CMT308: Business Continuity & Transformation

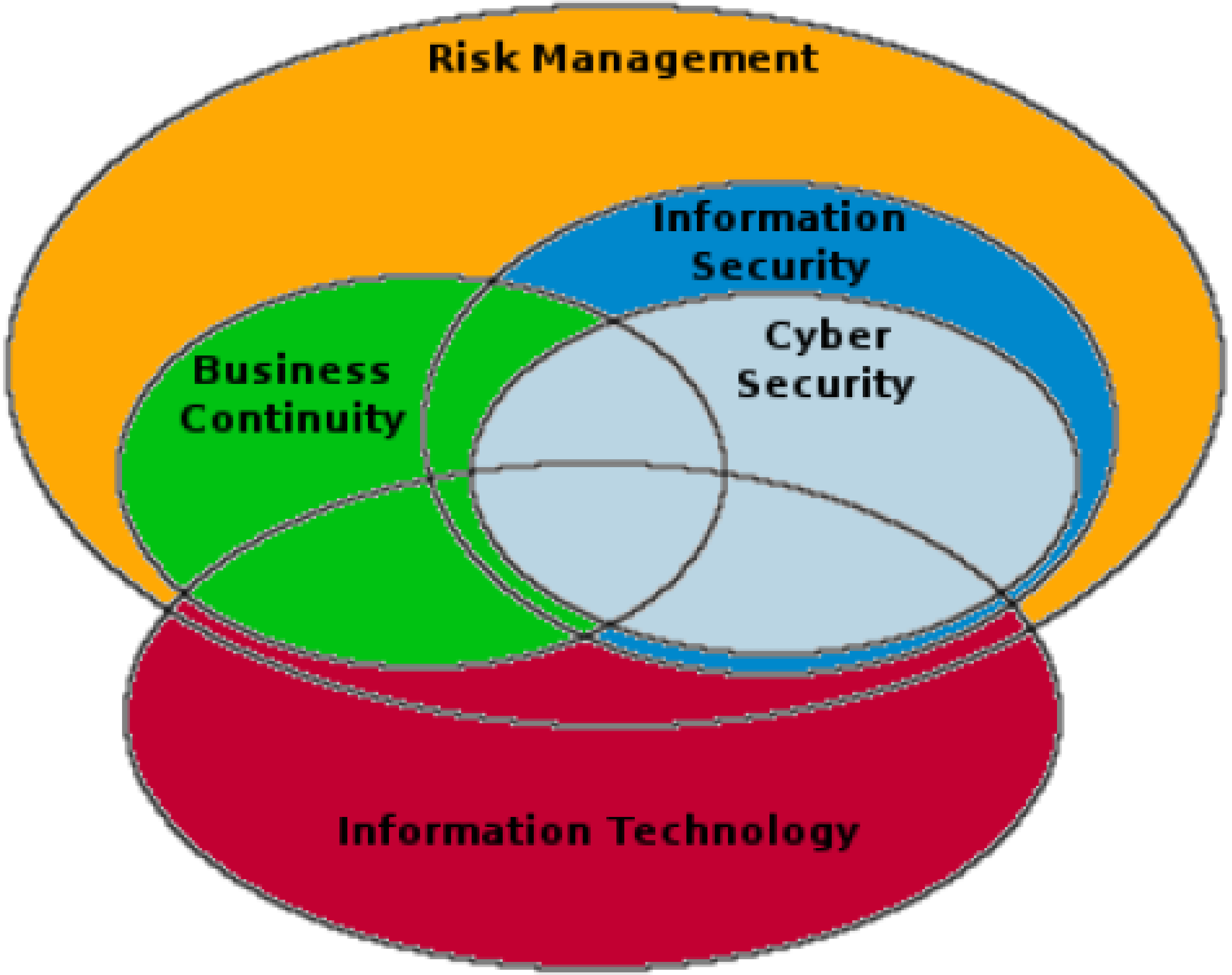
Omer Rana

ranaof@cardiff.ac.uk

7 sessions

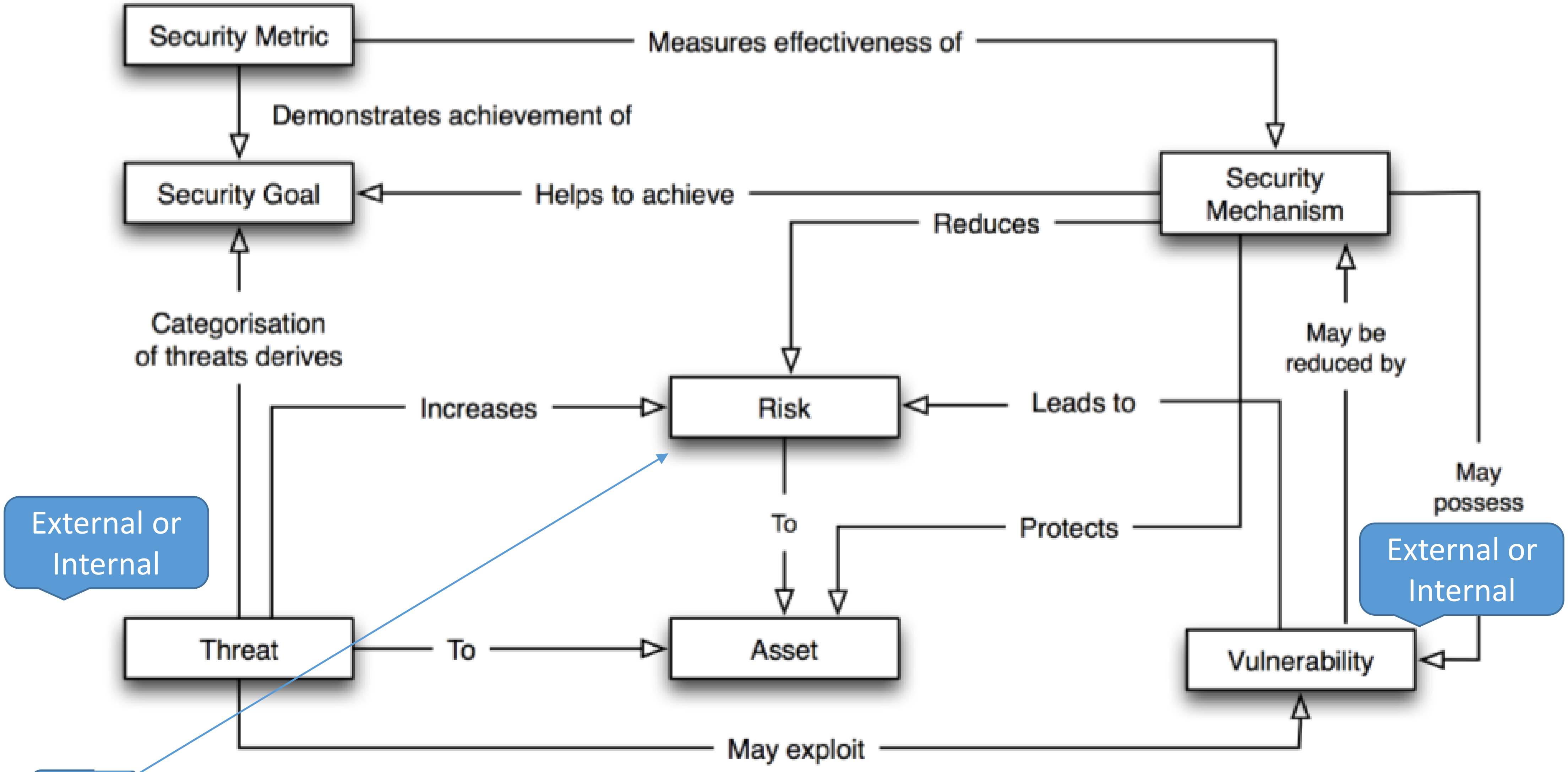
- Focusing on different aspects of business continuity
  - Core concepts
  - Enabling technologies
  - Case studies
- Standards
  - ISO22301, ISO27001, BS25999, BS27031
- Guidelines from National CyberSecurity Centre (NCSC)
- Guidelines from ENISA and NIST
- Each session will have a theme

Understanding the relationships



"As a UK business there is around a **1 in 3 chance that you will experience a cyber breach**. When something happens, such as a cyber incident, it can be difficult to know how to react. We understand you will want to resolve the problem and get back to business as soon as possible. One way you can help limit the impact a cyber breach has on your business, is to be prepared."

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019



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.**

DR YULIA CHERDANTSEVA

Module focus

- Module focus – **Business Processes**
  - Modelling and Analysis
- Should become experts in BPMN
  - Spend time understanding this
- Understanding and representing processes within:
  - An institution (business/company or other institution (Univ., Charity))
  - Inclusion of third-party systems – Internet of Things, Cloud computing, DB/systems
  - Outsourcing part of the infrastructure (issues around this)
- However – everything viewed through the lens of a business process

Research focused – this module will give you a taste of undertaking research

Make you practitioners

Business continuity – ensure integrity & continuity of underlying processes

Module focus

- Approaches can be of two types
- **Data Driven approaches:**
  - i.e. utilize historical data as an estimate of reliability
  - We can also use Bayesian Belief Networks (WEKA toolkit) & Bayesian Network classifier
  - Investigate use of Graph-based representation (e.g. Gephi)
  - Can benefit from advances in AI and Machine Learning
- **Policy (Qualitative) Driven approaches:**
  - Based on an assessment of assets and key business functions

Will attempt to combine these two themes

Session Themes

- Session 1: Introduction & Background (Oct 18)
- Session 2: Service Level Agreements (Nov 8)
- Session 3: Dependency & Resilience (Dec 6)
- Session 4: Migrating your system: Cloud Migration (Jan 31)
- Session 5: Chaos "Monkeys" from Netflix OSS – Resilience (Feb 14) – "Chaos Engineering" & Disturbance Benchmarking
- Session 6: Vulnerability Assessment & Mitigation Strategies (Mar 6)
- Session 7: Putting it all together … (Mar 27)

Written Assessment 50%: Coursework 1

Written Assessment 40%: Group Report

Presentation 10%

NO EXAM(!)

Business Continuity Management (BCM) is 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 Continuity …

- Often focus is on environmental controls to safeguard from natural disasters: power supply, fire, flood etc.
- Inadvertent threats pose some of the highest continuity risks, and yet personnel training and awareness programmes are often neglected
- Much wider topic – ranging from personnel management to economic viability … however for this module:

Focus on ensuring & protecting **the availability of the core IT assets used to support and provide the organization's critical business functions** (i.e. production, customer relationship, human resource)

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

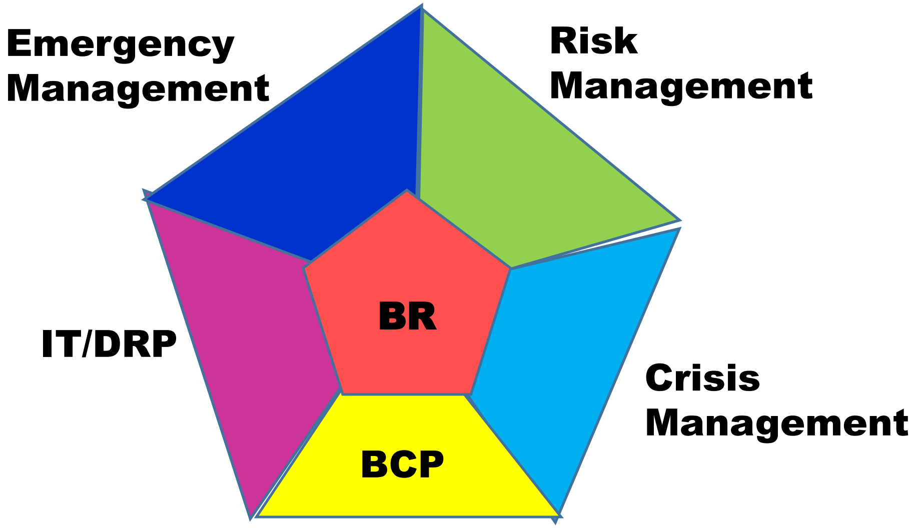
Contingency - the physical or process alternative to a single point of failure e.g. back up generator for power failures

