facilities (US EPA)	Analyzing drinking water to identify toxins and pathogens in local supplies can help to ensure safety and protect health.
Carry out analytical lab testing of food products (US DHS)	Performing analytical lab testing of food products can help to ensure food safety and protect health.
Manage and treat wastewater (US CISA)	Managing and treating wastewater can support the maintenance and management of infrastructure and the protection of health.
Maintain emergency medical services (Washington Military Department Emergency Management Division 2019)	Maintaining emergency medical services can minimize injuries, reduce health consequences, and minimize the impact of disasters and emergencies on the public.
Preserve lab samples (Dynes et al. 2009)	Preserving medical lab samples, such as keeping samples that require refrigeration at appropriate temperatures and restricting access to potentially harmful samples, can support patient safety and the continuation of care, treatment, and other services.
Order medications and view patient medication profiles (Dynes et al. 2009)	Ordering medication and viewing medication profiles can support patient safety and the continuation of care, treatment, and other medical services.
Preserve patient records (Institute for Crisis, Disaster, and Risk Management 2010)	Preserving medical records can support patient safety and the continuation of care, treatment, and other medical services.
Provide inpatient care (University of North Carolina at Chapel Hill)	Providing inpatient care can support patient safety and the continuation of care, treatment, and other medical services.
Maintain access to medical supplies (DoD 2008)	Providing inpatient care can support patient safety and the continuation of care, treatment, and other medical services.
Provide and maintain utilities connections (DoD 2008)	Providing and maintaining utilities connections can assist in sustaining baseline site activities, such as providing life support in a hospital, and protect the safety of staff and patients.

Source: https://trn.pnnl.gov/resource/TRN%20Critical%20Functions.docx

Examples of Critical Functions (Safety & Security Functions)	Description
Conduct hazardous waste material response (University of Memphis)	Providing hazardous waste material response services, like properly disposing of radioactive waste, toxic substances, and potentially explosive materials, can support good environmental health and can ensure public safety.
Protect sensitive information (US CISA)	Protecting sensitive information, such as through cybersecurity measures and need-to-know communication, can assist in maintaining baseline activities and reducing threats and vulnerabilities.
Analyze and provide intelligence (TRN 2022)	Analyzing and providing intelligence, such as by collecting and evaluating data, can help provide necessary information to make decisions, maintain current operations, and protect the safety and privacy of clients or the public.
Transport information (DoD 2008)	Transporting information can assist in maintaining baseline activities and reducing threats and vulnerabilities.
Maintain security across site (US DHS)	Maintaining security across a site, such as by ensuring lights remain on, locked doors do not open automatically, sensitive areas have reduced access, and alarms function appropriately can help to protect site staff, employees, and the public.
Provide and communicate meteorological forecasts (US DHS)	Providing and communicating meteorological forecasts, such as alerting populations of hazardous weather, can assist in protecting the public from harm and assist in informing the population on how to best protect infrastructure from potential damage.
Provide and maintain utilities connections (DoD 2008)	Providing and maintaining utilities connections can assist in sustaining baseline site activities and protect the safety of onsite staff.

Source: https://trn.pnnl.gov/resource/TRN%20Critical%20Functions.docx

Business Impact Analysis

Colour coding the priority helps to see the most critical business activities at a glance.

The recovery approach outlines the high-level mitigation strategies to restore business function.

ID	Business Activity	Activity Owner	Category	Area of Impact	RTO	MTD	Priority	Recovery Approach	Resources needed	References
1	Provision of clinical care and support services	Head Clinical Services	Services	Quality and standards of care Health	4 hrs	2 days	High	Deploy back up resources Utilise medical clinics and hospital services	Agency staff Medical services	Clinical manual ref 20/5477 Agency list ref 22/5436
2	Provision of meals	Head Operations	Services	Quality and standards of care Health	2 hrs	1 day	High	Utilise alternative caterers	Catering suppliers	Catering list ref 19/334
3	Provision of email and phone services	Head IT	Systems	Communication and administration	6 hrs	1 day	High	Use of mobile phones Technical expertise	IT advisors Comms team	ICT disaster recovery plan ref 22/399
4	Front reception and office administration	Head Corporate	Services / Administration	Communication and administration	1 day	2 days	Medium	Redeploy resources Agency staff	Agency staff Facilities team	Concierge manual ref 20/453

Having a unique ID helps to track activities.

