WEEK 3

Introduction

**BPMN** - **B**usiness **P**rocess **M**odelling **N**otation

* Modelling and Analysis

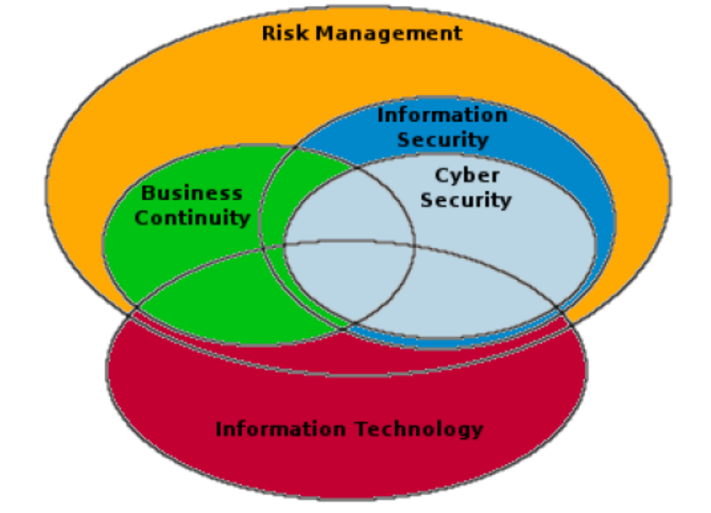
Focusing on different aspects of business continuity:

* Core concepts
* Enabling technologies
* Case studies

Standards

* ISO22301
* ISO27001
* BS25999 (Evolved from ISO22301)
* BS27031
* Guidelines from National Cybersecurity Centre (*NCSC*)
* Guidelines from **ENISA** and **NIST**

Understanding the Relationships



***RISK***: The level of impact on organisational **operations** (*including mission, functions, image, or reputation*), organisational **assets**, or **individuals** resulting from the operation of an information system given the **potential impact of a threat** and the **likelihood of that threat occurring.**

BUSINESS CONTINUITY: Ensure integrity & continuity of underlying processes.

* PaaS
  + **P**latform **a**s **a** **S**ervice
  + Cloud computing that provides virtualized computing resources over the internet.
* IaaS
  + **I**nfrastructure **a**s **a** Service

Business Continuity Management (BCM)

A process that provides a framework ensuring the continuity or uninterrupted provision of critical business functions and operations. It provides a basis for planning to ensure an organization’s long-term survivability following a disruptive event towards the “*business as usual*” functions and services.

BCM can be considered as a **risk treatment method**, complementary of a wider Risk Management method, explicitly focused on the **management** and **containment** of **continuity** **risks**, introduced by **certain natural** or **man-made threats** that, if realized, can cause unavailability of services (*business processes*).

Business Continuity in context

DISASTER RECOVERY

The creation & execution of plans to recover the data & systems of an organisation to the point immediately prior to the interruption.

CONTINGENCY

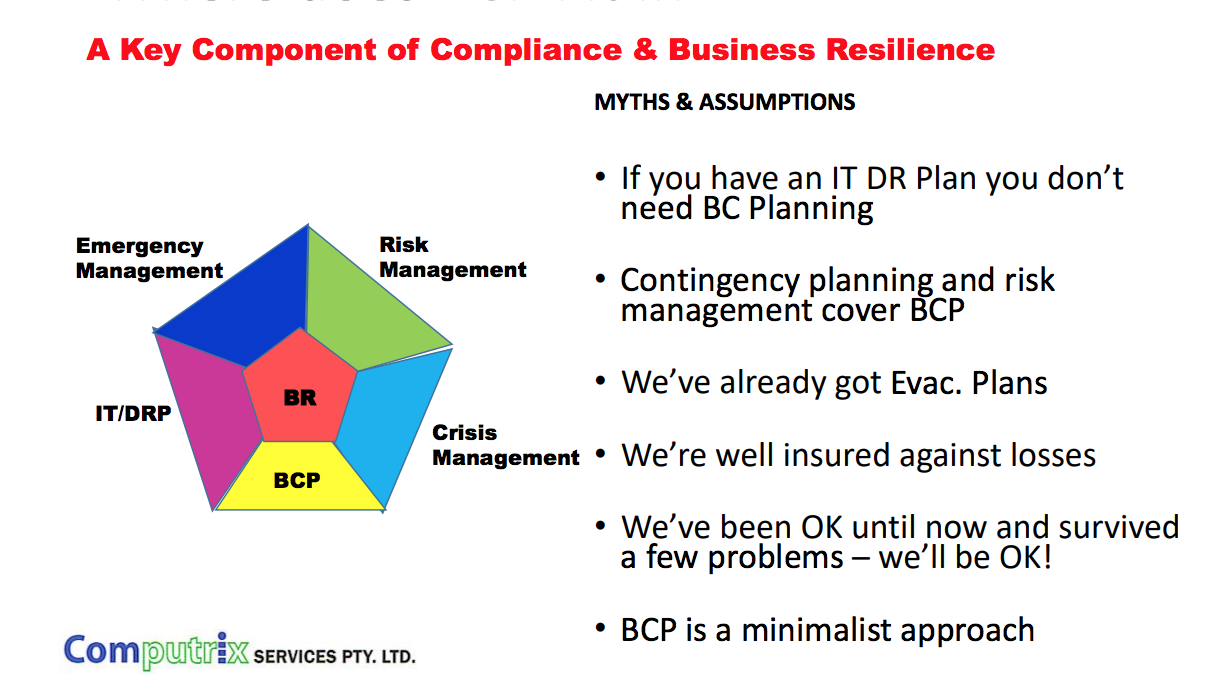
The physical or process alternative to a single point of failure *e.g. back up generator for power failures*.