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

Where does BCP Fit In

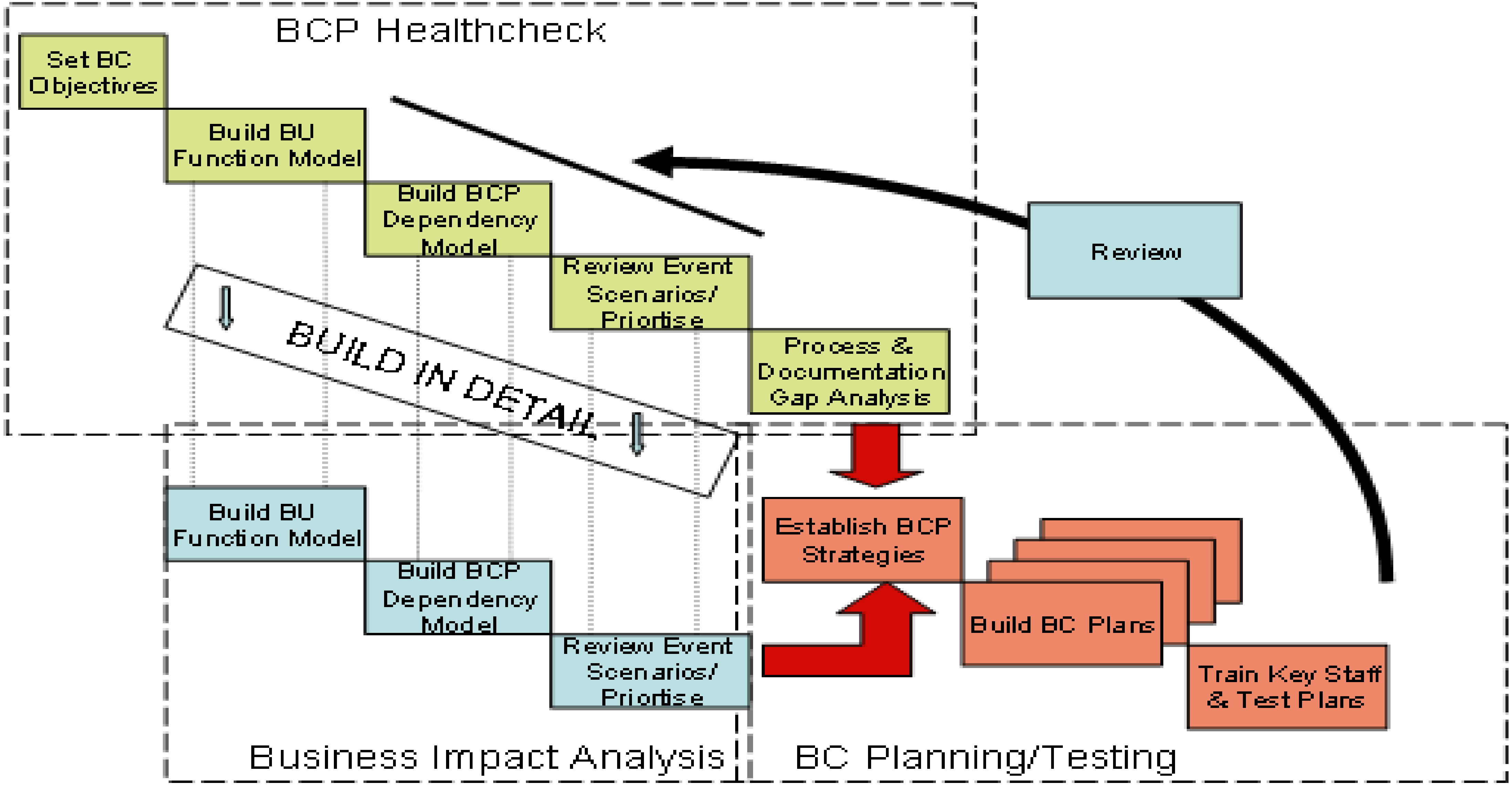
A Key Component of Compliance & Business Resilience



MYTHS & ASSUMPTIONS

- If you have an IT DR Plan you don't need BC Planning
- Contingency planning and risk management cover BCP
- We've already got Evac. Plans
- We're well insured against losses
- We've been OK until now and survived a few problems – we'll be OK!
- BCP is a minimalist approach

Computrix SERVICES PTY. LTD.


BCP Healthcheck
Set BC Objectives
Build BU Function Model
Build BCP Dependency Model
Review Event Scenarios/ Priortise
Process & Documentation Gap Analysis
Review
BUILD IN DETAIL
Build BU Function Model
Build BCP Dependency Model
Review Event Scenarios/ Priortise
Establish BCP Strategies
Build BC Plans
Train Key Staff & Test Plans
Business Impact Analysis
BC Planning/Testing

Computrix SERVICES PTY. LTD.

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

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/incident-management

UK National Cyber Security Centre (NCSC)

https://www.ncsc.gov.uk/information/cir-cyber-incident-response

- **Establish an incident response capability**: organization wide, may use in-house 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

https://www.ncsc.gov.uk/section/about-ncsc/incident-management

Considering Business Continuity: Impact

Generally five categories:

- Legal and Regulatory,
- Productivity,
- Financial stability,
- Reputation and
- Loss of Customer Confidence;

Considering Business Continuity: Impact

- **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.

Considering Business Continuity: Impact

- **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

lack of privacy and disruption of service to customers

Considering Business Continuity: Impact

- **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

Service Level Agreements – play a key part in this

Considering Business Continuity: Impact

- **Reputation and Loss of Customer Confidence** are 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.

- “Will customers and / or other companies cooperate with a company once they read in the paper that a company’s service quality is low or service delivery is regularly interrupted? Will top employees remain at a company so reputably damaged?”
- And, what will be the reaction of the company’s shareholders? What is the expected loss of future business revenue?
- What is the expected loss of market capitalization?

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 resources – 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).
- As SMEs are usually servicing a niche market, they are able to know if their customer base would be affected (e.g. go elsewhere or return)

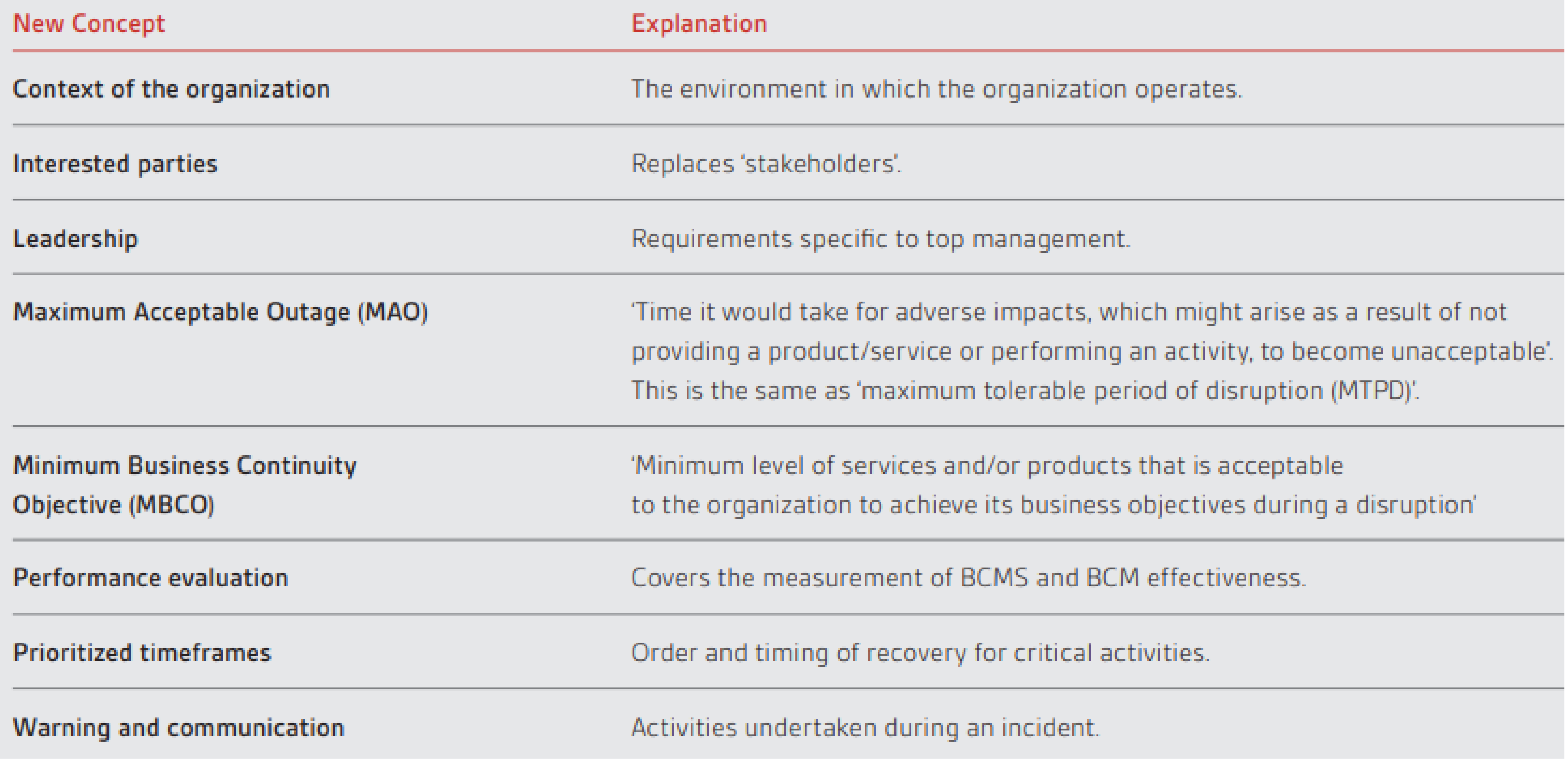
depending on the sector, customers may be obliged to use suppliers who comply with certain security/continuity standards

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

"Successful businesses expect the unexpected and plan for it. Disruptions to your business can result in data risk, revenue loss, failure to deliver services as normal or in extreme cases, failure to deliver at all."

ISO 22301/22313



New Concept	Explanation
Context of the organization	The environment in which the organization operates.
Interested parties	Replaces ‘stakeholders’.
Leadership	Requirements specific to top management.
Maximum Acceptable Outage (MAO)	‘Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable’. This is the same as ‘maximum tolerable period of disruption (MTPD)’.
Minimum Business Continuity Objective (MBCO)	‘Minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption’
Performance evaluation	Covers the measurement of BCMS and BCM effectiveness.
Prioritized timeframes	Order and timing of recovery for critical activities.
Warning and communication	Activities undertaken during an incident.

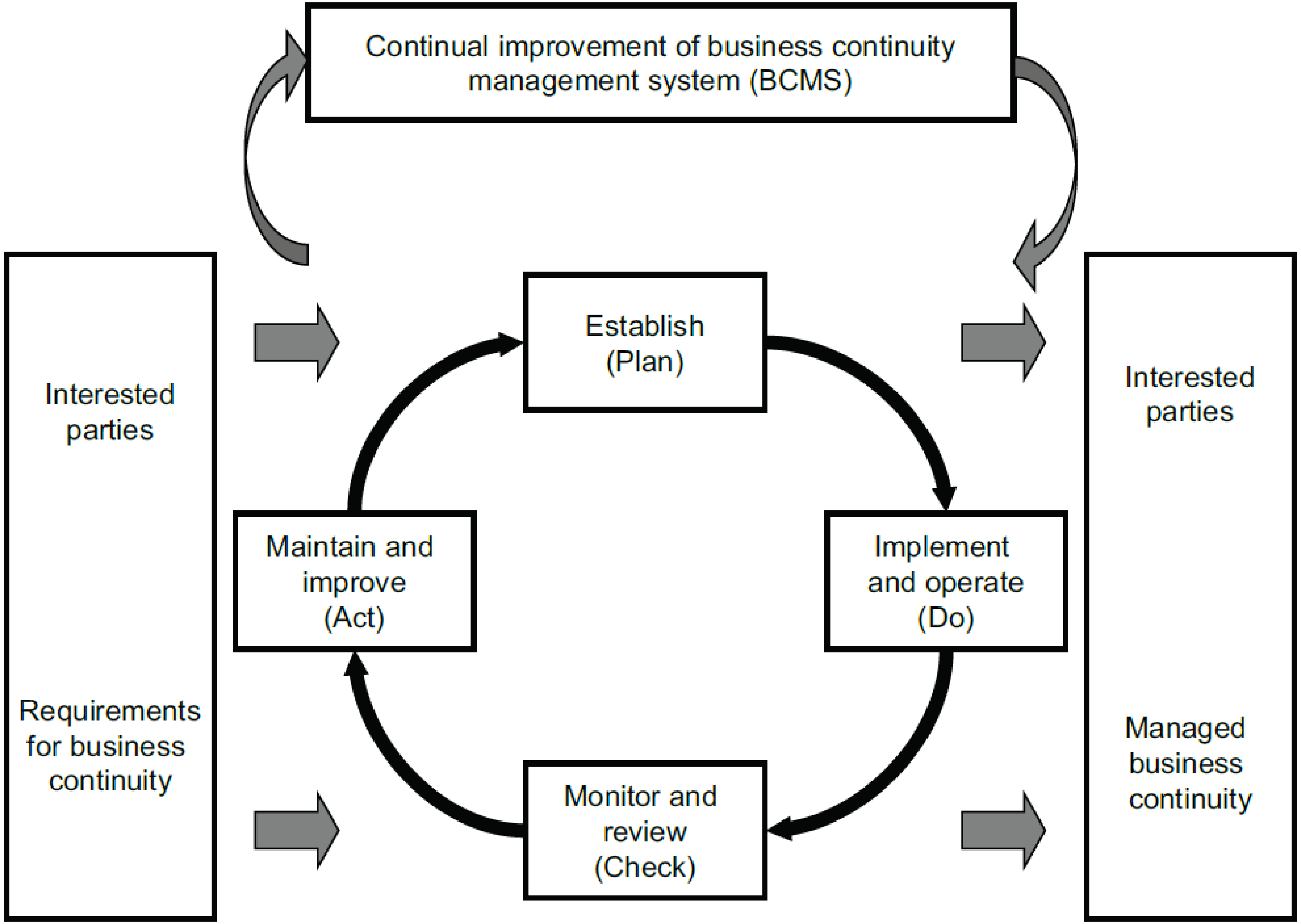
ISO 22301 *- Societal security - Business Continuity Management Systems – Requirements*

- 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

ISO 22301: Examples of Incidents to Consider

- Natural Disasters, Extreme Weather
- Fire,
- Interruption of Utility Supply,
- IT System Failure,
- Employee Health and Safety,
- Loss of Staff and Skills
- Data Breach,
- Cyber Attack,
- Theft or Malicious Damage,
- Terrorist Attack,
- Damage to Business Reputation,
- Supply Chain Disruption

PDCA model for BCMS



Continual improvement of business continuity management system (BCMS)

Interested parties

Requirements for business continuity

Establish (Plan)

Implement and operate (Do)

Monitor and review (Check)