Description of business activity or function that could be disrupted.

Categorising activities helps to understand nature of impact to business.

Defining area of impact helps to understand the relevant risks.

It is important to identify the resources that might be needed to support the recovery.

It is useful to include references to key documents that have the detailed information needed to support the recovery approach.

Including the role responsible for the business activity helps to understand who should lead recovery action.

Recovery Time Objective (RTO) or the 'cry point' is the amount of real time a business has to restore its processes to an acceptable service level after an event to avoid intolerable consequences associated with the disruption.

Maximum Tolerable Downtime(MTD) or the 'die point' is the maximum amount of time a business function can be discontinued without causing irreparable harm to the business. Sometimes referred to as Maximum Allowable Outage or Maximum Acceptable Outage.

Source: https://www.agedcarequality.gov.au/sites/default/files/media/topic-resource-4-business-impact-analysis.pdf

Type of Service/Operation	Core Activity Description	Dependent Services/Activities	*Maximum Tolerable Period of Disruption* (MTPD)	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Priority Ranking
Step 1	**Step 2**	**Step 3**	**Step 4**	**Step 5**	**Step 6**	**Step 7**
<Corporate / Clinical / Support Service>	*<Brief description of activities/ processes>*	*<List of services/activities that rely on the successful delivery of this area>*	*<Specification of the Maximum Tolerable Period of Disruption for Core Activity – Step 2>*	*<How long it should take to restore the service /operation>*	*<How far back ICT data is needed to effectively perform the services after an event>*	*<Ranking of activity based on figure 9)*
Radiology Department	X-ray Imaging	Emergency Services Orthopaedics Gastroenterology Cardiology	16 hours	Within 1 day	<1 hour	1
	CT Scan	Emergency Services Neurology Oncology Diagnostic Imaging	16 hours	Within 1 day	<1 hour	1
	MRI	Neurology Orthopaedics Oncology	72 hours	Within 1 day	<1 hour	2
	DXA Scan	Orthopaedics Endocrinology Rheumatology	72 hours	Within 1 day	<1 hour	2
	Radiation Therapy Planning	Neurology Oncology	72 hours	Within 1 day	<1 hour	2
	Radiation Safety and Dosimetry	All radiology services	6 hours	Within 1 day	<1 hour	1
	Weekly team meetings	All radiology services	7 days	Within 3 days	<1 day	3

Source: HSE Business Continuity Management Handbook (Irish Health Service) https://www.hse.ie/eng/services/list/3/emergencymanangement/business-continuity-management/hse-business-continuity-management-handbook.pdf

Source www.alamy.com (image id W7HDDN)

Incident

An adverse event beginning to attack the organization against cybersecurity assets, with has a realistic chance of success to threaten confidentiality, integrity or availability of information assets or other resources.

This Photo by Unknown Author is licensed under CC BY-SA

Possible, Probable or Definite?

Incident response teams

As a result of the contingency planning process, the organization will create

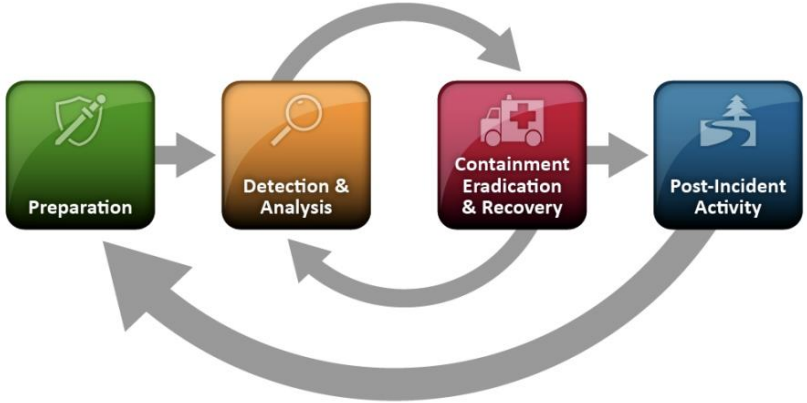
- Incident response planning team (IRPT)
- Security incident response team (CSIRT)