OPERATIONAL CONTINUITY

The alternative processes implemented during a failure, which allow the “*process*” to continue, whilst relying on the contingencies or Disaster Recovery Plans to restore full operations.

BUSINESS CONTINUITY

The processes by which business can be maintained to an acceptable level until full processes and systems are restored.



UK National Cyber Security Centre (NCSC)

* All organisations will experience **security incidents** at some point.
* Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.
* Businesses should implement an incidence management capability
  + Detect, manage and analyse security incidents.
* Managing Business Harm
  + Failure to realise an incident has happened.
* Continual Disruption
  + Address root cause of incidents (e.g. poor tech. or weakness in security approach).
* Non-Compliance With Legal & Regulatory Reporting
  + Compromising sensitive information covered by mandatory reporting.
* Establish An Incident Response Capability
  + Organization wide, may use inhouse or specialist management company.
* Define roles/responsibilities
  + Appoint (empower) individuals to handle incidents & identify clear terms of reference.
* Establish Data Recovery Capability
  + Backup of essential data – held in a physically secure location (ideally offsite). Ability to recover archived data for operational use should be regularly tested.
* Test Incident Management Plans
  + Business continuity & disaster recovery plans constantly tested.
* Information Sharing Strategy
  + For services or information bound by specific legal or regulatory reporting requirements you may have to report incidents.
* Forensics
  + Preservation & analysis of sequence of events that led to the incident.

Considering Business Continuity: Impact

Generally five categories:

1. LEGAL AND REGULATORY
2. PRODUCTIVITY
3. FINANCIAL STABILITY
4. REPUTATION
5. LOSS OF CUSTOMER CONFIDENCE

* Legal / Compliance Risks

Arising from violations of compliance with laws and regulations (*i.e. data retention*). Legal or compliance risks can expose an organization to negative publicity, fines, penalties, payment of damages and annulations of contracts.

Loss or destruction of customer information (i.e. personal data) such as credit card information, financial information and health information can also raise potential risks from third party claims.

Failure to meet Service Level Agreement requirements with customers regarding data service availability may result to significant lawsuits.

* Productivity Risk

Resulting from operational losses and **poor customer service delivery**.

Risks may emerge from unavailability of basic production services and operation functions.

Such risks may be relevant to all production activities that contribute in some way to the overall delivery of a product or service. Productivity Risks are not confined only to the use of technology; they can be the result of organizational activities.

The risks arising from inadequate or poorly controlled.

* Financial Stability Risks

Arise through unavailability of delivered products and services towards the organization’s customers.

Such risks may lead to major financial losses having impact directly or indirectly on the financial stability of the organization.

* Reputation and Loss of Customer Confidence

The most difficult and yet one of the most important risks to quantify and mitigate.

Such risks lead to the damage to the organization’s reputation, an intangible but important asset.

Small Companies (SMEs)

*Negative:* Small and Medium-scale Enterprises: potential impact of the risks they face is likely to be more destructive since the majority operate in specialised markets where even a short interruption to normal business can have a disproportionate effect – totally halting output and letting customers down.

***Positive:*** **No one knows their own business better than SMEs**, as they often **rely on limited resource**s – in best position to know how their business would cope without supporting infrastructures (e.g. IT systems) for a given period of time (e.g. morning, a day, or a week).

BS25999 to ISO 22301

Continuity Management is a holistic management process that “identifies in advance the potential impacts of a wide variety of disruptions to the organization’s availability. This includes all necessary activities allowing the organization to tolerate the loss of part or all of its operational capability.”