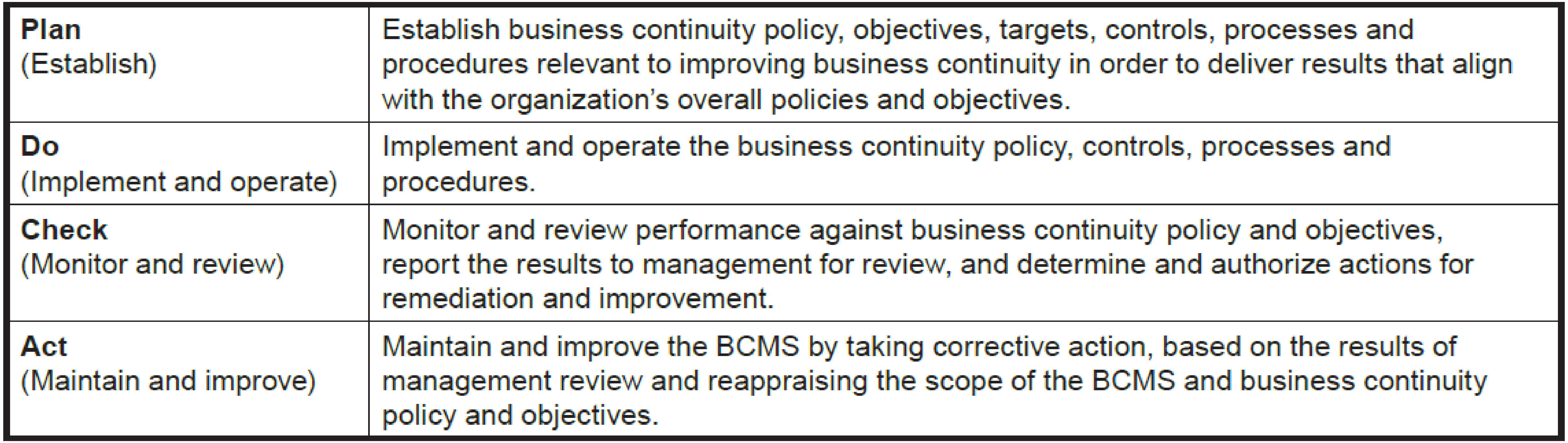
Maintain and improve (Act)

Interested parties

Managed business continuity

Wendy Ivins

PDCA model for BCMS



Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

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 … 1

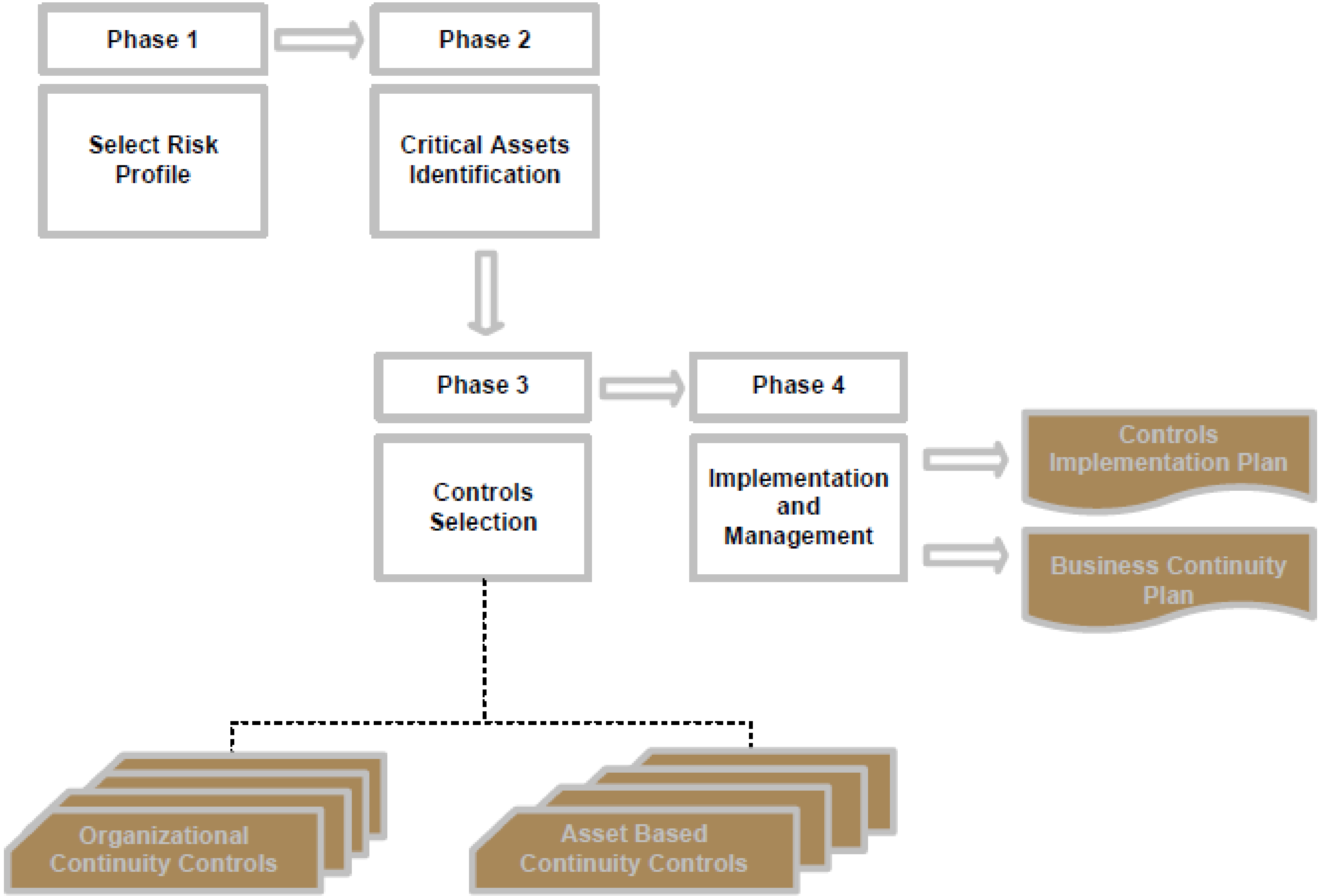
- Scope: identify the critical business functions of the organization to be protected
- Link to emergency management procedures and plans to ensure personnel safety.
- Identify critical ICT assets required to recover and sustain the minimum operating levels of the critical business functions in scope.
- 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 … 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

BCM approach: provide an acceptable (i.e. baseline) business continuity level with a low assessment and management effort.

ENISA’s BCM Process (OCTAVE ALLEGRO)

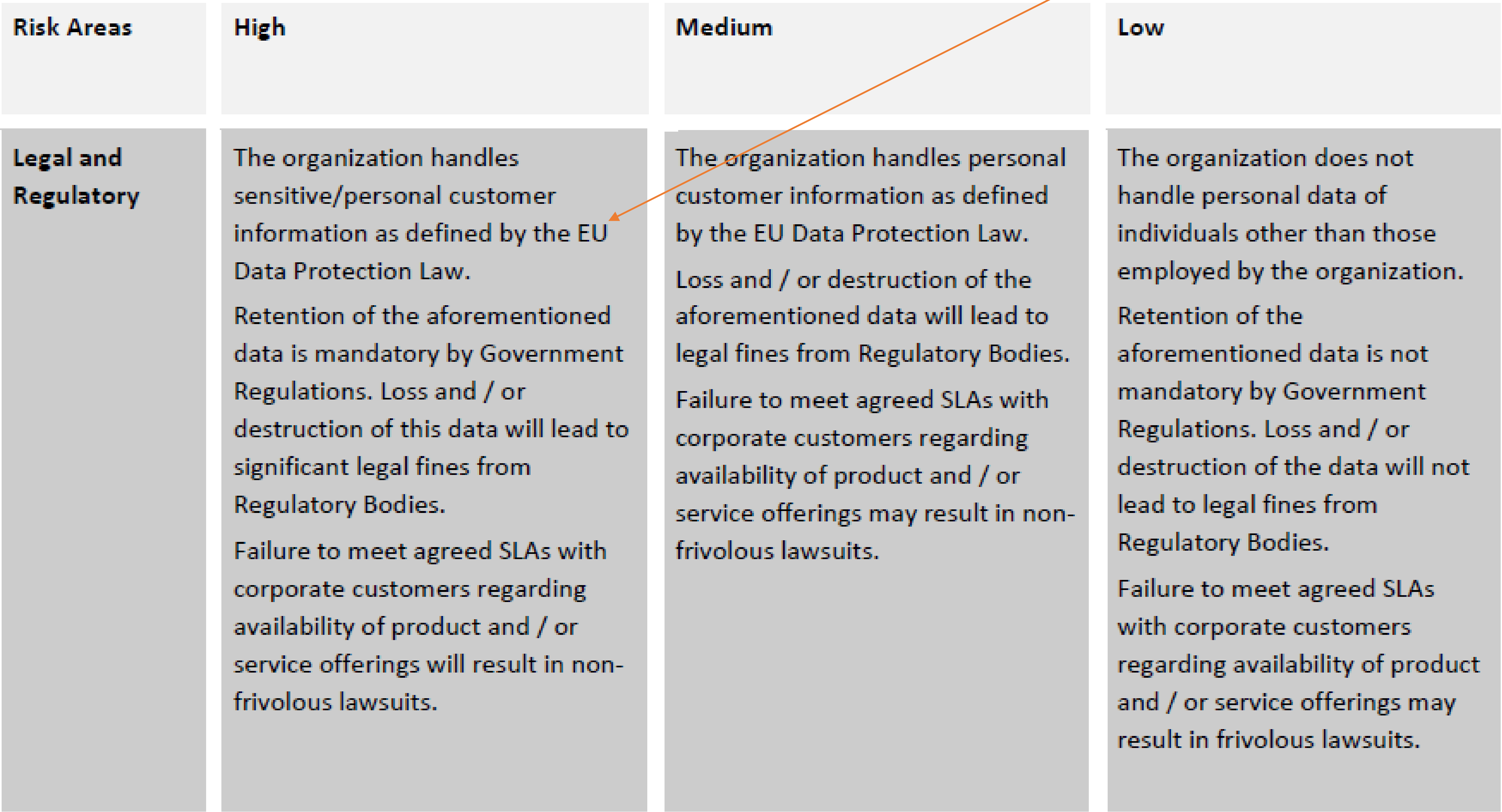

Phase 1
Select Risk Profile
Phase 2
Critical Assets Identification
Phase 3
Controls Selection
Phase 4
Implementation and Management
Controls Implementation Plan
Business Continuity Plan
Organizational Continuity Controls
Asset Based Continuity Controls

