CSE5ISM CYBERSECURITY INCIDENT MANAGEMENT Week 4-5

Dr Kayes

March 2025

Revision

Week 3

- Understand different cyber threat vectors (attack methods)
- Understand the purpose of different attack models
  - The cyber kill chain
  - Unified kill chain
  - The MITRE ATT&CK framework

Week 4-5: Lecture Outline

Business Measures, Business Continuity & Operational Resilience

- Analysis of vulnerabilities in business processes
- Severity hierarchy for information security incidents
- Classification and categorization of incidents
- Overview of the ISO 22301 Business Continuity Planning/Management
- Understand the elements required in a business continuity plan
- Overview of the ISO 22316:2017 Security and resilience -- Organizational resilience -- Principles and attributes
- Introduction to the ICOR's Organizational Resilience Framework

After any cyber threat/incident

- **Problem**
  - Expose MHR data to unauthorised parties due to lack of control/error/intentional/unintentional
  - Malware/Ransomware attacks
  - Injection attack on MHR system
- **Risk**
  - Lose users' trust on MHR system
  - Compromise credentials/corrupt health data
  - Spread viruses from one channel/node to others
- **Result**
  - MHR system down
  - Make Medicare claims and take money
  - The BCP/DRP can save a lot of money and time/efforts

After any cyber threat/incident

- **Business Continuity Plan (BCP)**
  - Goal: is to ensure the continuity of business processes during an emergency/disaster
  - Objective: is to return business back to initial state
  - Focus: Return to normal
- **Disaster Recovery Plan (DRP)**
  - DRP is a part of business continuity
  - Goal: is to restore critical business processes (data/resources, systems, and business operations)
  - Objective: is to restore critical business processes on a temporary location
  - Focus: Data recovery

More about BCP/DRP

- Identify the business processes/functions/data/infrastructure/applications (align with **IRP** critical data and infrastructure) and categorize them critical versus non-critical
- Define the necessary steps to restore them (the critical things to operate the business)
- Quantify the cost of business continuity
- Calculate the maximum time the organization can tolerate, such as down time
- Allow recovery team to administer recovery efforts that result in a timely restoration, until the operations restored to normal state
- Business case: people, process and technology
- Plan and implement
- Test, test and test
- Review and update the BCP when the business process changes

More about BCP/DRP

- Conduct a business impact analysis (BIA) against risks (cost/time to relocate, …)
- Identify incidents related to human errors, technical and/or natural disaster (incident classification)
- Assess the severity of incidents and categorize them based on severity
- Apply consistency in categorising incidents and severity
- Facilitate information sharing and consistency across different stakeholders

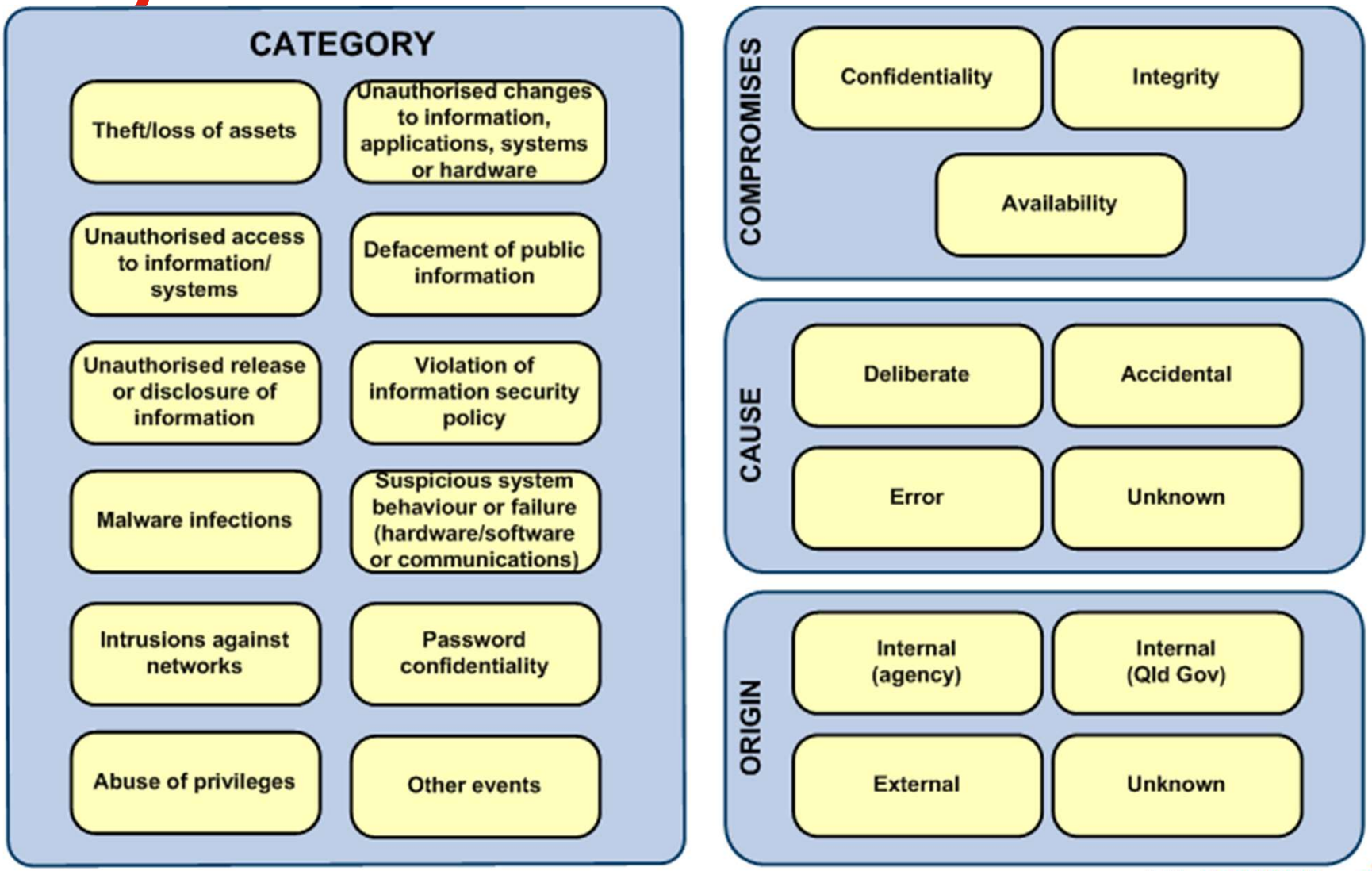
Incident Response Plan (IRP)

- When a cyber security incident occurs, a plan is in place to respond appropriately to the situation.
- **Aim:** to prevent the cyber security incident from escalating, restore any impacted information or services, and preserve any evidence.