* Now an international standard: **ISO 22301**

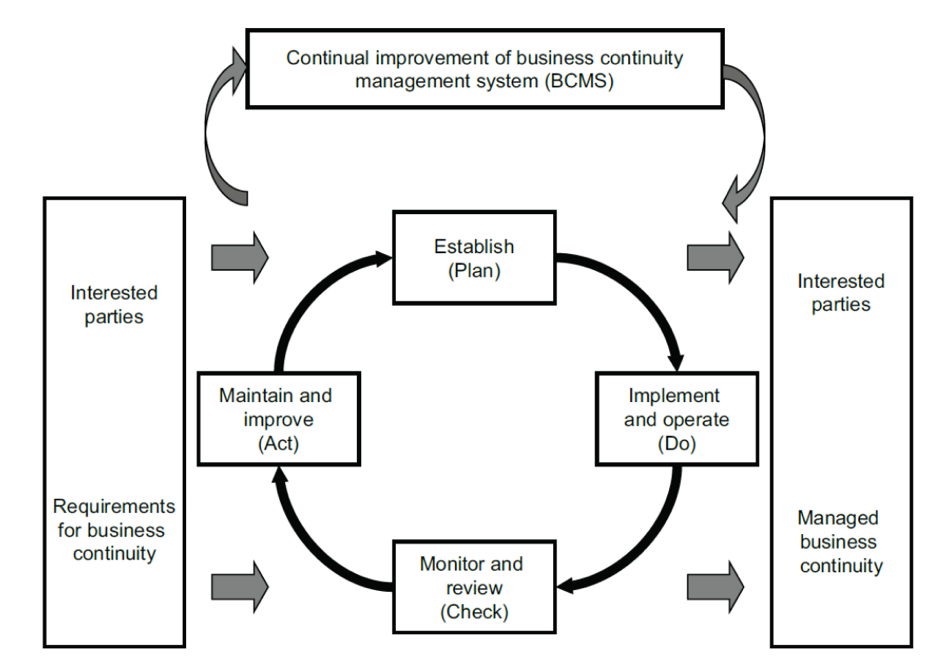
ISO 22301

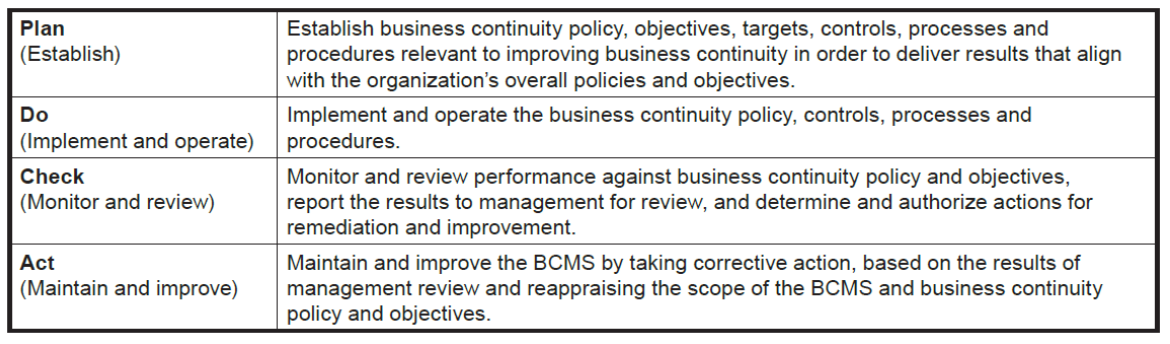
Societal security - Business Continuity Management Systems – Requirements

ISO 22301 applies the “Plan-Do-Check-Act” (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization’s Business Continuity Management System (BCMS).

* Aims to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
* Enables an organization to **design** a **BCMS** that **is appropriate to its needs** and that meets its interested parties’ requirements.

PDCA model for BCMS





BCM is expected to:

* Understand the **overall risk context** within which the organization operates;.
* Identify/document the **critical business functions** that the organization has to deliver.
* Identify what **barriers or interruptions can be encountered** in trying to deliver these critical business functions.
* Understand how the organization can continue to deliver these functions should interruptions occur.
* Understand the likely range of outcomes when continuity controls and other mitigation strategies are implemented.
* Ensure that all staff understand their roles and responsibilities when a major disruption occurs.
* **Build consensus and commitment** to the implementation, deployment and exercising of business continuity.
* Integrate business continuity as part of routine “business as usual”.

BCM checklist & procedures

Safety of personnel (*health & safety*) and associated procedures due to direct, indirect or potential effects of any incident or emergency (*i.e. evacuation, shelter-in-place, area of refuge*).