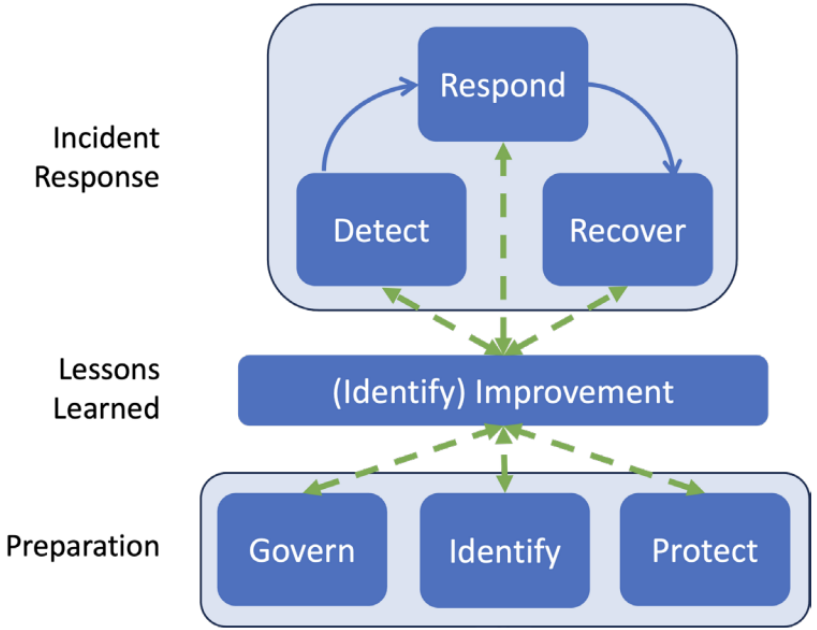
NIST Cybersecurity Framework[1]

- **Identify**
  Develop an understanding to manage cybersecurity risks
- **Protect**
  Develop and implement appropriate safeguards to guarantee delivery of services
- **Detect**
  Develop and implement activities to identify the occurrence of a cybersecurity event
- **Respond**
  Develop and implement the appropriate activities to take action regarding a detected event
- **Recover**
  Develop and implement the appropriate plans for maintain resilience and restore any capability or service disrupted by a cybersecurity event

1: https://www.nist.gov/cyberframework

NIST Incident Response Lifecycle



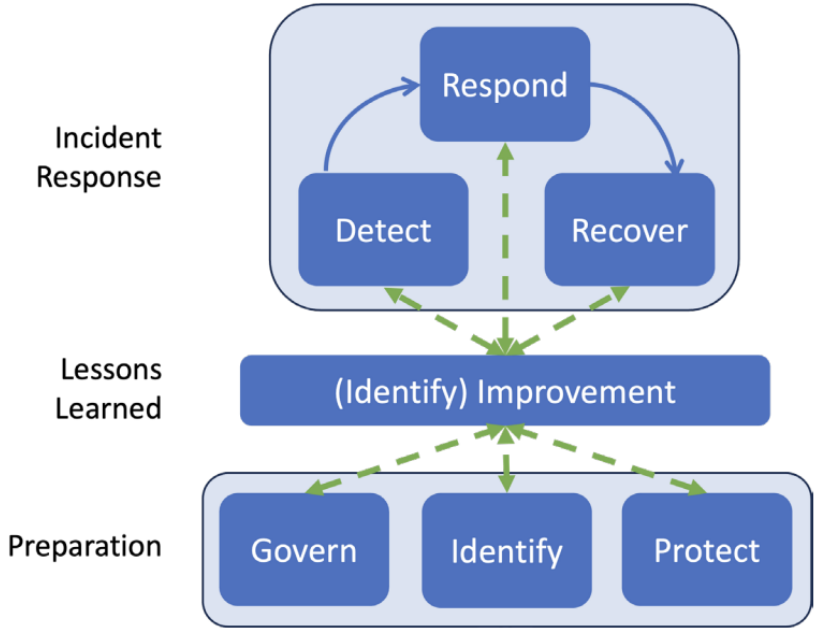


Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST Special Publication (SP) NIST SP 800-61r**2**

Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST Special Publication (SP) NIST SP 800-61r**3**

NIST Incident Response Lifecycle

- **Govern (GV)**: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated and monitored
- **Identify (ID)**: The organization's current cybersecurity risks are understood
- **Protect (PR)**: Safeguards to manage the organization's cybersecurity risks are used
- **Detect (DE)**: Possible cybersecurity attacks and compromises are found and analyzed
- **Respond (RS)**: Actions regarding a detected cybersecurity incident are taken
- **Recover (RC)**: Assets and operations affected by a cybersecurity incident are restored



Source: Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST Special Publication (SP) NIST SP 800-61r3

Incident Response Policy

It should contain :

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of cybersecurity incidents and related terms
- Organizational structure and definition of roles, responsibilities and levels of authority
- Requirement for reporting certain types of incidents
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms

Incident Response Planning and IRPT

- Led by CISO or other Cybersecurity Manager
- Heavy Cybersecurity, IT and OT presence
- Plus non-technical members

Incident Response Plan Elements

- Mission
- Strategies and goals
- Senior management approval
- Approach to incident response
- Communication strategies
- Metrics for measuring IR
- Roadmap for maturing IR

This Photo by Unknown Author is licensed under CC BY

Incident Response Plan Procedures

C: Computer or Cyber in CERT/CSIRT

- A set of actions to be taking during the incident
- A set of actions to be taken after the incident is contained
- A set of actions to be taken before the incident occurs

Basis	CERT (Computer Emergency Response Team)	CSIRT (Computer Security Incident Response Team)
Primary Focus	Proactive measures to prevent incidents and enhance security	Reactive response to security incidents within an organization
Scope	Works on a national or organizational level	Typically focused on specific organizations or sectors
Approach	Emphasizes prevention and preparedness	Focuses on immediate response and remediation
Skill Development	Offers training and resources for cybersecurity personnel	Provides tailored support and training for specific organizational needs
Community Building	Fosters communities of practice for knowledge sharing	Builds internal capabilities to enhance organizational security awareness

Source: https://www.infosectrain.com/

Incident Response Plan

Incident Response Plan Example

This document discusses the steps taken during an incident response plan. To create the plan, the steps in the following example should be replaced with contact information and specific courses of action for your organization.

1) The person who discovers the incident will call the grounds dispatch office. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:
    a) Helpdesk
    b) Intrusion detection monitoring personnel
    c) A system administrator
    d) A firewall administrator