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

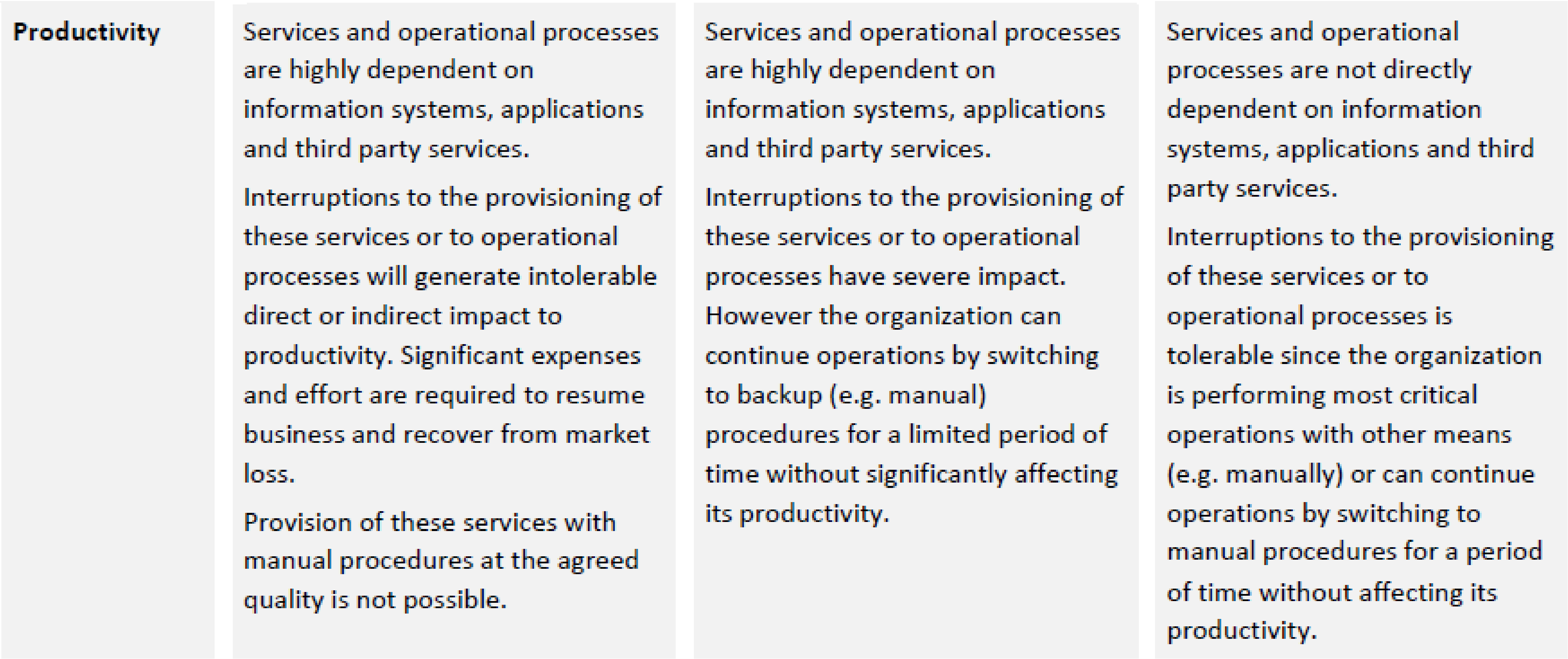
Phase 1: Select Risk Profile

GDPR



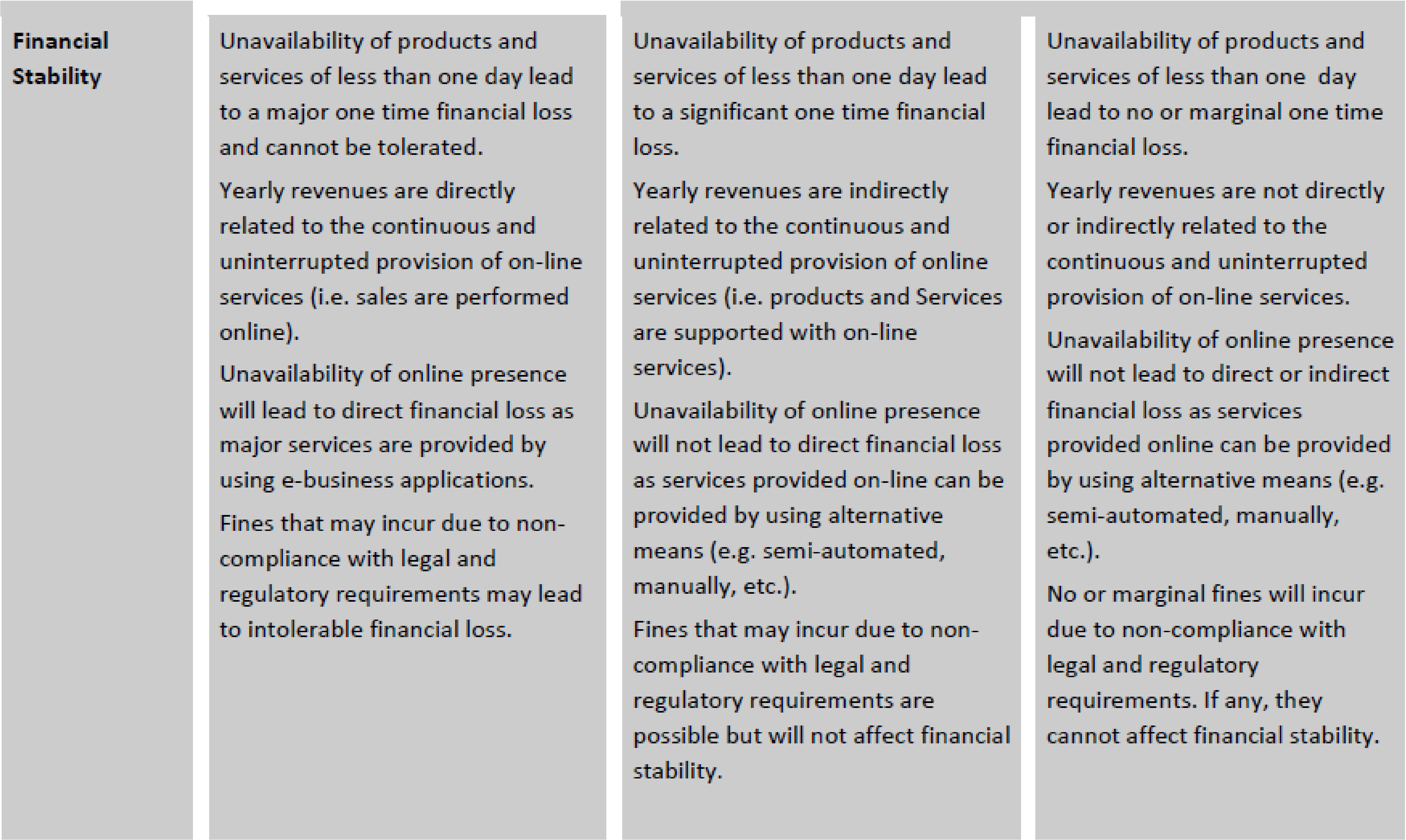
Risk Areas	High	Medium	Low
Legal and Regulatory	The organization handles sensitive/personal customer information as defined by the EU Data Protection Law. Retention of the aforementioned data is mandatory by Government Regulations. Loss and / or destruction of this data will lead to significant legal fines from Regulatory Bodies. Failure to meet agreed SLAs with corporate customers regarding availability of product and / or service offerings will result in non-frivolous lawsuits.	The organization handles personal customer information as defined by the EU Data Protection Law. Loss and / or destruction of the aforementioned data will lead to legal fines from Regulatory Bodies. Failure to meet agreed SLAs with corporate customers regarding availability of product and / or service offerings may result in non-frivolous lawsuits.	The organization does not handle personal data of individuals other than those employed by the organization. Retention of the aforementioned data is not mandatory by Government Regulations. Loss and / or destruction of the data will not lead to legal fines from Regulatory Bodies. Failure to meet agreed SLAs with corporate customers regarding availability of product and / or service offerings may result in frivolous lawsuits.

Phase 1: Select Risk Profile



Productivity	Services and operational processes are highly dependent on information systems, applications and third party services. Interruptions to the provisioning of these services or to operational processes will generate intolerable direct or indirect impact to productivity. Significant expenses and effort are required to resume business and recover from market loss. Provision of these services with manual procedures at the agreed quality is not possible.	Services and operational processes are highly dependent on information systems, applications and third party services. Interruptions to the provisioning of these services or to operational processes have severe impact. However the organization can continue operations by switching to backup (e.g. manual) procedures for a limited period of time without significantly affecting its productivity.	Services and operational processes are not directly dependent on information systems, applications and third party services. Interruptions to the provisioning of these services or to operational processes is tolerable since the organization is performing most critical operations with other means (e.g. manually) or can continue operations by switching to manual procedures for a period of time without affecting its productivity.

Phase 1: Select Risk Profile

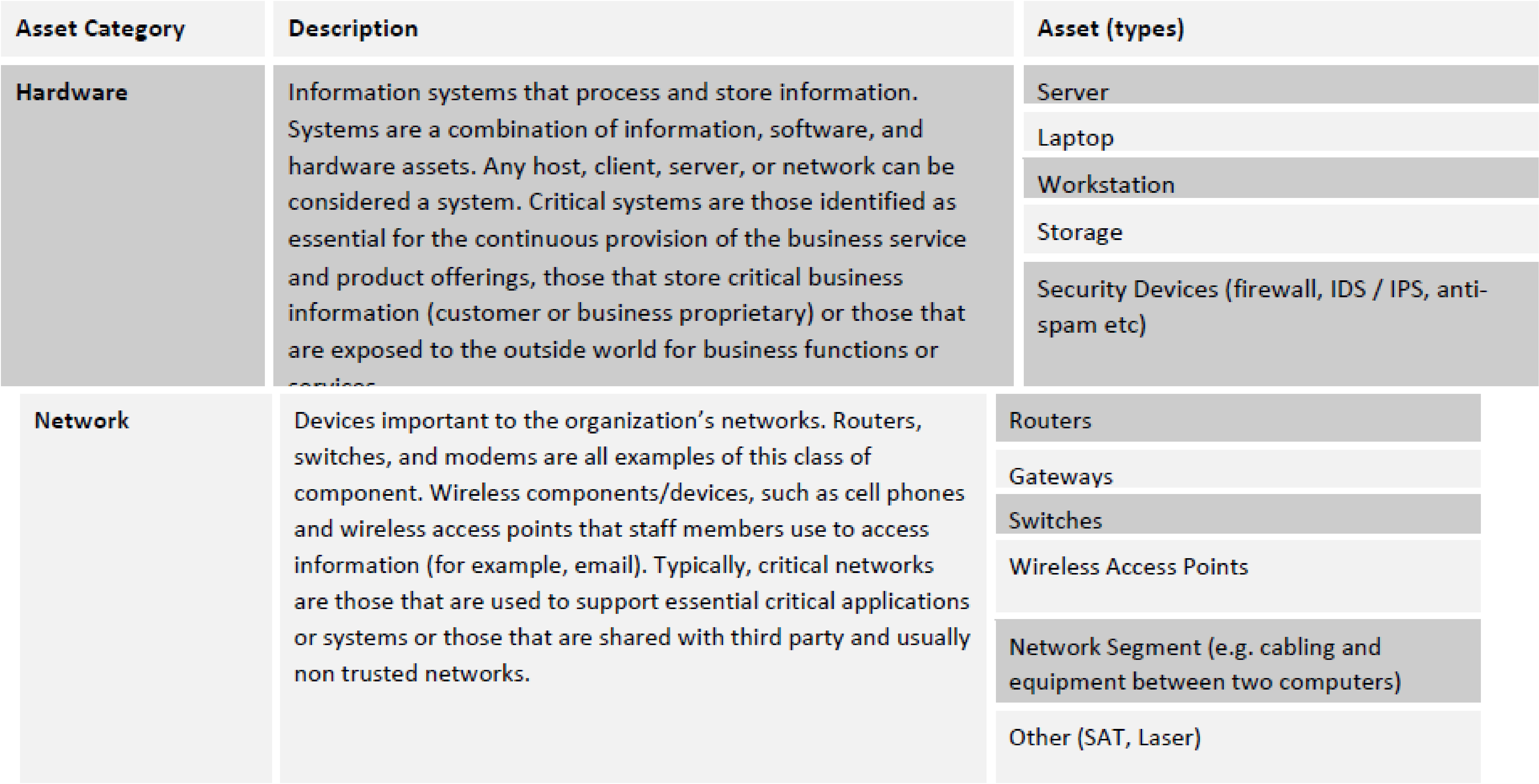


Financial Stability	Unavailability of products and services of less than one day lead to a major one time financial loss and cannot be tolerated. Yearly revenues are directly related to the continuous and uninterrupted provision of on-line services (i.e. sales are performed online). Unavailability of online presence will lead to direct financial loss as major services are provided by using e-business applications. Fines that may incur due to non-compliance with legal and regulatory requirements may lead to intolerable financial loss.	Unavailability of products and services of less than one day lead to a significant one time financial loss. Yearly revenues are indirectly related to the continuous and uninterrupted provision of online services (i.e. products and Services are supported with on-line services). Unavailability of online presence will not lead to direct financial loss as services provided on-line can be provided by using alternative means (e.g. semi-automated, manually, etc.). Fines that may incur due to non-compliance with legal and regulatory requirements are possible but will not affect financial stability.	Unavailability of products and services of less than one day lead to no or marginal one time financial loss. Yearly revenues are not directly or indirectly related to the continuous and uninterrupted provision of on-line services. Unavailability of online presence will not lead to direct or indirect financial loss as services provided online can be provided by using alternative means (e.g. semi-automated, manually, etc.). No or marginal fines will incur due to non-compliance with legal and regulatory requirements. If any, they cannot affect financial stability.

Phase 2: Critical Asset Identification

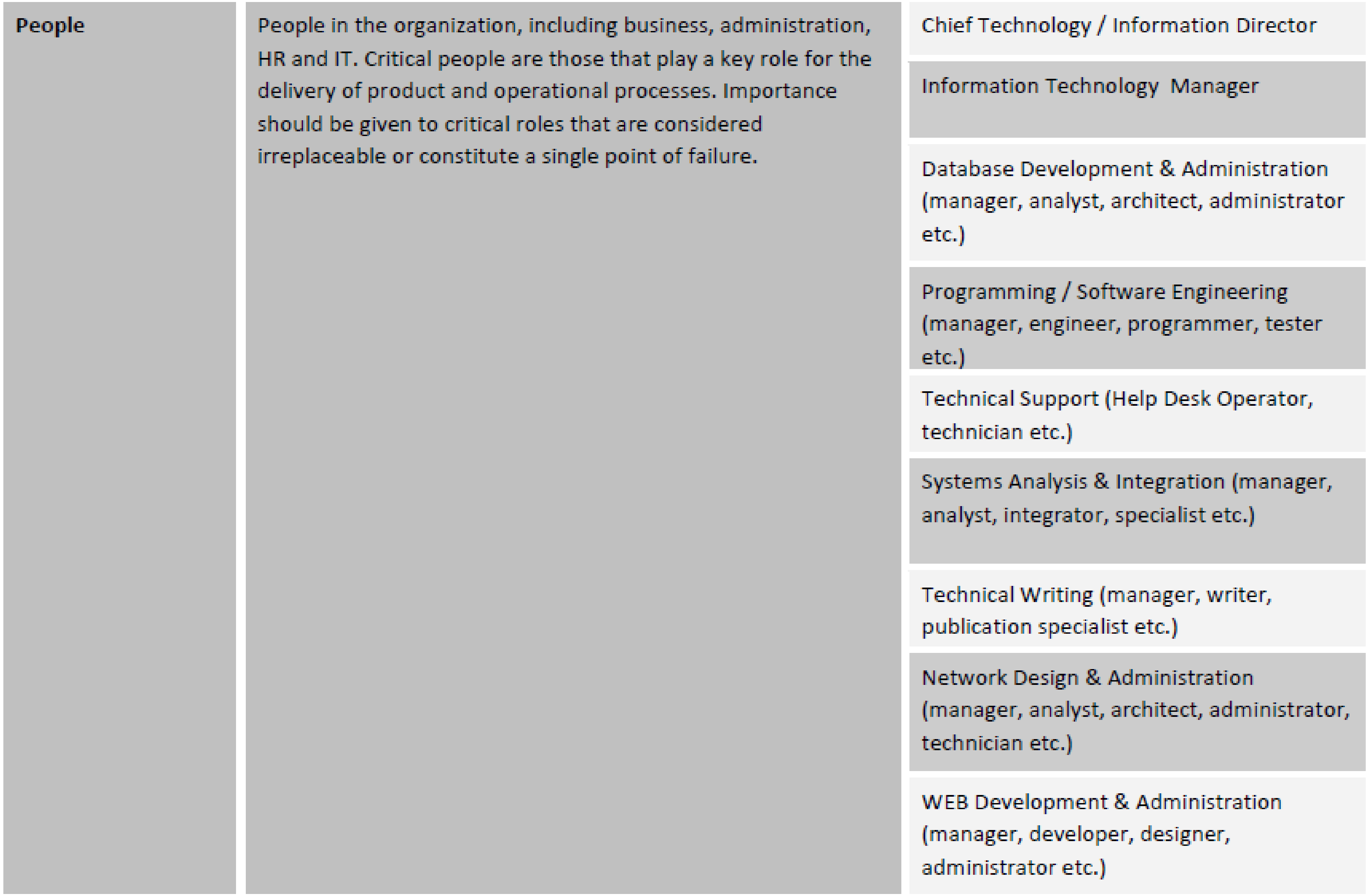
- Critical business functions: those whose interruption will lead to an **organisation suffering from serious financial, legal, and/or other damages or penalties.**
- Earliest possible recovery of such functions after a disruption is the main objective of a Business Continuity Plan
- **Together with 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 2: Asset types (… can change over time)