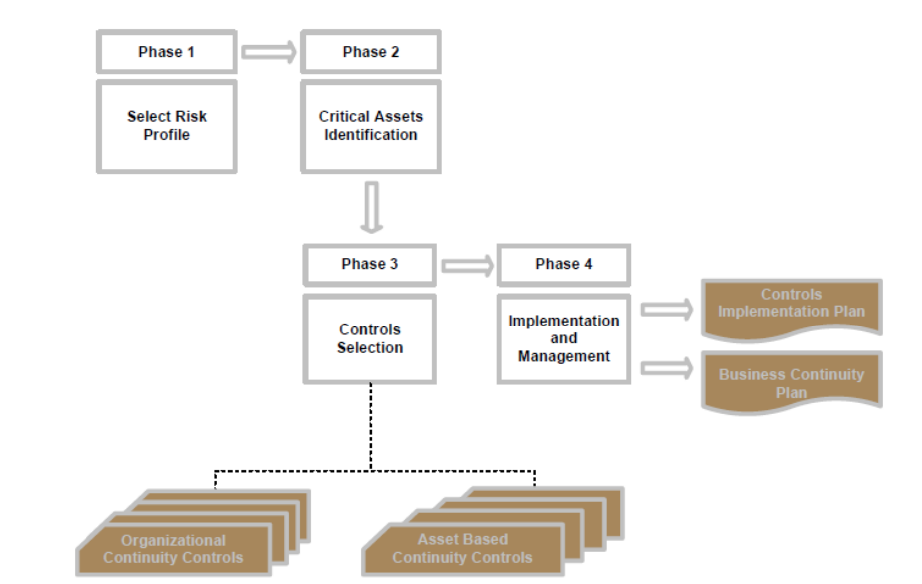
Business Continuity Plan: Step 1

* **Scope**: identify the critical business functions of the organization to be protected.
* Link to emergency management procedures and plans to ensure personnel safety.
* Identify critical ICT assets required to recover and sustain the minimum operating levels of the critical business functions in scope.
* Define the resource requirements (people, work area, IT, telecommunications) for the plan implementation
* Set the structure of the business continuity response with a focus on ICT.
  + Establish roles and responsibilities during an incident.
  + Disaster recovery plan: How to recover operations in a case of a disaster.
  + Per ICT asset contingency plan: How to recover a specific ICT asset.

Business Continuity Plan: Step 2

* Define the controls used to safeguard the continuity of the functions in scope.
* Provide contact list(s) with business continuity responsible employees / teams / managers.
* Provide contact details of vendors / suppliers committed to supporting the recovery efforts.
* Provide contact list of Governmental authorities / bodies.
* Define activities for Testing, Reassessing and Maintaining the organization’s Business Continuity Plan.

ENISA’s BCM Process (OCTAVE ALLEGRO)



Phase 1: Select Risk Profile

* Assessment Team evaluates business risk profile by using a predefined set of qualitative criteria.
* Considered across the categories defined previous – e.g. Legal, Productivity, Financial Stability, Reputation/Customer less.

Phase 2: Critical Asset Identification

* Critical business functions: those whose interruption will lead to an **organisation suffering from serious financial, legal, and/or other damages or penalties**.
* Earliest possible recovery of such functions after a disruption is the main objective of a Business Continuity Plan.
* **Together with the assessed Risk Profile, critical business functions** are key parameter for the BCP (*i.e. complexity, required effort, recovery costs, etc.).*
* **Business function recovery priority** determines the **absolute maximum time within which the function can be unavailable and the SME can remain viable**.
  + i.e. the maximum period of time in which the function can be down before severe damage has been caused to the organization.
* Recovery period depends on SLA: less than 1 day, 1 to 3 days and up to 5 days.

Phase 3: Asset types (… can change over time)

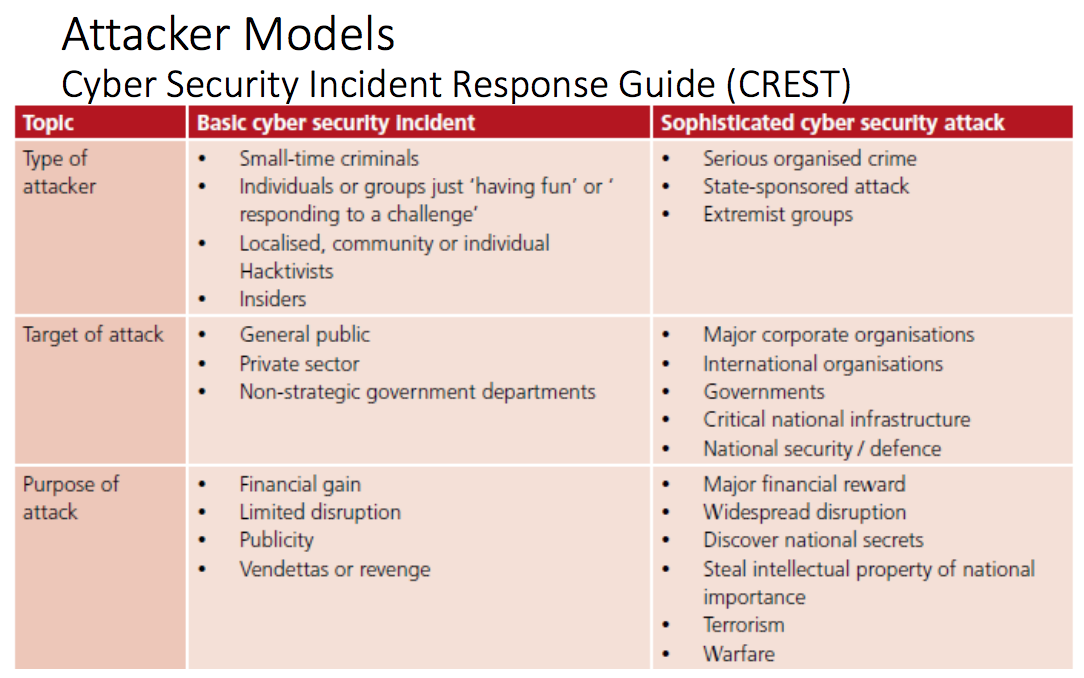
**Organizational controls**: Contain controls concerned with **practices** and **management** **procedure**.