Business Continuity Plan (BCP)

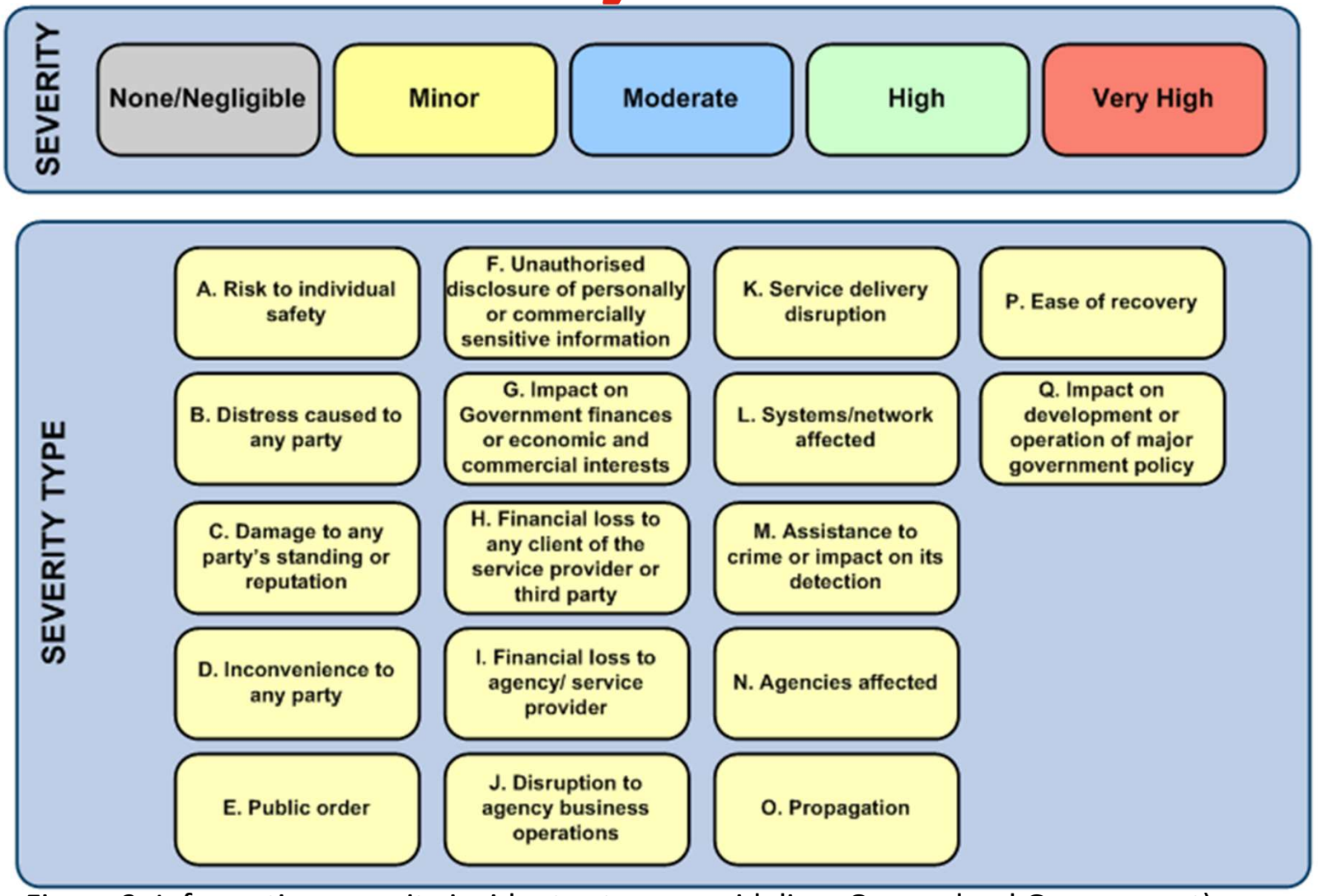
- A contingency plan to restore critical functions for continued business operations.
- **Aim:** is to keep the business operating, potentially in a degraded mode, if an incident causes a partial or total outage of information systems.
- A **Business Continuity Plan (BCP)** is usually **different** from a **Disaster Recovery Plan (DRP)**. BCP and DRP plans have **inter-dependencies**
- A DRP plan typically involves **switching the business over to alternative processing facilities**, spare data centres, etc, and **plans for switching back**
- The BCP is to **keep the business running** whilst the DRP is the recovery plan while there is any disaster

Security Incident Classification



(Source: Figure 2, Information security incident category guideline, Queensland Government)

Security Incident Severity Classification



(Source: Figure 2, Information security incident category guideline, Queensland Government)

(Source: Information security incident category guideline, Queensland Government)

Case Study 1 – A staff member has incorrectly sent an email with sensitive agency information to another staff member. After investigation, it was determined by the agency that the recipient had no prior involvement in the leaking of this information i.e., did not instigate the email, and was not in breach of any agency information security policy. The sender confirmed that the incident was a result of an error.