Source: https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc

CSIRT

Computer/Cyber Security Incident Response Team

This Photo by Unknown Author is licensed under CC BY-SA-NC

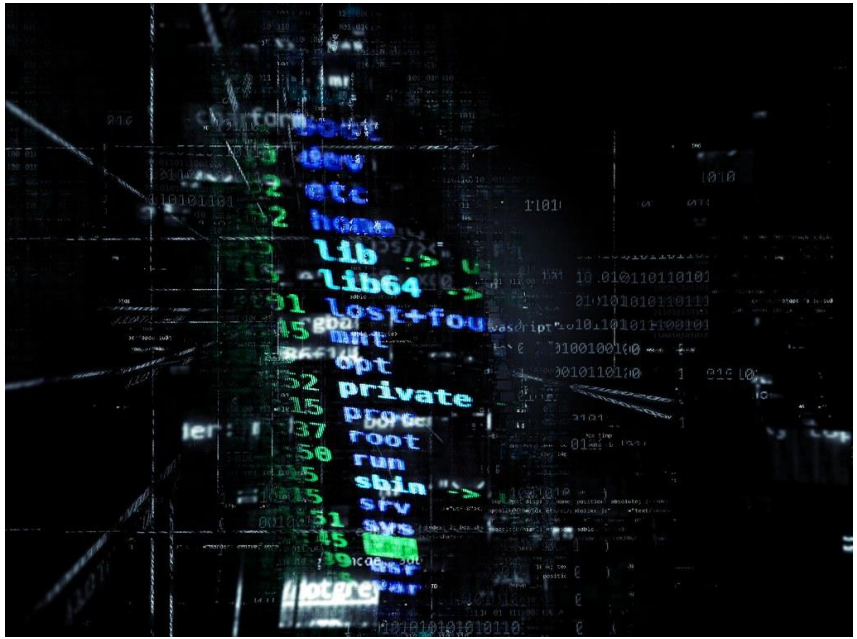
CSIRT Liaison

- Liaison between the organisation and CSIRT
- Allows anyone to report a suspicious activity

This Photo by Unknown Author is licensed under CC BY-SA

Incident Response Actions

- Detection of an incident that is underway and notification of the CSIRT
- Reaction of the CSIRT to the incident, activating the IR plan, and selecting an appropriate response strategy
- Recovery phase, where CSIRT works with the rest of the company to restore normal operations



This Photo by Unknown Author is licensed under CC BY-SA-NC

NIST Handling Checklist (I)

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	

NIST Handling Checklist (II)

Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	

NIST Handling Checklist (III)

Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Note: even though these activities are now part of CSF 2.0 and executed “continuously”, they are interesting from an educational standpoint – thus their presence here

Source of the tables (point 1.-9.): Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST Special Publication (SP) NIST SP 800-61r2

Going beyond

NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

NIST National Institute of Standards and Technology • U.S. Department of Commerce

NIST Special Publication 800
NIST SP 800-61r3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

A CSF 2.0 Community Profile

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya*
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

**Former NIST employee; all work for this publication was done while at NIST.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-61r3

April 2025

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

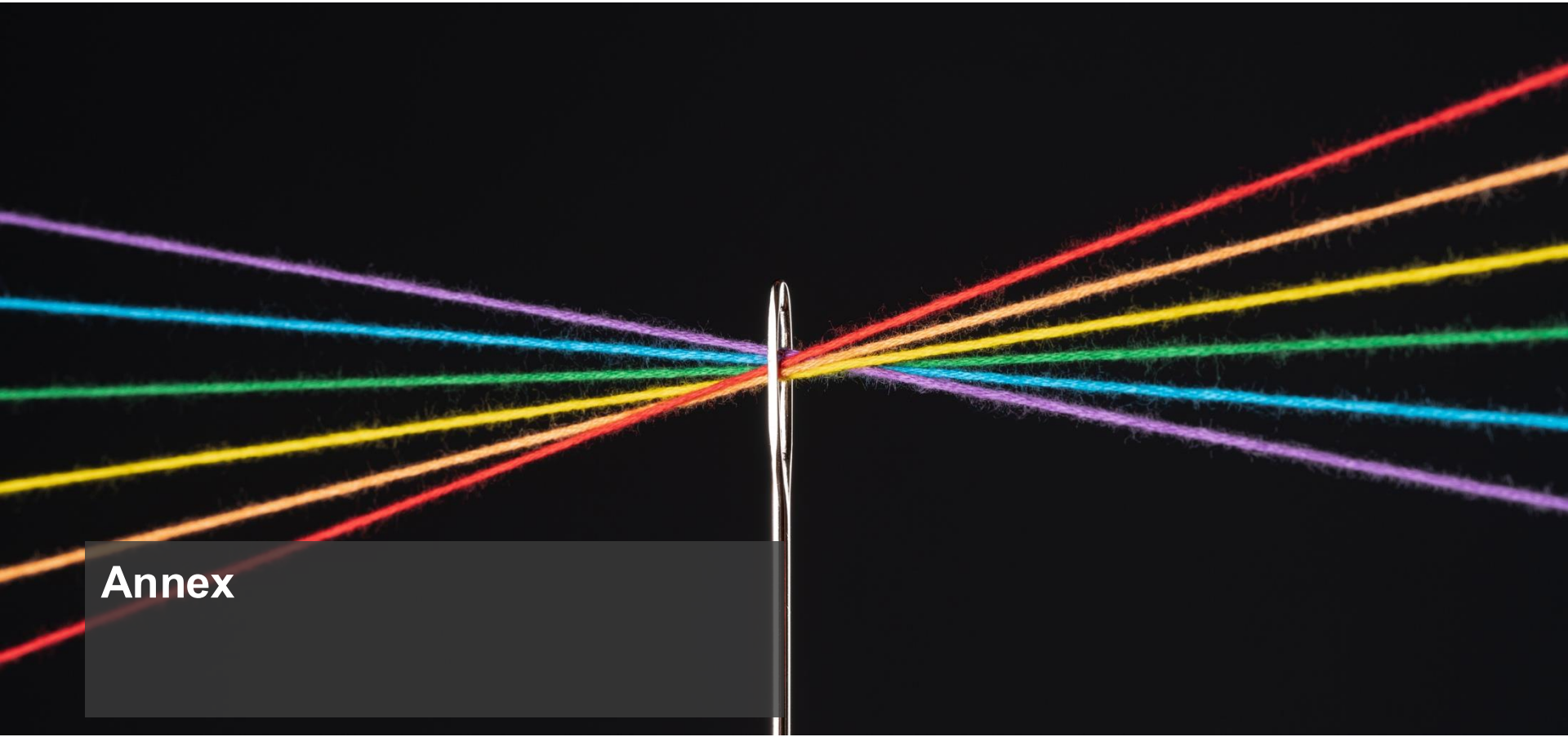
Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Victoria Pillitteri
Suzanne Lightman
Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