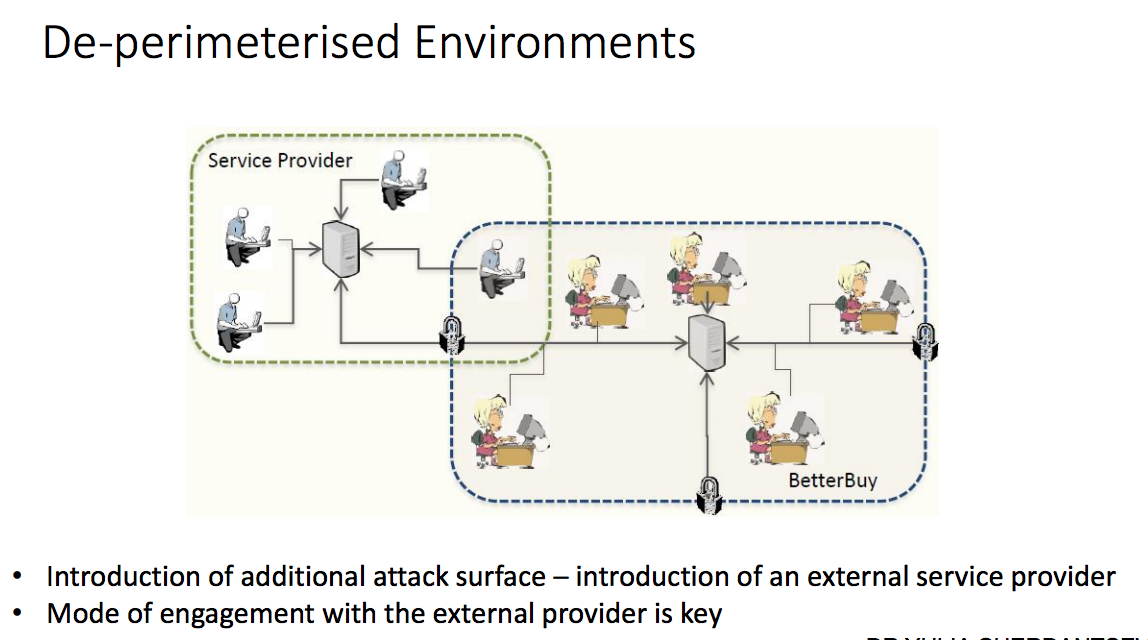
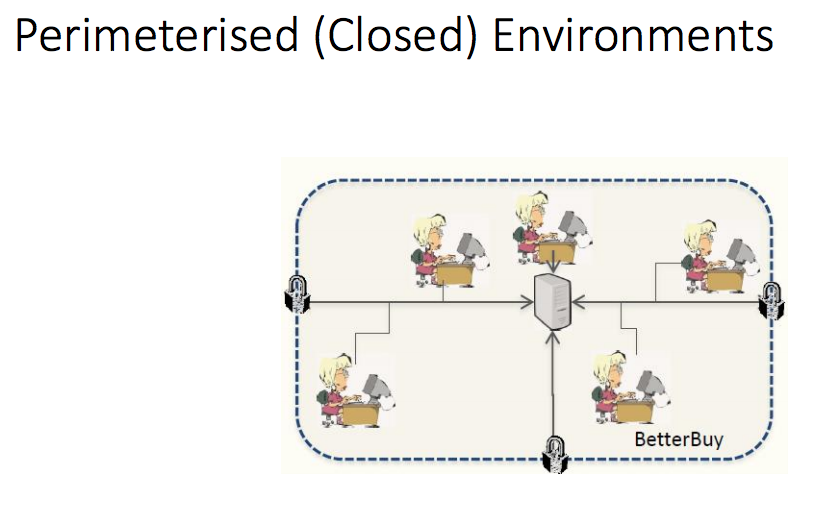
**Asset control**: Applicable to categories of critical assets.