- **Incident:** The confidentiality of agency information has been compromised
- **Incident Category:** Unauthorised disclosure of agency information
- **Incident Impact/Compromise:** Confidentiality (the staff member released sensitive agency information to another staff)
- **Cause:** Accidental (confirmed that it was not intentional and no prior involvements)
- **Origin:** Internal (occurred between two staff members)
- **Severity Type:** impacted measurably as the sender of the email has disclosed sensitive information without authorisation
- **Severity Metric(s):** moderate

Classification by Severity (severity metrics)

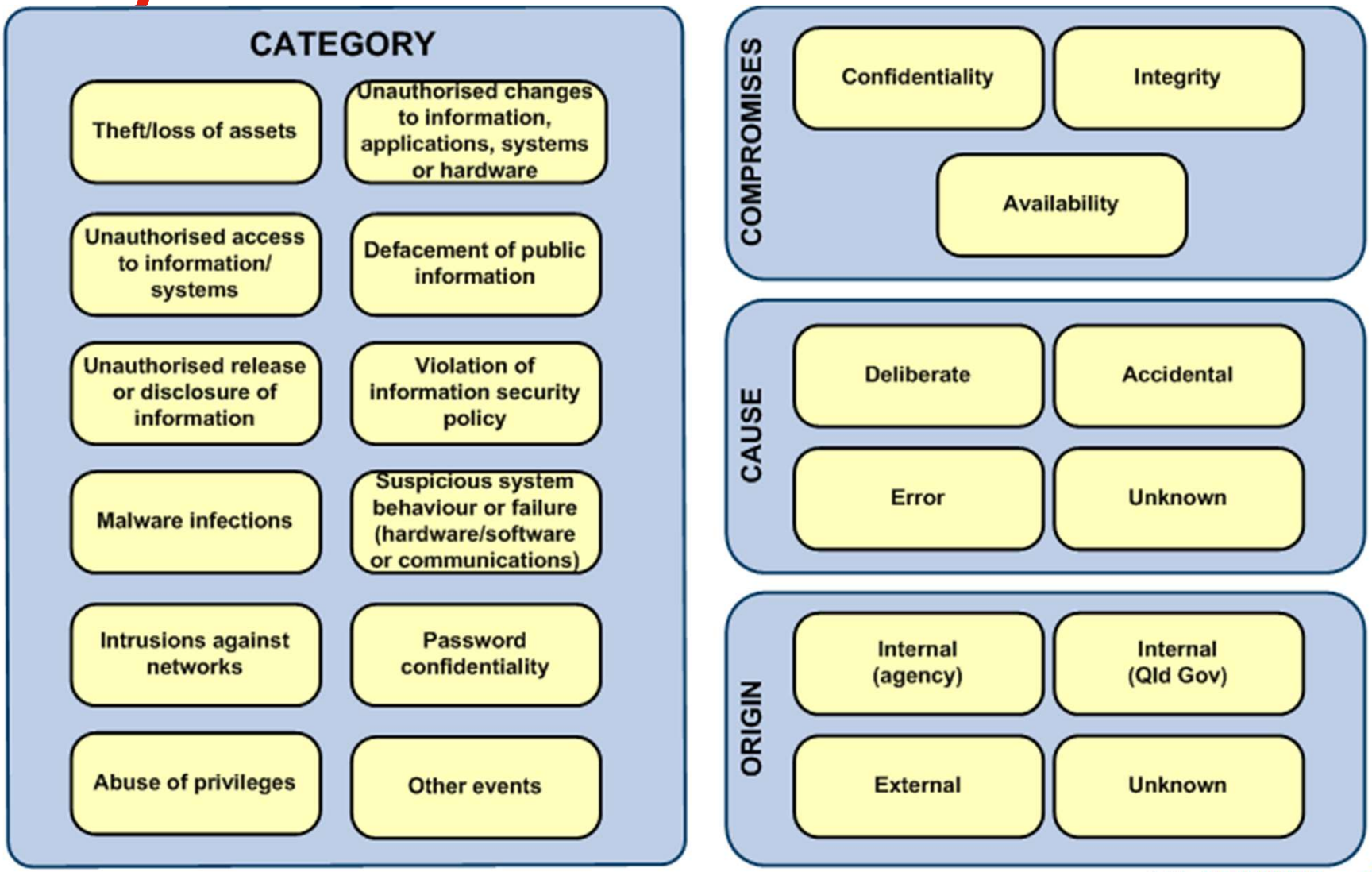
- Focus on impact (i.e., CIA compromise) of various components, such as; financial loss, loss of goodwill, loss of customers, etc.
- If an incident as assessed has scores in a range from 'none/negligible' to 'high', then the highest severity rating identified that should be applied to the incident.
- **S: Severe** (i.e., very high): the incident may threaten business continuity if it occurs.
  - Consequences: business processes are disturbed for a prolonged period of time,
- **H: High**: a high impact on the business.
  - Consequences: business processes are disturbed for some time,
- **M: Moderate**: the incident may have a some impact on the business.
  - Consequences: some financial loss and there is perhaps some loss of
- **L: Low/Minor**: low impact on the business.
  - Consequences: Losses are probably limited to costs made
- **N: None/Negligible**: No impact at all.

Examples - Severity Type

- **Risk to individual safety**: Possible Consideration to measure severity (Consider any risk of injury or impact on safety at all, as well as the possibility of loss of life. An example could include release of names or locations of under-cover officers, people under protection orders.) – high (any risk to personal safety) – very high (threaten life directly)
- **Damage to any party's standing or reputation:** Issues to consider include potential for adverse publicity, either locally or wider, and the potential to damage occurring to either the service provider's or client's ongoing reputation. If inappropriate access to information was granted, would it be of interest to the media? – moderate (moderate embarrassment) - high (significant embarrassment) – very high (severe embarrassment)
- **Systems affected:** How many systems have been affected by the incident? Are these critical systems? – None – few non-critical – many non-critical – any critical – many critical
- **Unauthorised disclosure of personally or commercially sensitive information:** Examples include medical records and other personal information and commercially sensitive information that could impact on current or future business. – no disclosure – minor – measurable – significant – substantial impact to person/business/agency