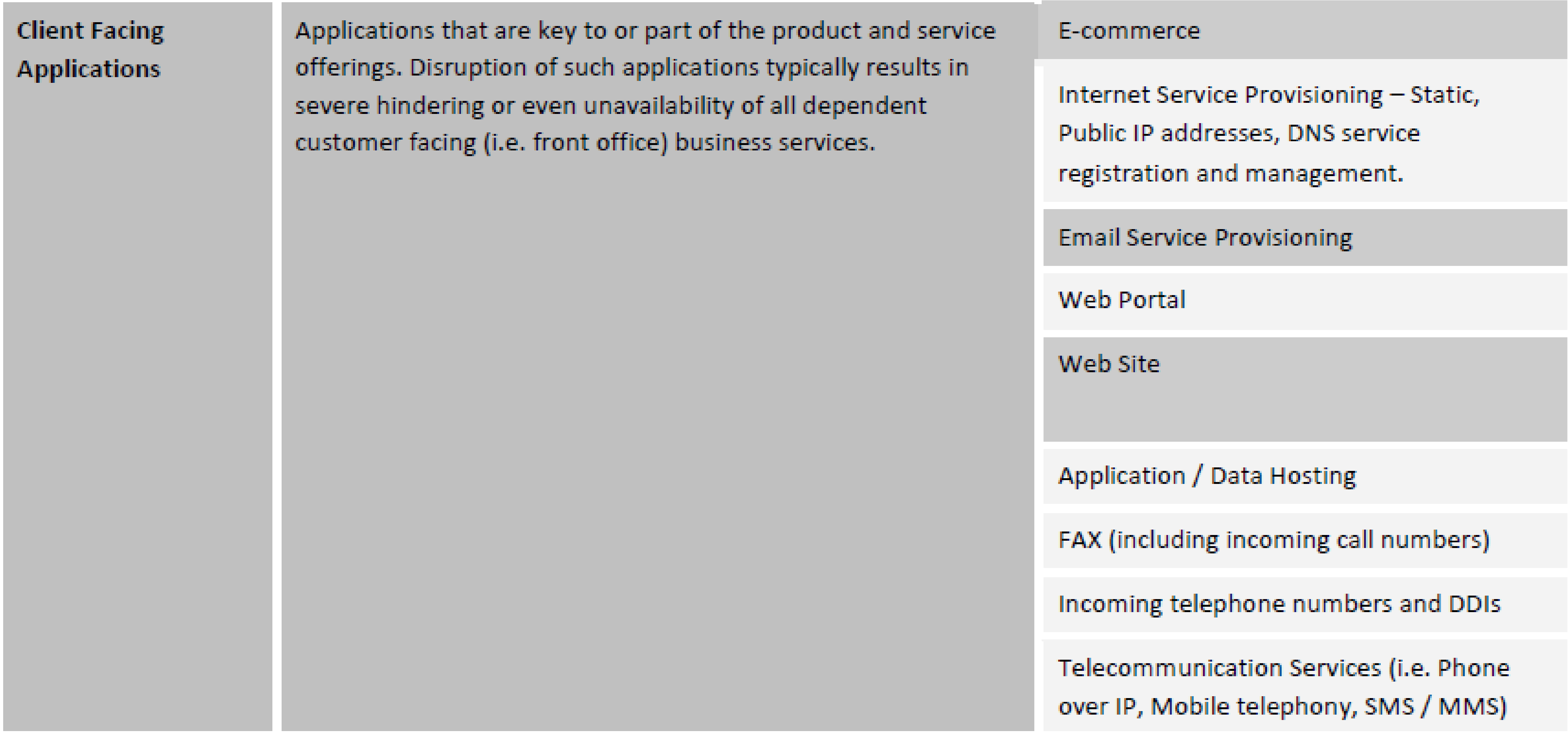
Asset Category	Description	Asset (types)
Hardware	Information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings, those that store critical business information (customer or business proprietary) or those that are exposed to the outside world for business functions or services	Server
		Laptop
		Workstation
		Storage
		Security Devices (firewall, IDS / IPS, anti-spam etc)
Network	Devices important to the organization’s networks. Routers, switches, and modems are all examples of this class of component. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with third party and usually non trusted networks.	Routers
		Gateways
		Switches
		Wireless Access Points
		Network Segment (e.g. cabling and equipment between two computers)
		Other (SAT, Laser)

Phase 2: Asset types (… can change over time)



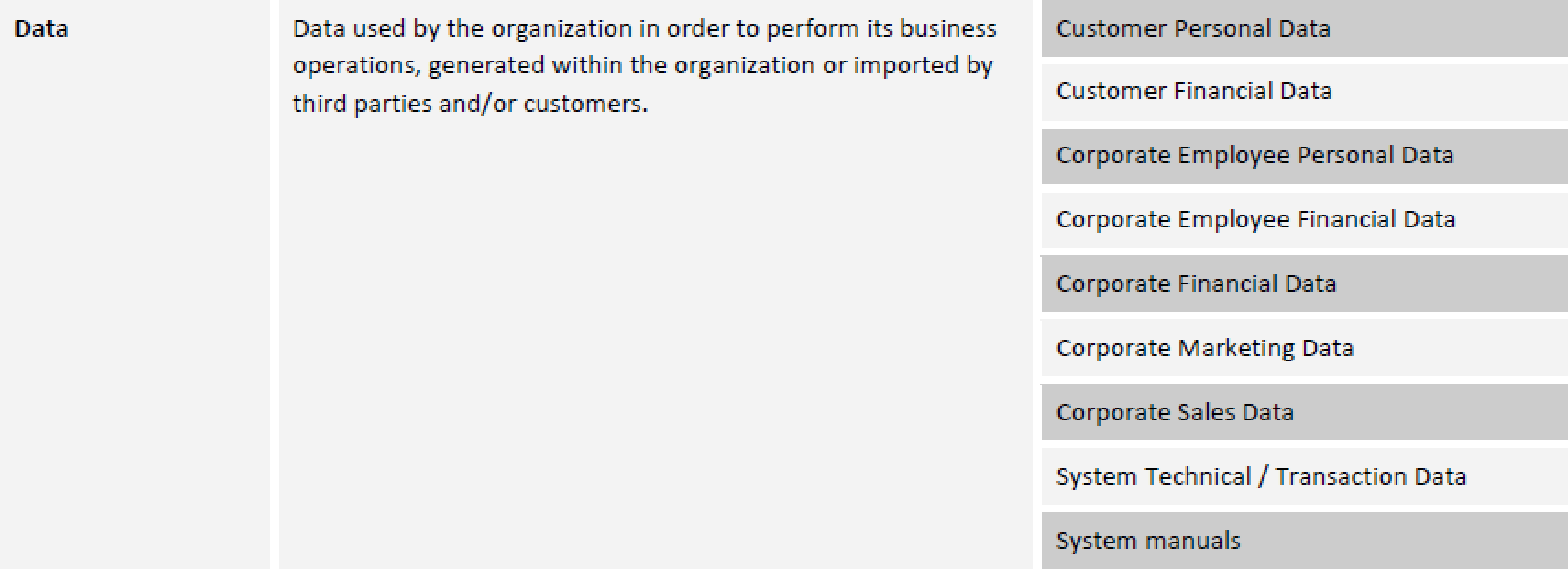
People	People in the organization, including business, administration, HR and IT. Critical people are those that play a key role for the delivery of product and operational processes. Importance should be given to critical roles that are considered irreplaceable or constitute a single point of failure.	Chief Technology / Information Director
		Information Technology Manager
		Database Development & Administration (manager, analyst, architect, administrator etc.)
		Programming / Software Engineering (manager, engineer, programmer, tester etc.)
		Technical Support (Help Desk Operator, technician etc.)
		Systems Analysis & Integration (manager, analyst, integrator, specialist etc.)
		Technical Writing (manager, writer, publication specialist etc.)
		Network Design & Administration (manager, analyst, architect, administrator, technician etc.)
		WEB Development & Administration (manager, developer, designer, administrator etc.)

Phase 2: Asset types (… can change over time)



Client Facing Applications	Applications that are key to or part of the product and service offerings. Disruption of such applications typically results in severe hindering or even unavailability of all dependent customer facing (i.e. front office) business services.	E-commerce
		Internet Service Provisioning – Static, Public IP addresses, DNS service registration and management.
		Email Service Provisioning
		Web Portal
		Web Site
		Application / Data Hosting
		FAX (including incoming call numbers)
		Incoming telephone numbers and DDIs
		Telecommunication Services (i.e. Phone over IP, Mobile telephony, SMS / MMS)

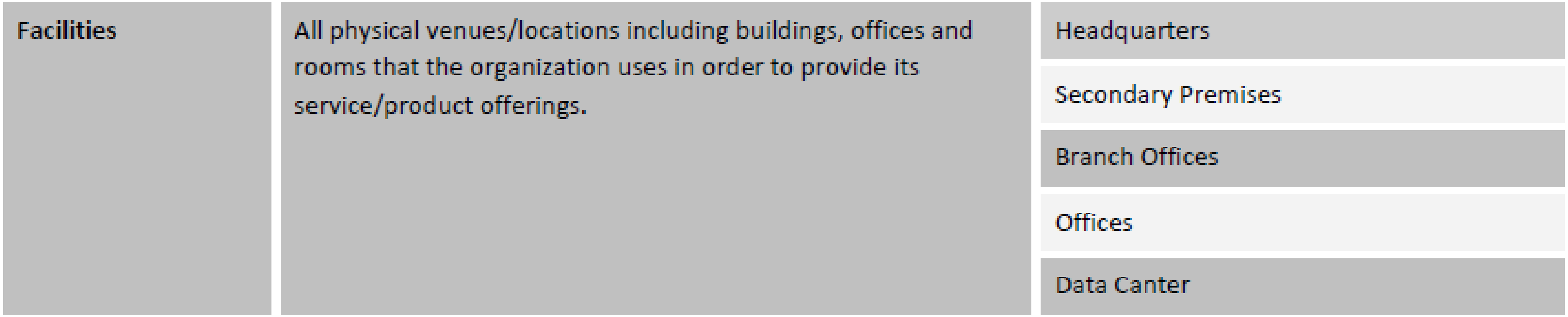
Phase 2: Asset types (... can change over time)



Data	Data used by the organization in order to perform its business operations, generated within the organization or imported by third parties and/or customers.	Customer Personal Data
		Customer Financial Data
		Corporate Employee Personal Data
		Corporate Employee Financial Data
		Corporate Financial Data
		Corporate Marketing Data
		Corporate Sales Data
		System Technical / Transaction Data
		System manuals

Most interesting and dynamic growth area.
How do you think this changes with the emerging use of AI algorithms?