References

- Contingency Planning Guide for Federal Information Systems, NIST Special Publication 800-34 Rev. 1
- Computer Security Incident Handling Guide, Special Publication 800-61 Rev. 3
- Computer Security Incident Handling Guide, Special Publication 800-61 Rev. 2 (withdrawn)
- Guide to Operational Technology (OT) Security
- IoT Device Cybersecurity Guidance for the Federal Government, Special Publication 800-213A
- Technical Resilience Navigator, Site Planning, U.S. Department of Energy
- Security and resilience — Business continuity management systems — Guidelines for business impact analysis, ISO/TS 22317:2021



Annex

NIST Cybersecurity Framework[1]

- **Identify**
  Develop an understanding to manage cybersecurity risks
- **Protect**
  Develop and implement appropriate safeguards to guarantee delivery of services
- **Detect**
  Develop and implement activities to identify the occurrence of a cybersecurity event
- **Respond**
  Develop and implement the appropriate activities to take action regarding a detected event
- **Recover**
  Develop and implement the appropriate plans for maintain resilience and restore any capability or service disrupted by a cybersecurity event

1: https://www.nist.gov/cyberframework

Identify

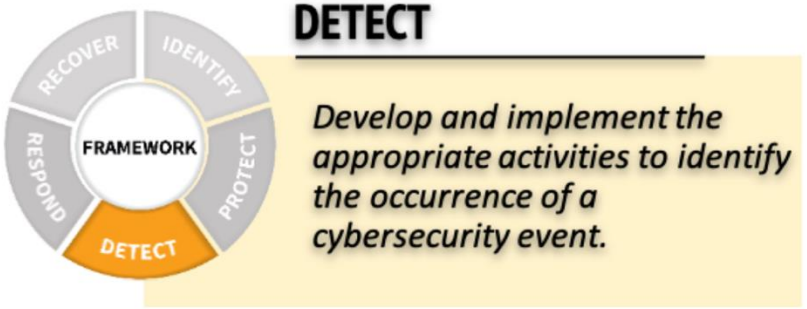
- Identify critical enterprise processes and assets
- Document information flows
- Maintain hardware and software inventory
- Establish policies for cybersecurity that include roles and responsibilities
- Identify threats, vulnerabilities, and risk to assets

Protect

- Manage access to assets and information
- Protect sensitive data
- Conduct regular backups
- Securely protect your devices
- Manage device vulnerabilities
- Train users

Detect

- Test and update detection processes
- Maintain and monitor logs
- Know the expected data flows for your enterprise
- Understand the impact of cybersecurity events



Respond

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

Recover

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