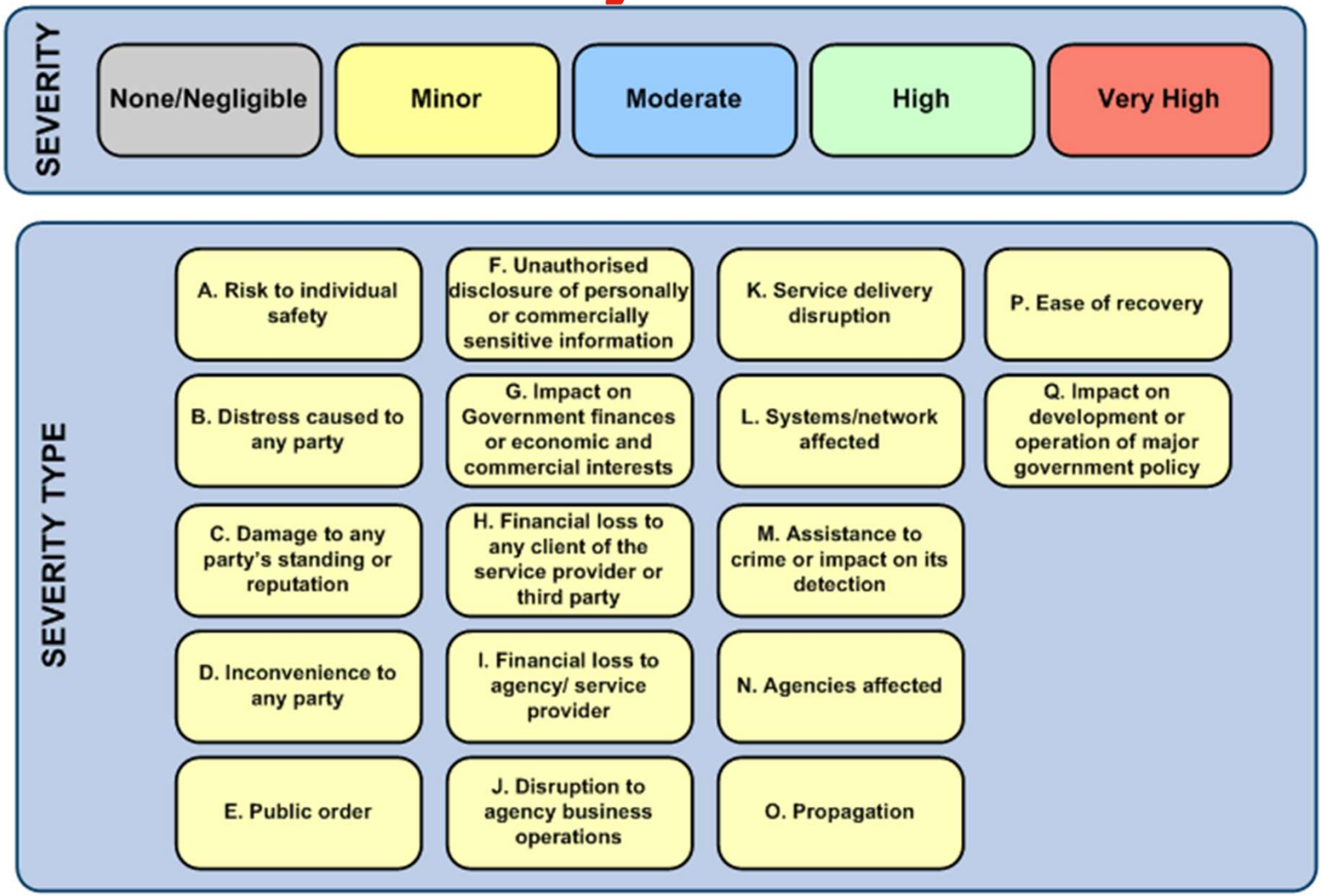
Case Study

Security Incident Classification



(Source: Figure 2, Information security incident category guideline, Queensland Government)

Security Incident Severity Classification



(Source: Figure 2, Information security incident category guideline, Queensland Government)

(Source: Information security incident category guideline, Queensland Government)

Case Study 1 (…) – A staff member has incorrectly sent an email with sensitive agency information to another staff member. After investigation, it was determined by the agency that the recipient had no prior involvement in the leaking of this information i.e., did not instigate the email, and was not in breach of any agency information security policy. The sender confirmed that the incident was a result of an error.

- **Incident:** The confidentiality of agency information has been compromised
- **Incident Category:** Unauthorised disclosure of agency information
- **Incident Impact/Compromise:** Confidentiality (the staff member released sensitive agency information to another staff)
- **Cause:** Accidental (confirmed that it was not intentional and no prior involvements)
- **Origin:** Internal (occurred between two staff members)
- **Severity Type:** impacted measurably as the sender of the email has disclosed sensitive information without authorisation
- **Severity Metric(s):** moderate

Case Study 2 – An agency has detected a network intrusion from an external source. This particular attempt was successful in adversely affecting the security of agency information, as the agency's security controls were not able to prevent the intrusion from occurring. As a result of the attack, the agency's website was defaced, with the attacker's removing the existing content, and replacing it with offensive material. The incident is under investigation to identify where the attack has come from.