Phase 2: Asset types (… can change over time)

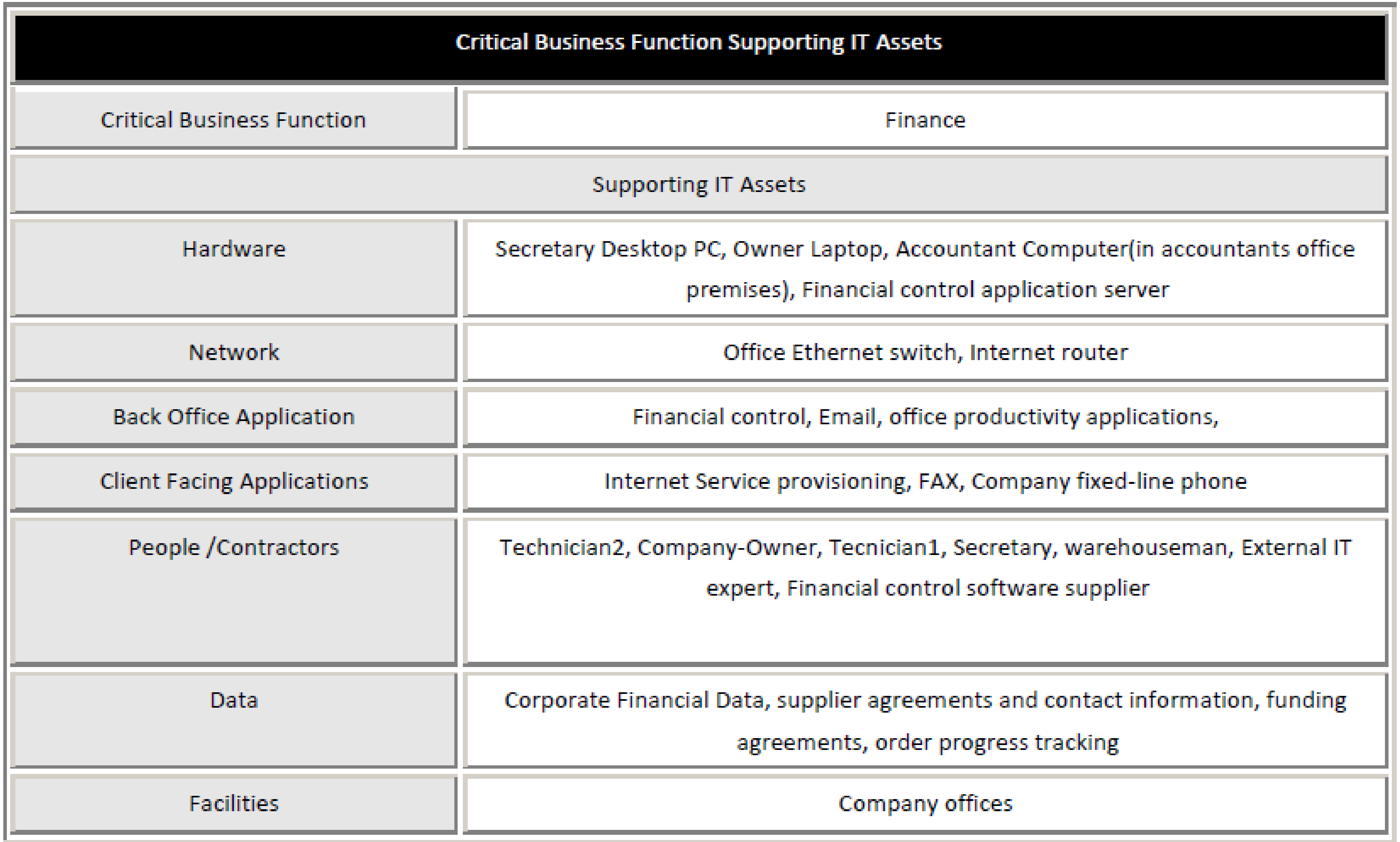


Facilities	All physical venues/locations including buildings, offices and rooms that the organization uses in order to provide its service/product offerings.	Headquarters
		Secondary Premises
		Branch Offices
		Offices
		Data Canter

How does location change with the emergence of Cloud computing?

Use of a combination of on-premises, Edge and Cloud environments.

Example: Finance function



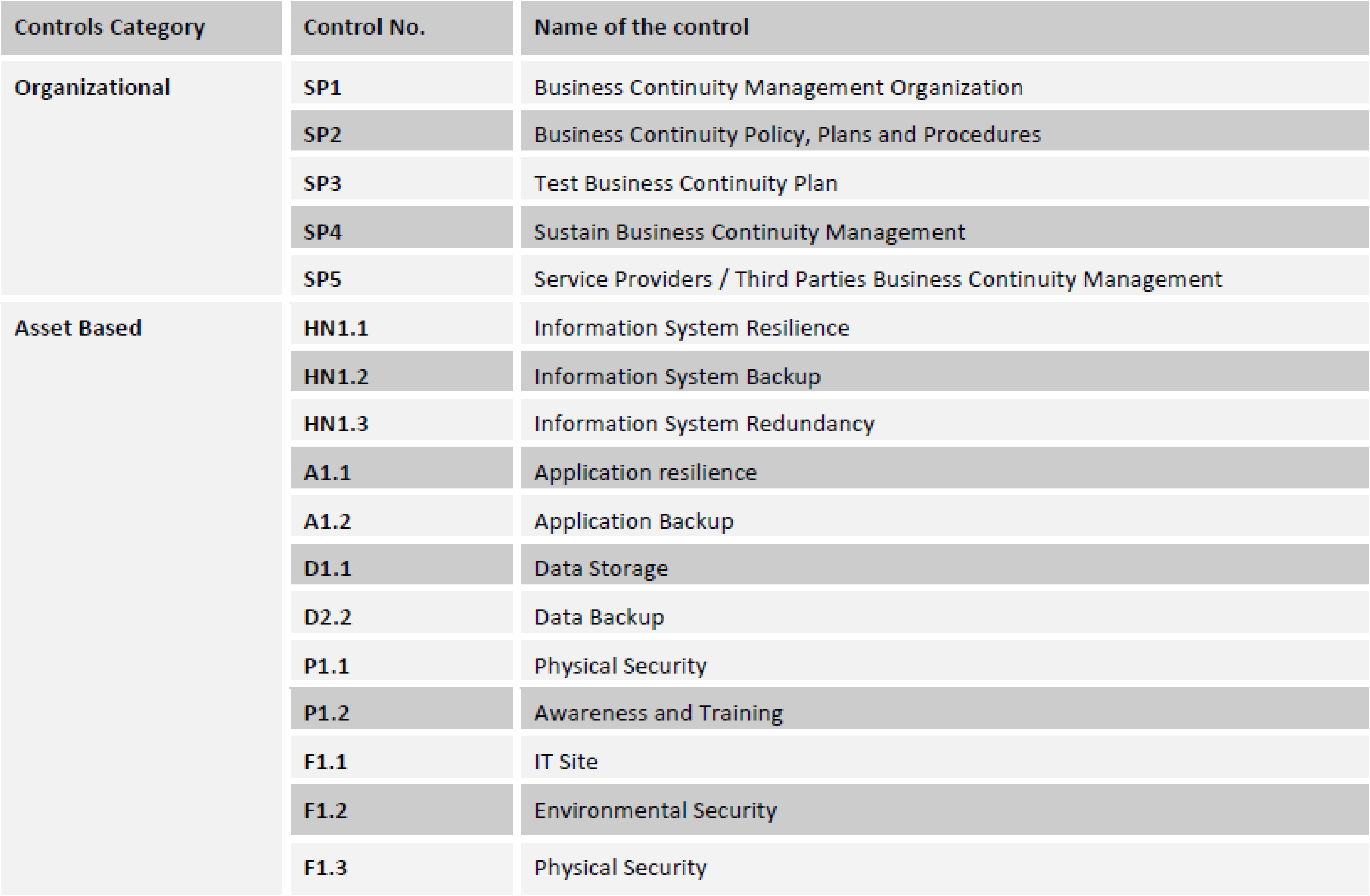
Critical Business Function Supporting IT Assets	
Critical Business Function	Finance
Supporting IT Assets	
Hardware	Secretary Desktop PC, Owner Laptop, Accountant Computer(in accountants office premises), Financial control application server
Network	Office Ethernet switch, Internet router
Back Office Application	Financial control, Email, office productivity applications,
Client Facing Applications	Internet Service provisioning, FAX, Company fixed-line phone
People /Contractors	Technician2, Company-Owner, Tecnician1, Secretary, warehouseman, External IT expert, Financial control software supplier
Data	Corporate Financial Data, supplier agreements and contact information, funding agreements, order progress tracking
Facilities	Company offices

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

- **Organizational controls**: contain controls concerned with practices and management procedures
- **Asset control**: applicable to categories of critical assets. Control cards are essentially pre-selected and grouped according to risk profiles and asset recovery priority.

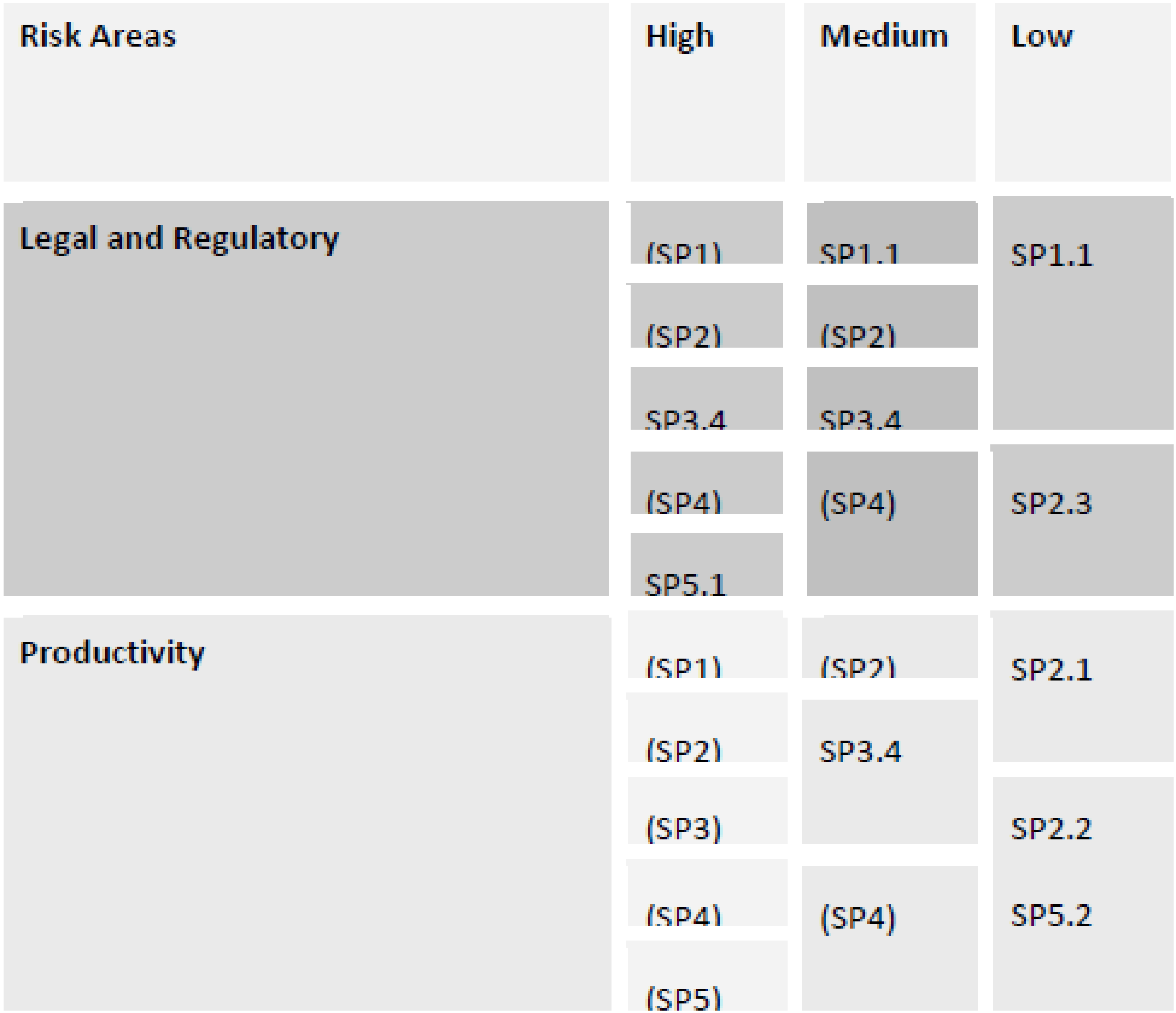
Mapping of Risk to Controls

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



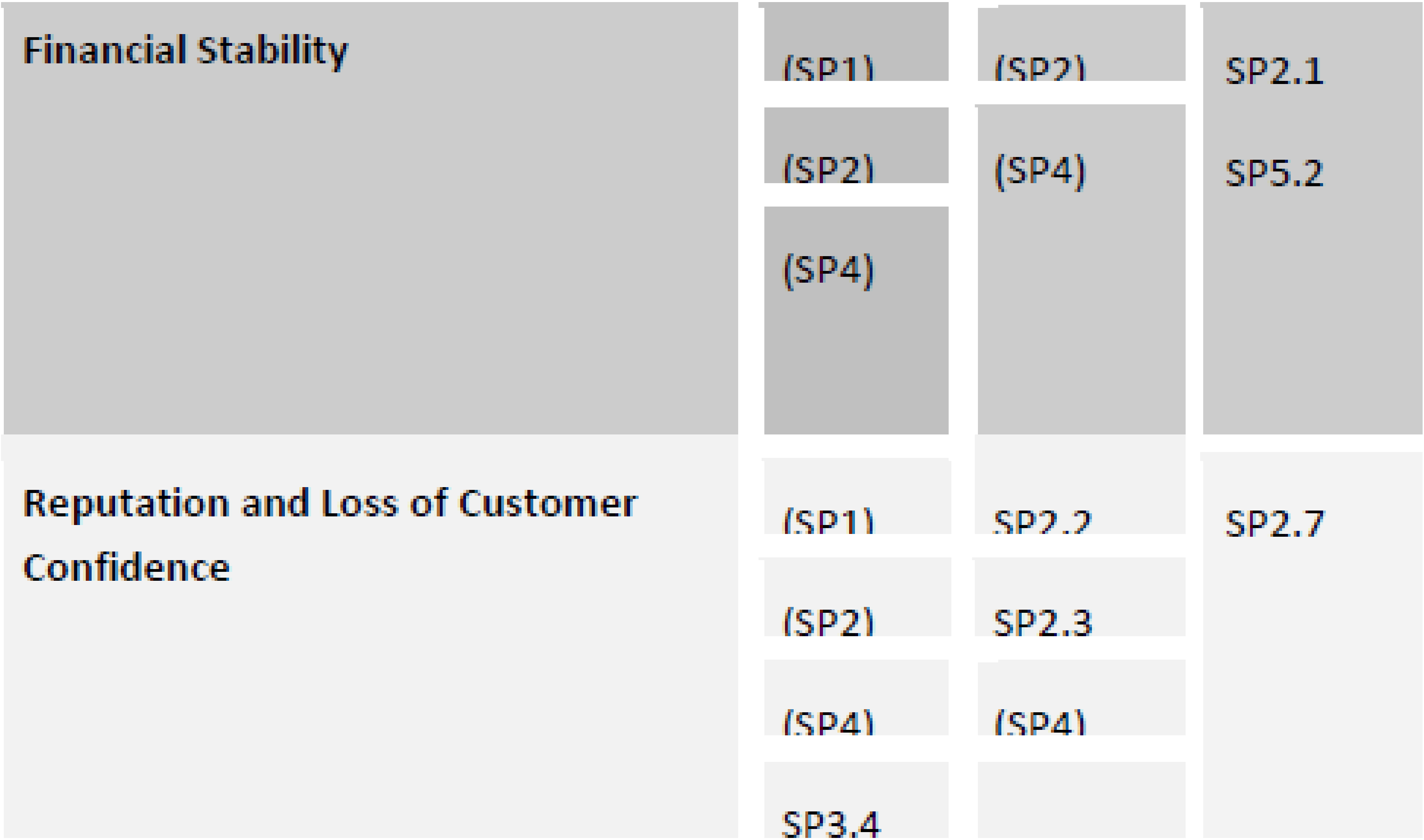
Controls Category	Control No.	Name of the control
Organizational	SP1	Business Continuity Management Organization
	SP2	Business Continuity Policy, Plans and Procedures
	SP3	Test Business Continuity Plan
	SP4	Sustain Business Continuity Management
	SP5	Service Providers / Third Parties Business Continuity Management
Asset Based	HN1.1	Information System Resilience
	HN1.2	Information System Backup
	HN1.3	Information System Redundancy
	A1.1	Application resilience
	A1.2	Application Backup
	D1.1	Data Storage
	D2.2	Data Backup
	P1.1	Physical Security
	P1.2	Awareness and Training
	F1.1	IT Site
	F1.2	Environmental Security
	F1.3	Physical Security