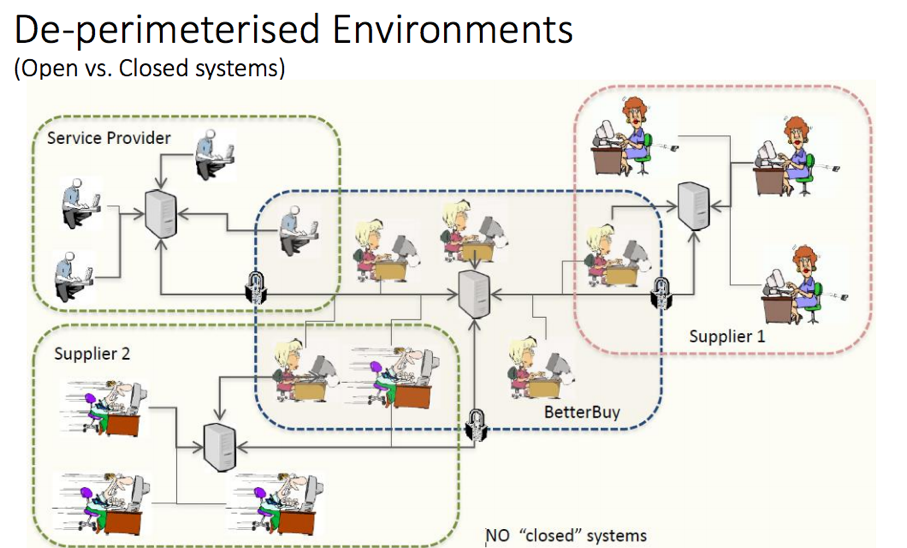
Control cards are essentially **pre-selected** and grouped according to **risk profiles** and **asset recovery priority**.

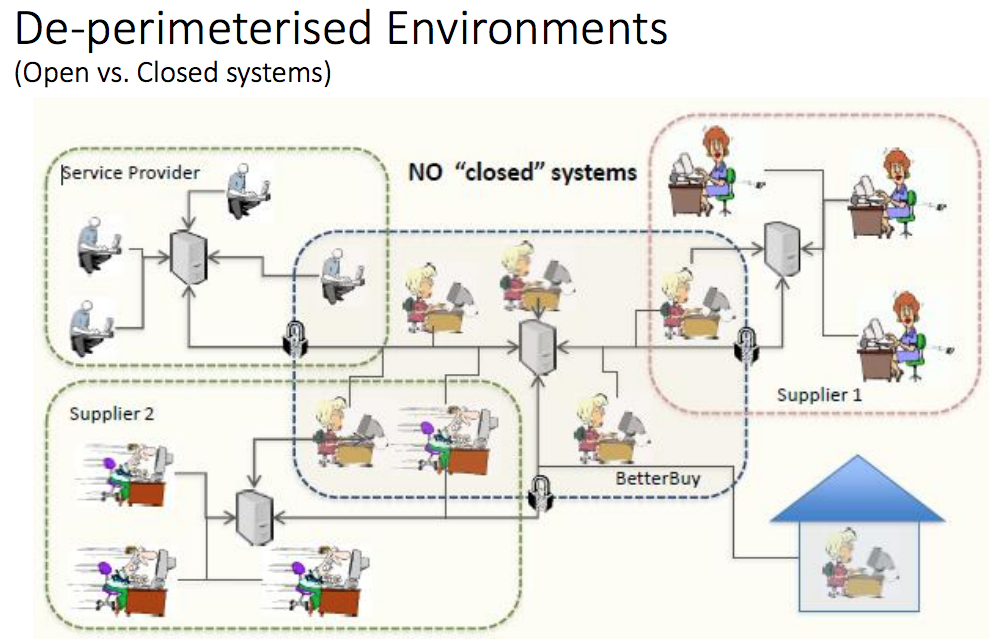
Phase 4: Implementation plan

* Using control cards as “*continuity requirements*” assess the gaps between these and current business continuity practices both at an organizational and critical asset level.
* Prioritization is key here – not all requirements realizable in practice.









Small Business Guide: Response & Recovery

**STEP 1:**

* Prepare for incidents.
  + Identify critical assets & systems.
  + Identify business processes & systems.
  + Prioritise risk.
  + Make an incident plan.

**STEP 2**:

* Identify what is happening. (*Computer running slow? Accounts locked?*)
  + Are you being attacked?
  + Identify what happened.
  + Stop the incident getting worse (*antivirus alerts & server/audit logs*)

***10 CRUCIAL QUESTIONS:***

1. What problem has been **reported**, and by who?
2. What **services, programs** and/or **hardware aren’t working**?
3. Are there any signs that **data has been lost**? For example, have you received ransom requests, or has your data been posted on the internet?
4. What **information** (if any) has been **disclosed** to **unauthorised parties**, **deleted** or **corrupted**?
5. Have your **customers noticed any problems**? **Can** they **use** your **services**?
6. Who **designed** the **affected system**, and **who maintains it**?
7. When did the **problem** **occur** or **first come to your attention**?
8. What is the **scope of the problem**, **what areas** of the **organisation** are **affected**?
9. Have there been any **signs as to whether the problem has occurred internally** within your organisation **or externally** **through** your **supply chain**?
10. What is the **potential business impact of the incident**?