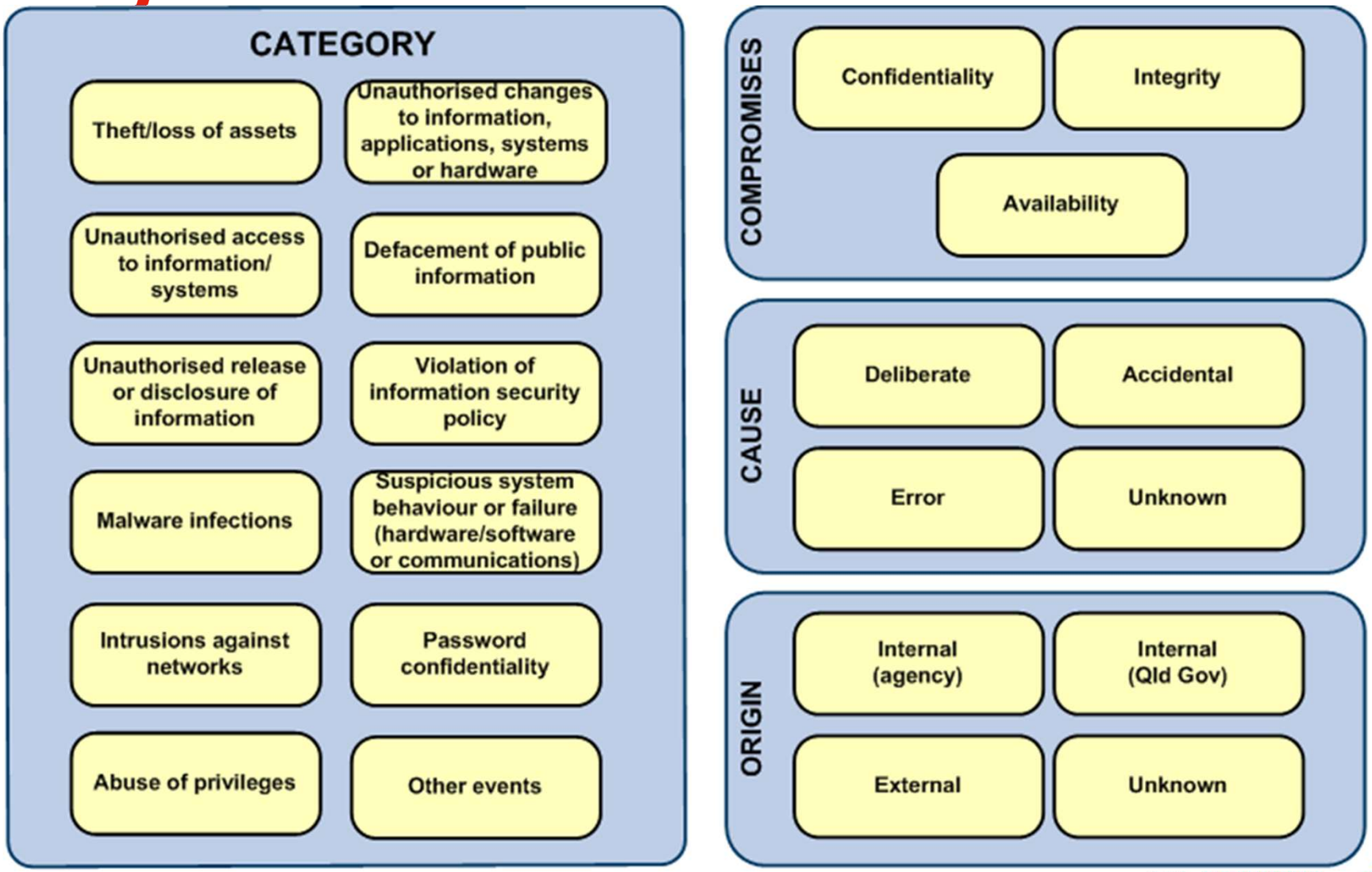
(Source: Information security incident category guideline, Queensland Government)

Case Study 2 – An agency has detected a network intrusion from an external source. This particular attempt was successful in adversely affecting the security of agency information, as the agency's security controls were not able to prevent the intrusion from occurring. As a result of the attack, the agency's website was defaced, with the attacker's removing the existing content, and replacing it with offensive material. The incident is under investigation to identify where the attack has come from.

- **Incident Classification:** This occurrence has been classified as two separate incidents, as both incidents that have arisen as a result require different responses:
- (1) the network intrusion requires action to increase the security controls; and
- (2) the website defacement requires the agency to restore their website and its content.

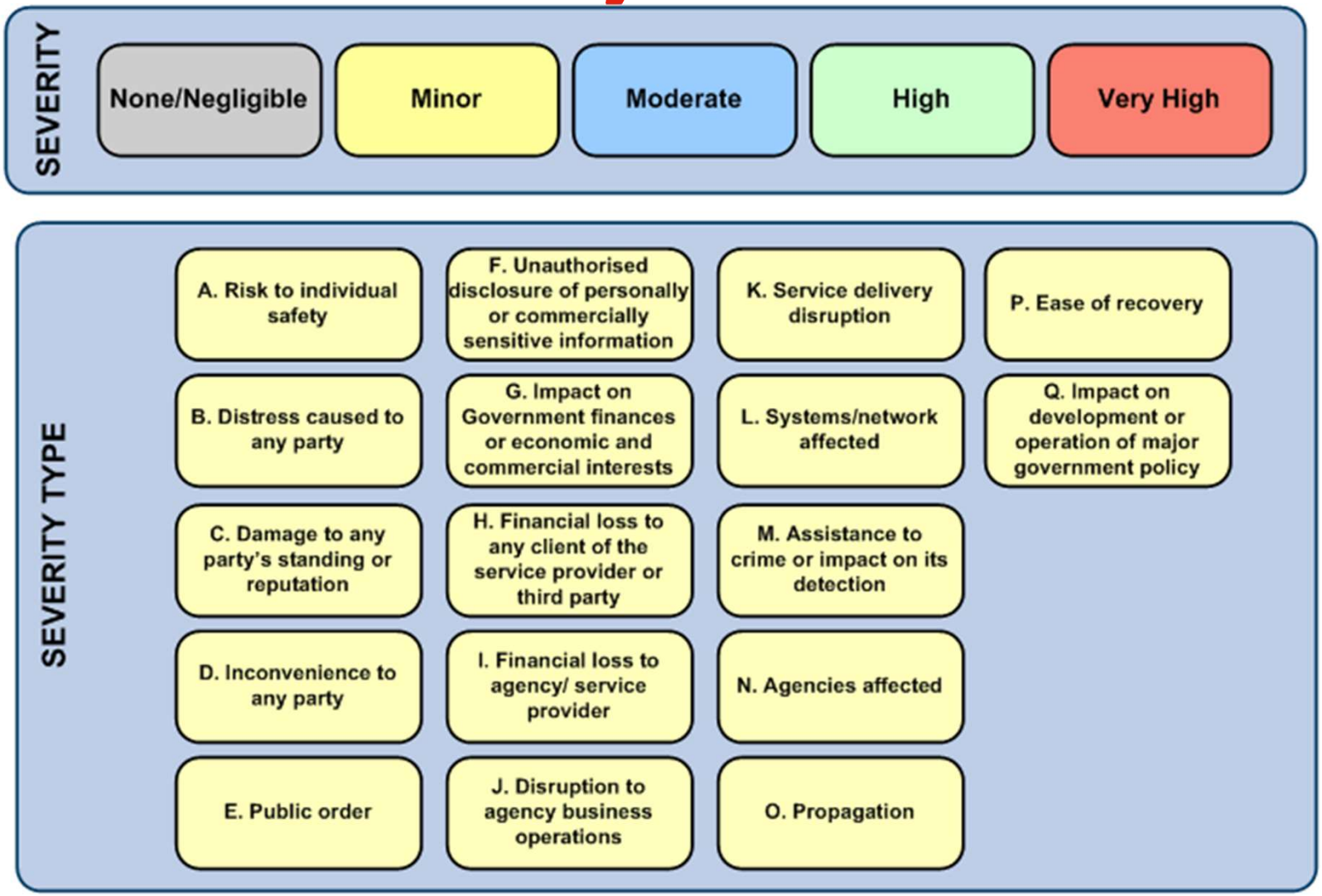
(Source: Information security incident category guideline, Queensland Government)