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



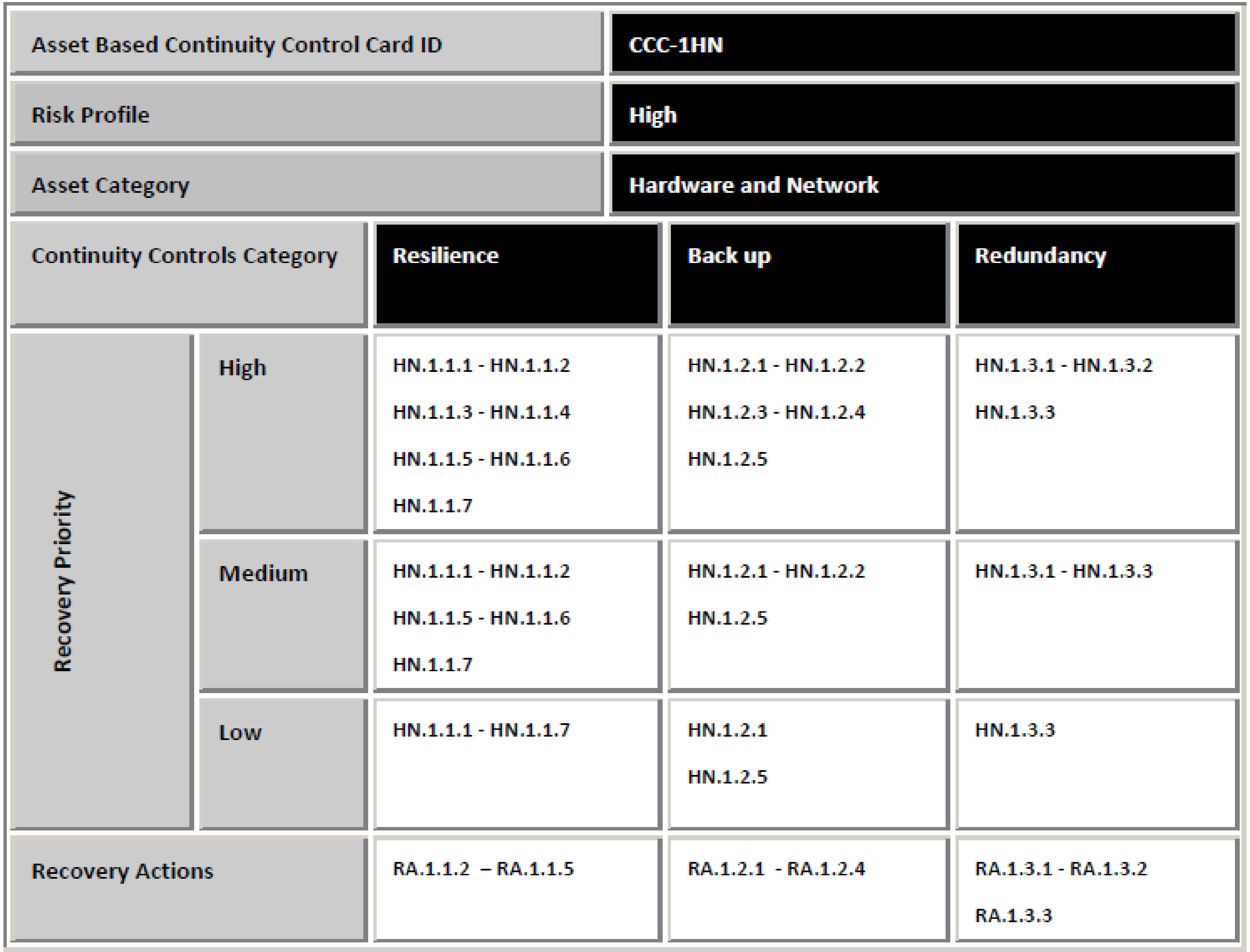
Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1) (SP2) SP3.4 (SP4) SP5.1	SP1.1 (SP2) SP3.4 (SP4)	SP1.1 SP2.3
Productivity	(SP1) (SP2) (SP3) (SP4) (SP5)	(SP2) SP3.4 (SP4)	SP2.1 SP2.2 SP5.2

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



Financial Stability	(SP1) (SP2) (SP4)	(SP2) (SP4)	SP2.1 SP5.2
Reputation and Loss of Customer Confidence	(SP1) (SP2) (SP4) SP3.4	SP2.2 SP2.3 (SP4)	SP2.7

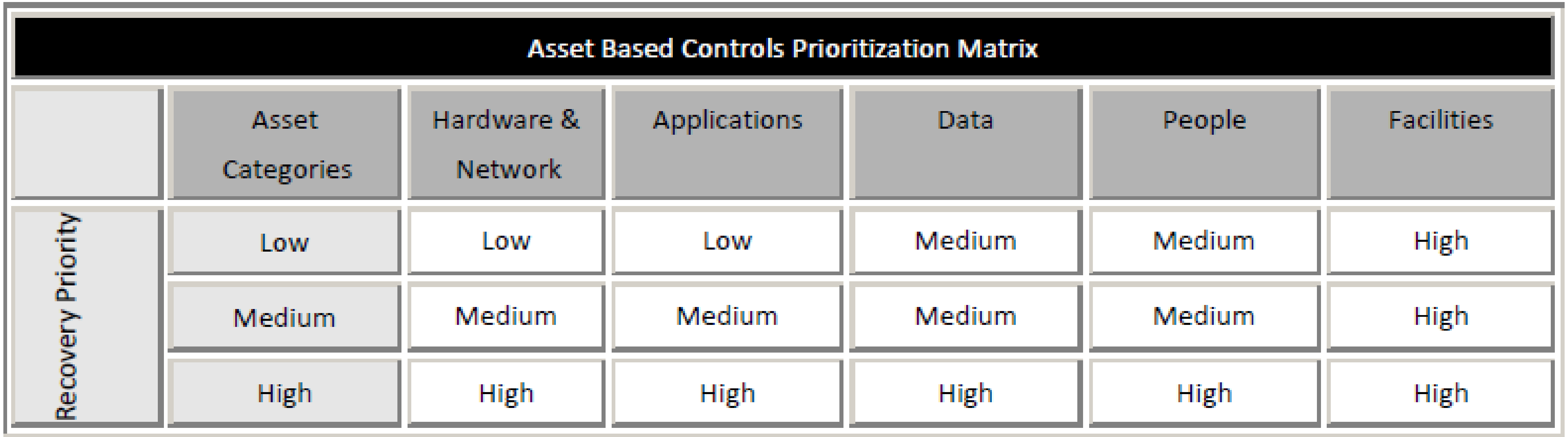
Phase 3: Asset continuity control cards (CCC)



Asset Based Continuity Control Card ID		CCC-1HN		
Risk Profile		High		
Asset Category		Hardware and Network		
Continuity Controls Category		Resilience	Back up	Redundancy
Recovery Priority	High	HN.1.1.1 - HN.1.1.2 HN.1.1.3 - HN.1.1.4 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.3 - HN.1.2.4 HN.1.2.5	HN.1.3.1 - HN.1.3.2 HN.1.3.3
	Medium	HN.1.1.1 - HN.1.1.2 HN.1.1.5 - HN.1.1.6 HN.1.1.7	HN.1.2.1 - HN.1.2.2 HN.1.2.5	HN.1.3.1 - HN.1.3.3
	Low	HN.1.1.1 - HN.1.1.7	HN.1.2.1 HN.1.2.5	HN.1.3.3
Recovery Actions		RA.1.1.2 – RA.1.1.5	RA.1.2.1 - RA.1.2.4	RA.1.3.1 - RA.1.3.2 RA.1.3.3

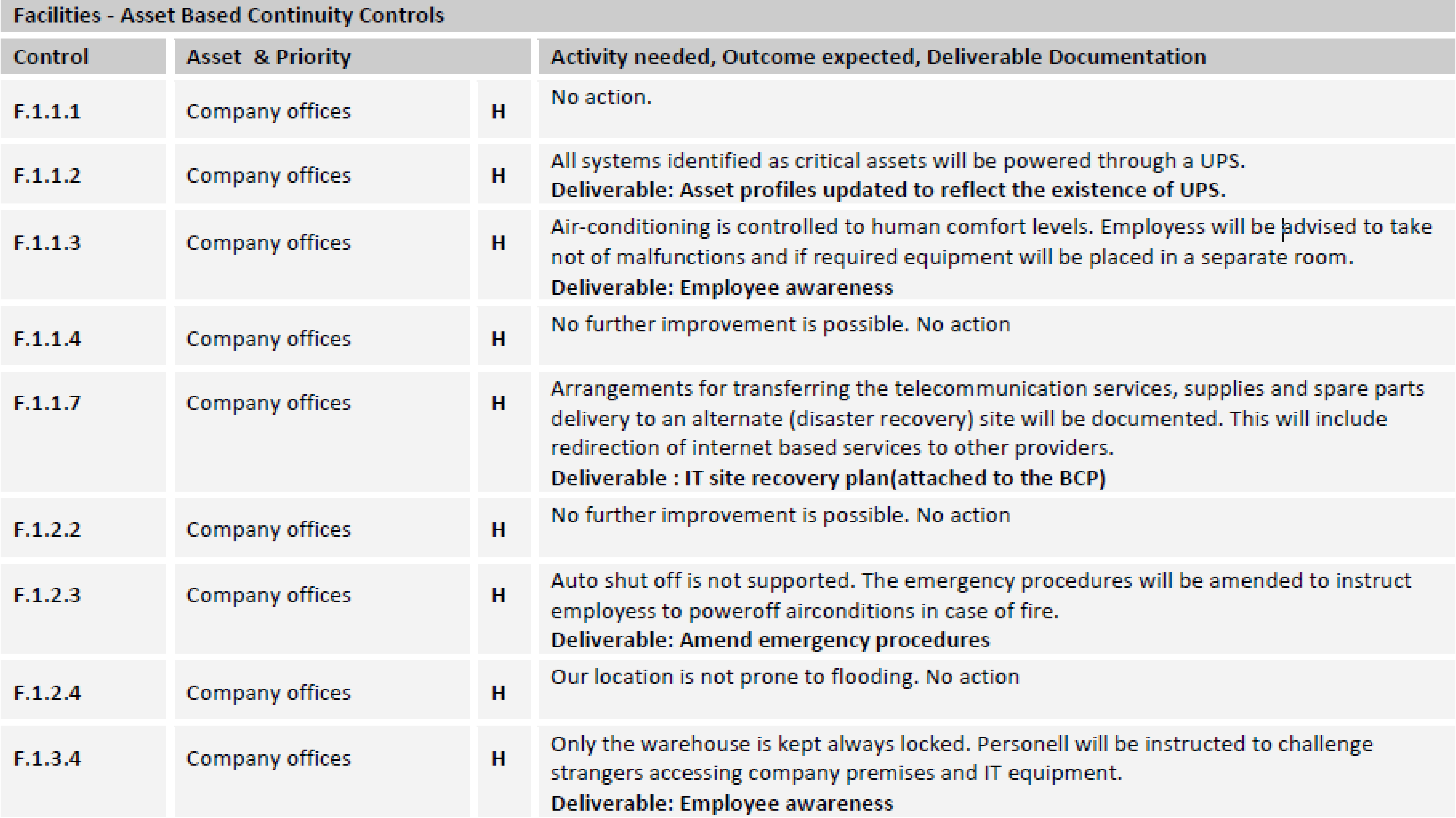
Phase 4: Implementation plan …

- 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



Asset Based Controls Prioritization Matrix

	Asset Categories	Hardware & Network	Applications	Data	People	Facilities
Recovery Priority	Low	Low	Low	Medium	Medium	High
	Medium	Medium	Medium	Medium	Medium	High
	High	High	High	High	High	High