**STEP 3**:

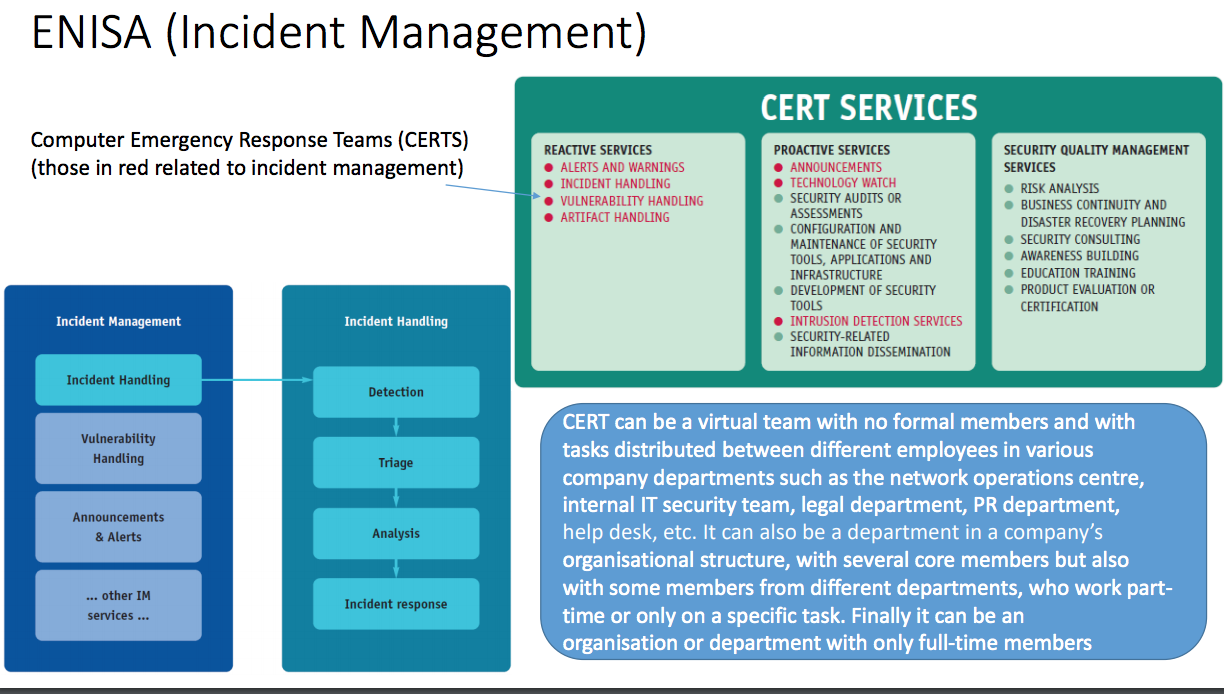
* Resolve the incident.
  + IT system managed **externally** or **internally**.

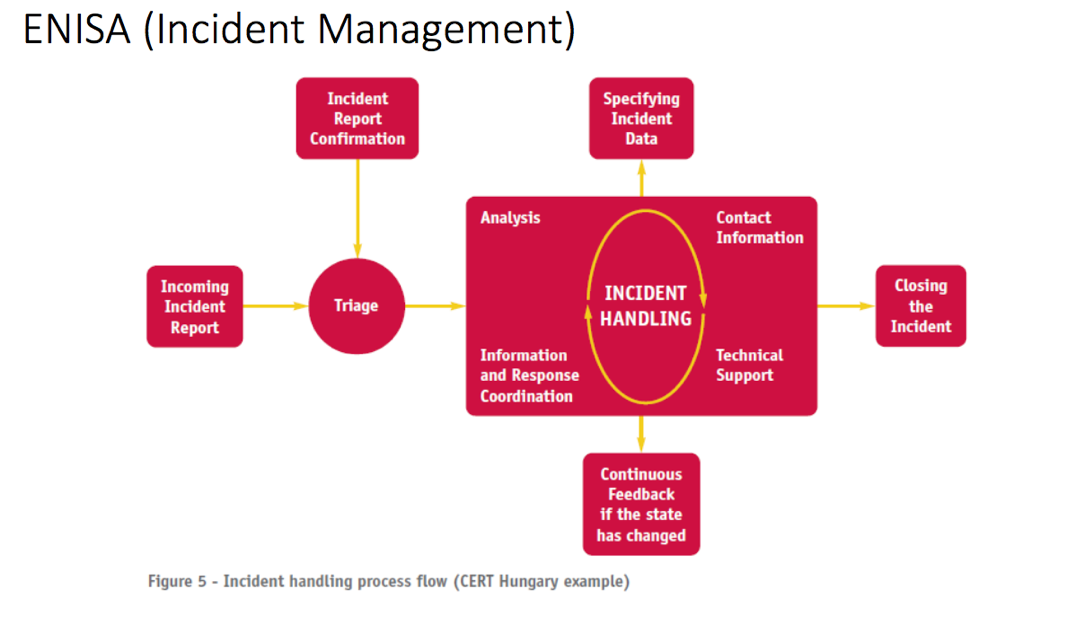
**STEP 4**:

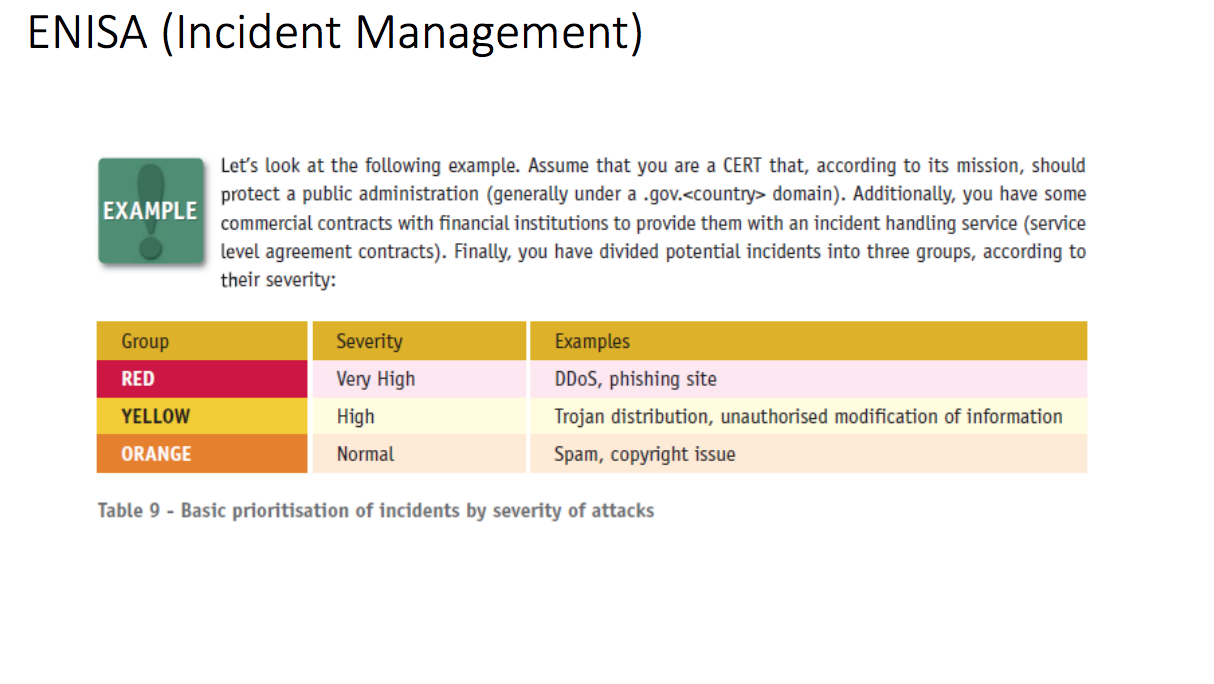
* Report incident to wider stakeholders.
  + Report to law enforcement – e.g. Information Commissioner’s Office (ICO) (<https://ico.org.uk/for-organisations/report-a-breach/>).
  + Keep everyone informed (staff & customers) – time that is proportionate to the effect of the incident.
  + Consider legal advice.

**STEP 5**:

* Learn from the incident
  + Review actions taken during response.
  + Update your incident plan & strengthen your defences (*e.g. password policy*).
  + Consider the terms of your contracts (*e.g. 3rd party contracts & SLAs*)







Incident Taxonomy (European CERT) – Latvian CERT

* **Attacks** on the **critical** **infrastructure**.
* **Attacks** on the **internet** **infrastructure**.
  + *e.g., root or system-level attacks on any server system, or any part of the backbone network infrastructure, denial of service attacks.*
* Deliberate **persistent** **attacks** on **specific** **resources**, i.e., any compromise which **leads** or may lead **to** **unauthorised access to systems**.
* **Widespread automated attacks against internet sites**, e.g., sniffing attacks, ‘social engineering’ attacks, password cracking attacks.
* **Threats, harassment,** and **other criminal offences** involving **individual user accounts**.
* **Botnets**
  + i.e., activities related to the network of compromised systems controlled by a party which is the source of an incident.
* **Denial of service** on **individual** user **accounts**, *e.g. mail bombing.*
* **Forgery** and **misrepresentation**, and other security-related **violations** of local **rules** and **regulations**,
  + e.g. e-mail forgery, SPAM, etc.
* **Compromise** of **single desktop systems**.
* **Copyright** **violations**