Security Incident Classification



(Source: Figure 2, Information security incident category guideline, Queensland Government)

Security Incident Severity Classification



(Source: Figure 2, Information security incident category guideline, Queensland Government)

(Source: Information security incident category guideline, Queensland Government)

Case Study 2(a) – An agency has detected a network intrusion from an external source. This particular attempt was successful in adversely affecting the security of agency information, as the agency's security controls were not able to prevent the intrusion from occurring. As a result of the attack, the agency's website was defaced, with the attacker's removing the existing content, and replacing it with offensive material. The incident is under investigation to identify where the attack has come from.

- **Incident:** The agency website was defaced
- **Incident Category:** Defacement of public information
- **Incident Impact/Compromise:** Integrity and Availability (removed and altered the public website information, which is not currently available there)
- **Cause:** Deliberate (the website was defaced through a network intrusion attack)
- **Origin:** External
- **Severity Type:** Significant interruption on the agency website information, measuring downtime, how long was business operations disrupted
- **Severity Metric(s):** Very high

(Source: Information security incident category guideline, Queensland Government)

Case Study 2(b) – An agency has detected a network intrusion from an external source. This particular attempt was successful in adversely affecting the security of agency information, as the agency's security controls were not able to prevent the intrusion from occurring. As a result of the attack, the agency's website was defaced, with the attacker's removing the existing content, and replacing it with offensive material. The incident is under investigation to identify where the attack has come from.

- **Incident:** A network intrusion from an external source
- **Incident Category:**
- **Incident Impact/Compromise:**
- **Cause:**
- **Origin:**
- **Severity Type:**
- **Severity Metric(s):**

Case Study 3 – A healthcare professional (Nurse) has been caught viewing confidential records of a patient that belong to a GP, without authorisation. The records were left unattended on a PC. The nurse claims she was unaware that she did not have the appropriate authority to view the MHR. The incident response investigation shows that the leaked information was very sensitive, however, she did not have prior involvement in such matters.

- **Incident:**
- **Incident Category:**
- **Incident Impact/Compromise:**
- **Cause:**
- **Origin:**
- **Severity Type:**
- **Severity Metric(s):**

BCP Framework

- **ISO/IEC 27031:2011** — Guidelines for information and communication technology readiness for **business continuity**.
  - Describes the concepts and principles of ICT readiness for business continuity.
  - Provides a framework of methods and processes to identify and specify all aspects of BCP planning, e.g. performance criteria, design, and implementation.
  - Covers preparedness of ICT services/infrastructures to support critical business operations during disruptions.
  - Provides BCP performance metrics: business impact analysis, recovery time objectives and recovery point objectives.
  - Encompasses all events and incidents (including security related) that could impact ICT infrastructure and systems.
  - Uses the Plan-Do-Check-Act (PDCA) model as the business continuity management system described in ISO 22301

ISO/IEC 22301:2012

- Business Continuity Management

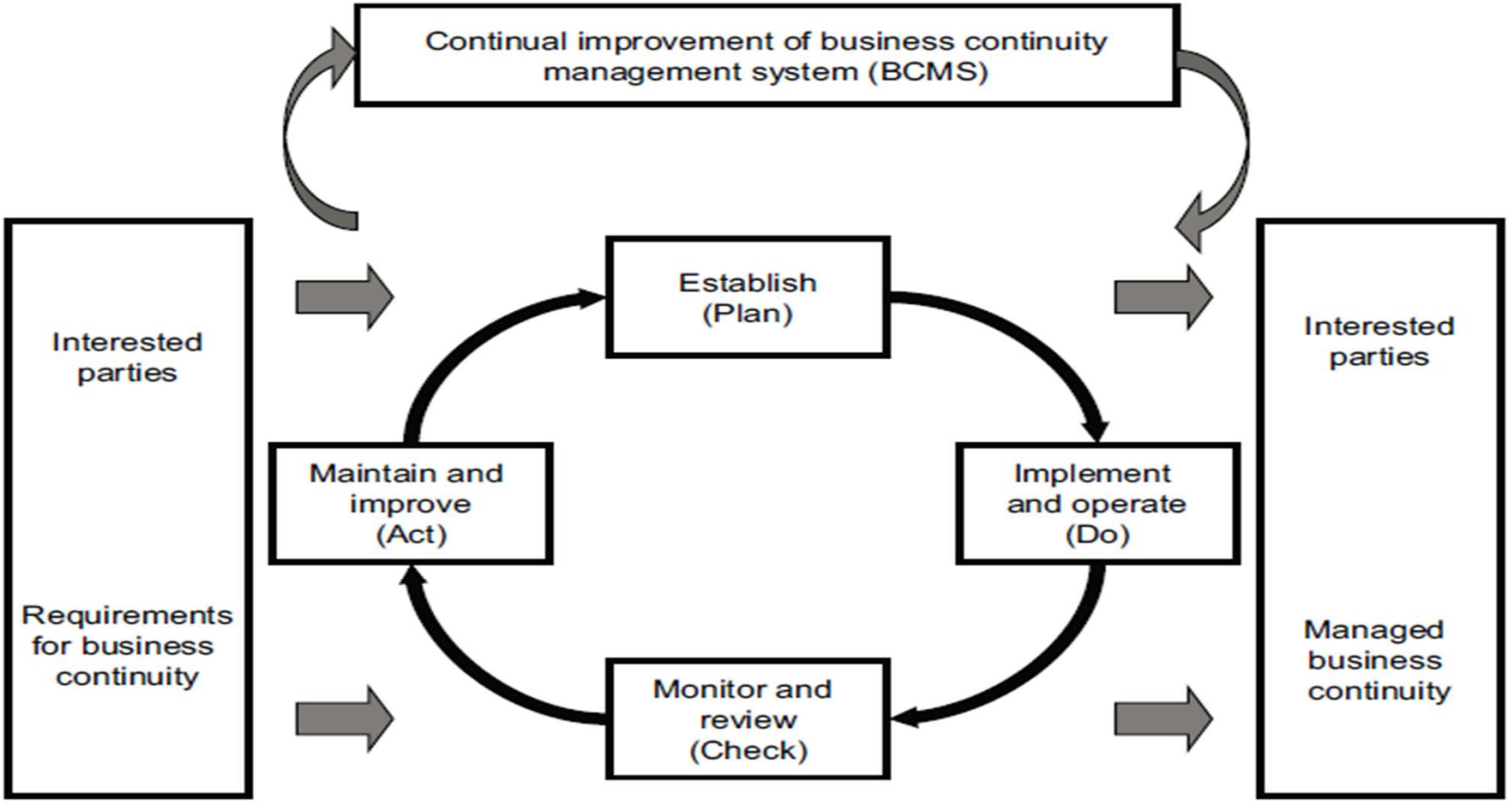
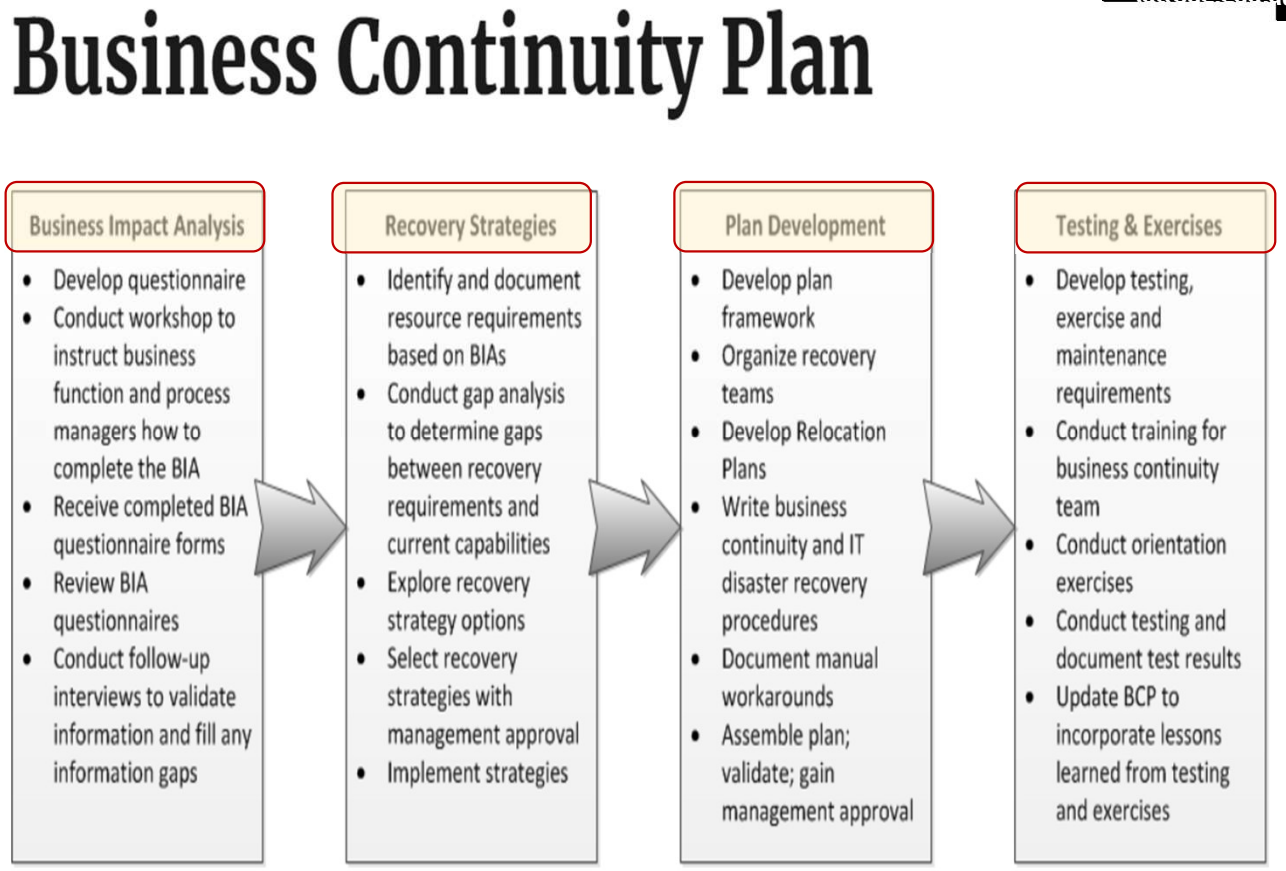


Figure 1 — PDCA model applied to BCMS processes

BCP framework



A four-step process can be used.

1. **Business Impact Analysis**
2. **Recovery Strategies**
3. **Plan Development**
4. **Testing and Exercise**

These steps and their highlights are taken from

- https://www.ready.gov/business/implementation/continuity
- Please Go to this web page to read this information

BIA (Business Impact Analysis)

- BIA is a process that organisations use
- to **analyze the impact** or effect of a business disruption could have on
  - **Business Activities** that support the provision of products and services.
- The results of this analysis are used to set
  - business continuity targets,
  - Recovery priorities,
  - Recovery objectives, and
  - Business priority targets.

Questions in a BIA

- What are the daily activities conducted in each area of my business?
- What are the long-term or ongoing activities performed by each area of my business?
- What are the potential losses if these business activities could not be provided?
- How long could each business activity be unavailable for (either completely or partially) before my business would suffer?
- Do these activities depend on any outside services or products?
- How important are the activities to my business?
  - on a scale of 1 to 5 (1 being the most important and 5 being the least important),
  - where would each activity fall in relation to the rest of the business?

https://www.fema.gov/media-library-data/1388776348838-b548b013b1cfc61fa92fc4332b615e05/Business_ImpactAnalysis_Worksheet_2014.pdf

Ready Business

Business Impact Analysis Worksheet

Department / Function / Process _____

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

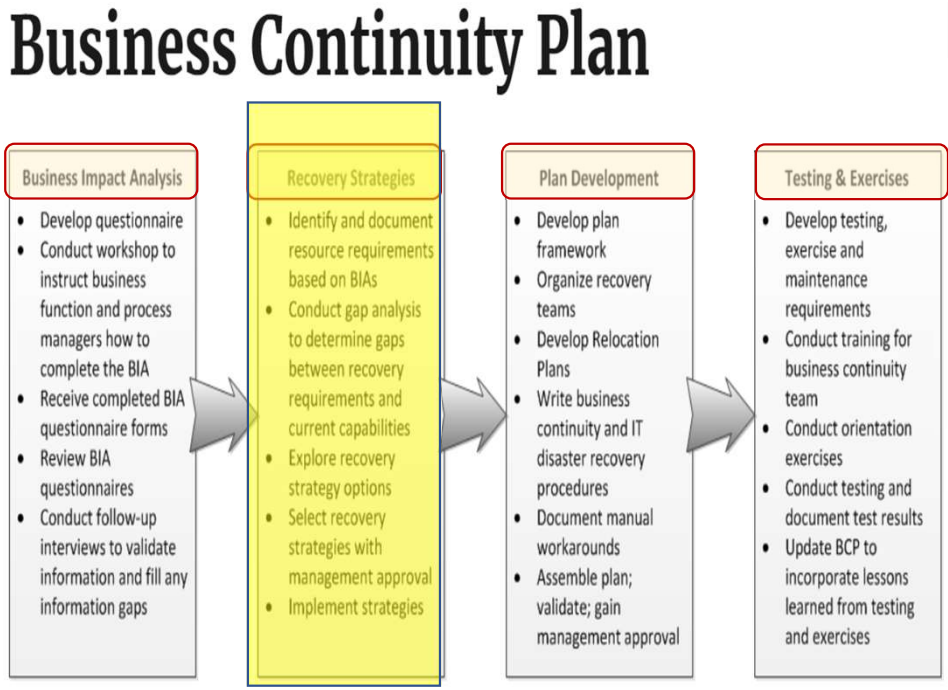
Financial Impact

Quantify operational impacts in financial terms.

ready.gov/business

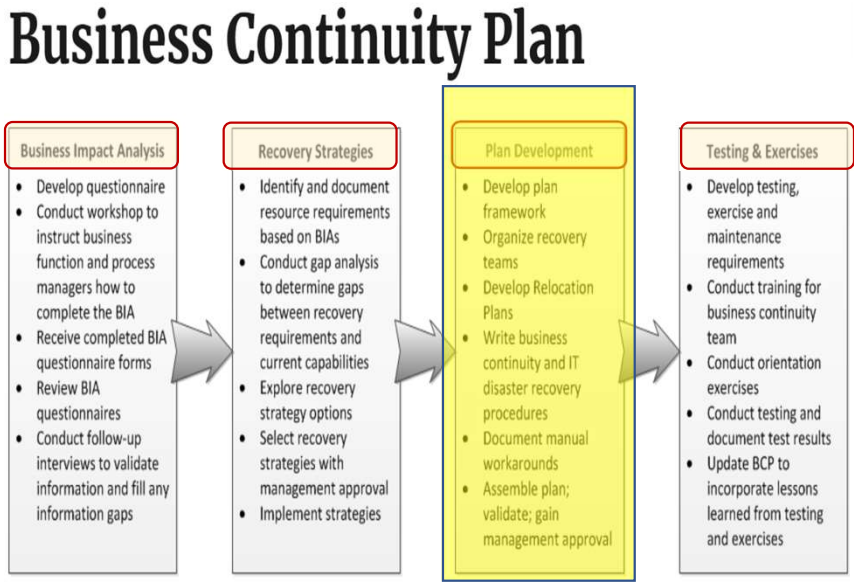
BCP: Recovery Strategies

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategies
- Select recovery strategies with management approval
- Implement strategies



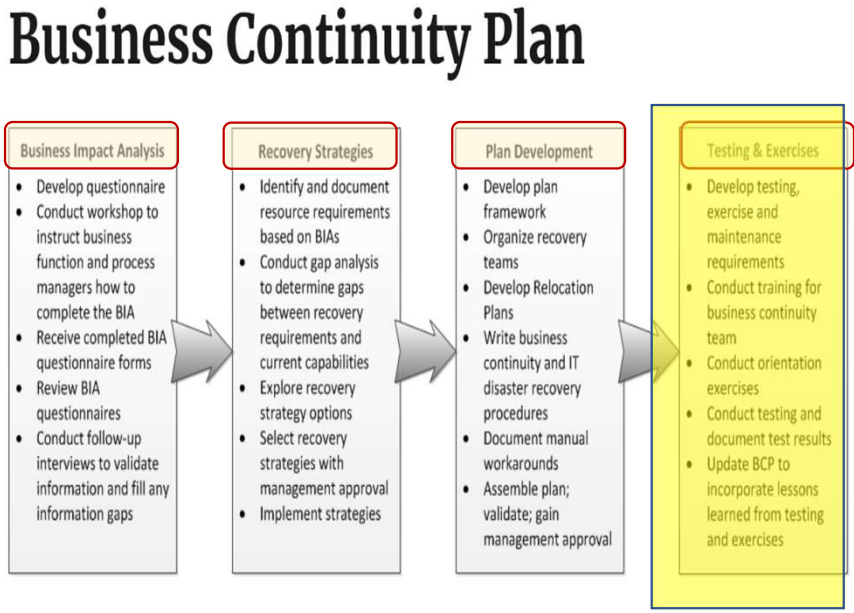
BCP: Plan Development

- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble the plan
- Validate the plan
- Gain management approval



BCP: Testing & Exercises

- **Develop** for **testing, exercise and maintenance requirements.**
- Conduct training for business continuity team.
- Conduct orientation exercises.
- Conduct testing and document test results.
- Update BCP to incorporate lessons learned from testing and exercises.



LA TROBE UNIVERSITY

See You Next Session

latrobe.edu.au