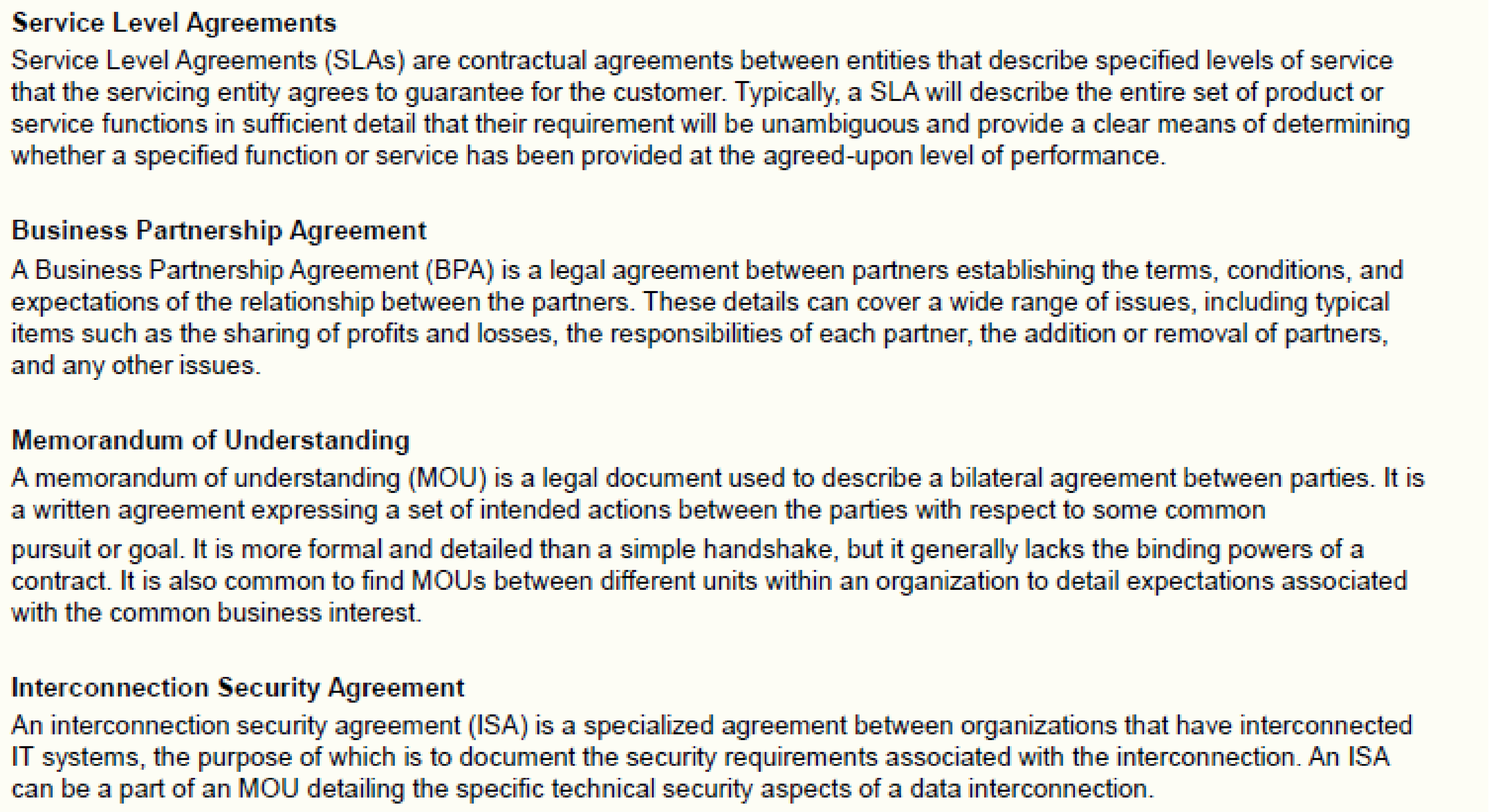


Facilities - Asset Based Continuity Controls			
Control	**Asset & Priority**		**Activity needed, Outcome expected, Deliverable Documentation**
F.1.1.1	Company offices	**H**	No action.
F.1.1.2	Company offices	**H**	All systems identified as critical assets will be powered through a UPS. **Deliverable: Asset profiles updated to reflect the existence of UPS.**
F.1.1.3	Company offices	**H**	Air-conditioning is controlled to human comfort levels. Employess will be advised to take not of malfunctions and if required equipment will be placed in a separate room. **Deliverable: Employee awareness**
F.1.1.4	Company offices	**H**	No further improvement is possible. No action
F.1.1.7	Company offices	**H**	Arrangements for transferring the telecommunication services, supplies and spare parts delivery to an alternate (disaster recovery) site will be documented. This will include redirection of internet based services to other providers. **Deliverable : IT site recovery plan(attached to the BCP)**
F.1.2.2	Company offices	**H**	No further improvement is possible. No action
F.1.2.3	Company offices	**H**	Auto shut off is not supported. The emergency procedures will be amended to instruct employess to poweroff airconditions in case of fire. **Deliverable: Amend emergency procedures**
F.1.2.4	Company offices	**H**	Our location is not prone to flooding. No action
F.1.3.4	Company offices	**H**	Only the warehouse is kept always locked. Personell will be instructed to challenge strangers accessing company premises and IT equipment. **Deliverable: Employee awareness**

BC Controls Implementation Plan

Control	Responsible	External support required	Milestones Mm/Dd	Implementation Priority
SP.1.1	Company Owner	No		Low
SP2.1	Technician1	External IT Expert and the Assessment team		Low
SP2.2	Technician1	External IT Expert		Low
SP2.3	WarehouseMan	No		Low
SP2.7	SalesMan1	External IT Expert		Medium
SP5.2	SalesMan1	External IT Expert		Medium
HN.1.1.1	Technician1	External IT Expert		
HN.1.1.5	Technician1	No		
HN.1.1.7	Technician1	External IT Expert		
HN.1.2.1	Technician1	External IT Expert		
HN.1.2.5	Technician1			
HN.1.3.3	SalesMan2			

External Agreements – key for outsourcing



Service Level Agreements

Service Level Agreements (SLAs) are contractual agreements between entities that describe specified levels of service that the servicing entity agrees to guarantee for the customer. Typically, a SLA will describe the entire set of product or service functions in sufficient detail that their requirement will be unambiguous and provide a clear means of determining whether a specified function or service has been provided at the agreed-upon level of performance.

Business Partnership Agreement

A Business Partnership Agreement (BPA) is a legal agreement between partners establishing the terms, conditions, and expectations of the relationship between the partners. These details can cover a wide range of issues, including typical items such as the sharing of profits and losses, the responsibilities of each partner, the addition or removal of partners, and any other issues.

Memorandum of Understanding

A memorandum of understanding (MOU) is a legal document used to describe a bilateral agreement between parties. It is a written agreement expressing a set of intended actions between the parties with respect to some common pursuit or goal. It is more formal and detailed than a simple handshake, but it generally lacks the binding powers of a contract. It is also common to find MOUs between different units within an organization to detail expectations associated with the common business interest.

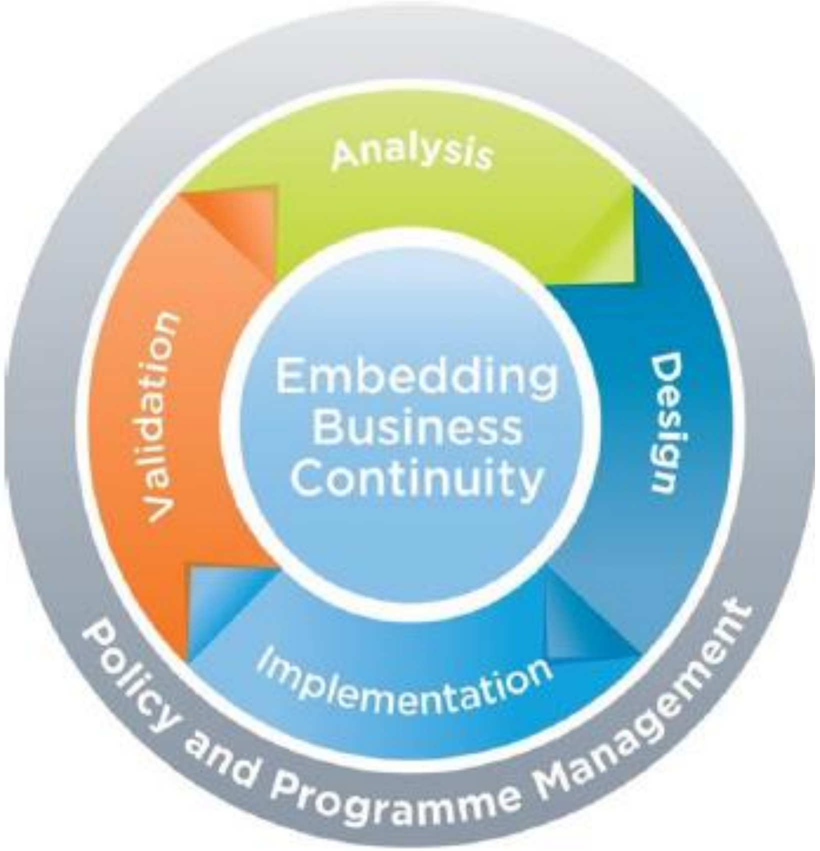
Interconnection Security Agreement

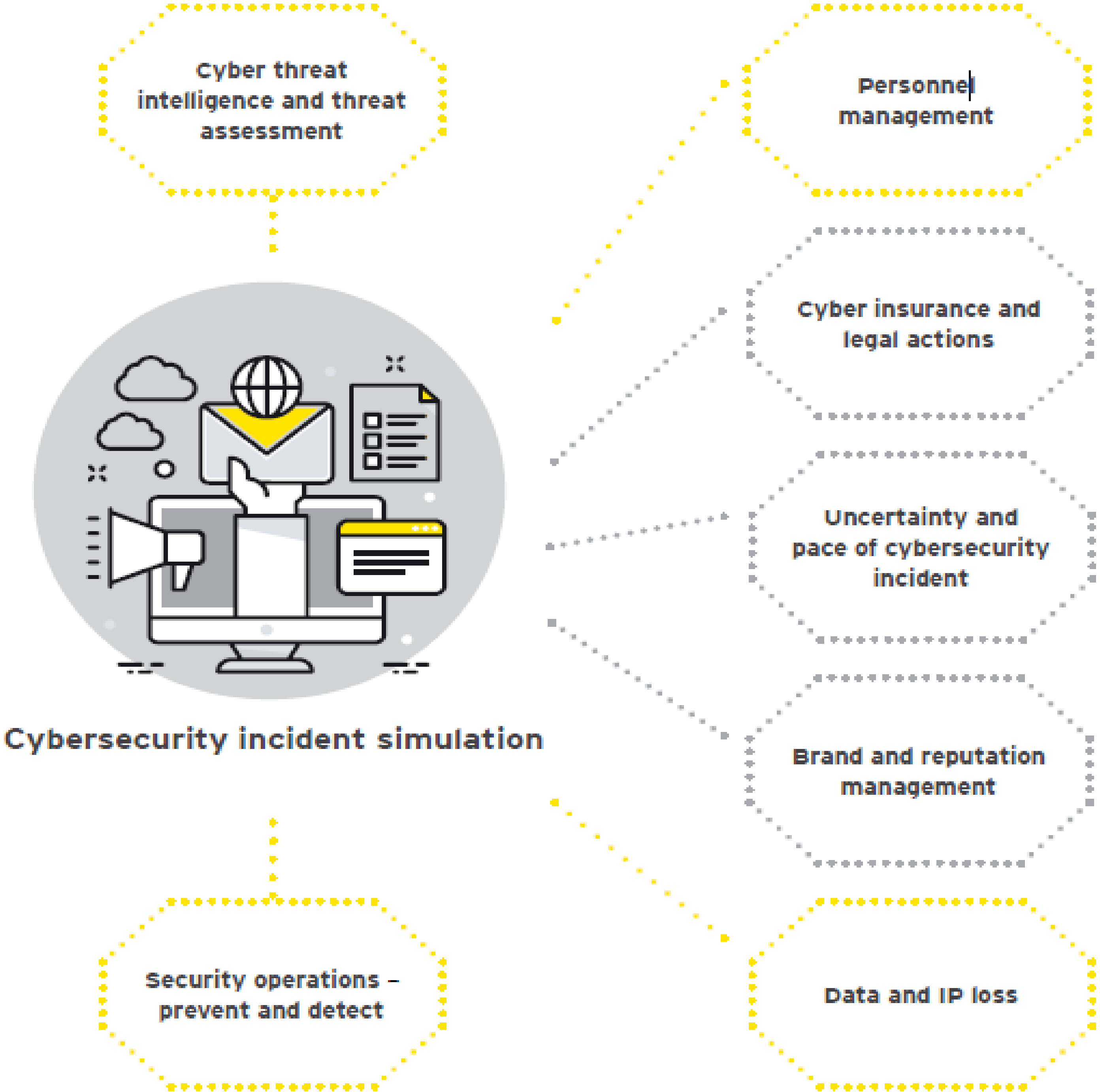
An interconnection security agreement (ISA) is a specialized agreement between organizations that have interconnected IT systems, the purpose of which is to document the security requirements associated with the interconnection. An ISA can be a part of an MOU detailing the specific technical security aspects of a data interconnection.

Conklin et al. Principles of Computer Security. 4th Ed., 2016 pp. 58

Integrating BCM & Cybersecurity (from PwC)

- Is the BCP program team a cyber security threat?
- Appropriate security measures included in BC Plan – including physical security for facilities and security over data?
- Consider security in IT recovery strategy & cyber consideration when selecting a 3rd party (e.g. cloud migration)


Analysis
Design
Implementation
Validation
Embedding Business Continuity
Policy and Programme Management



Cyber threat intelligence and threat assessment

Cybersecurity incident simulation

Security operations – prevent and detect

Personnel management

Cyber insurance and legal actions

Uncertainty and pace of cybersecurity incident

Brand and reputation management

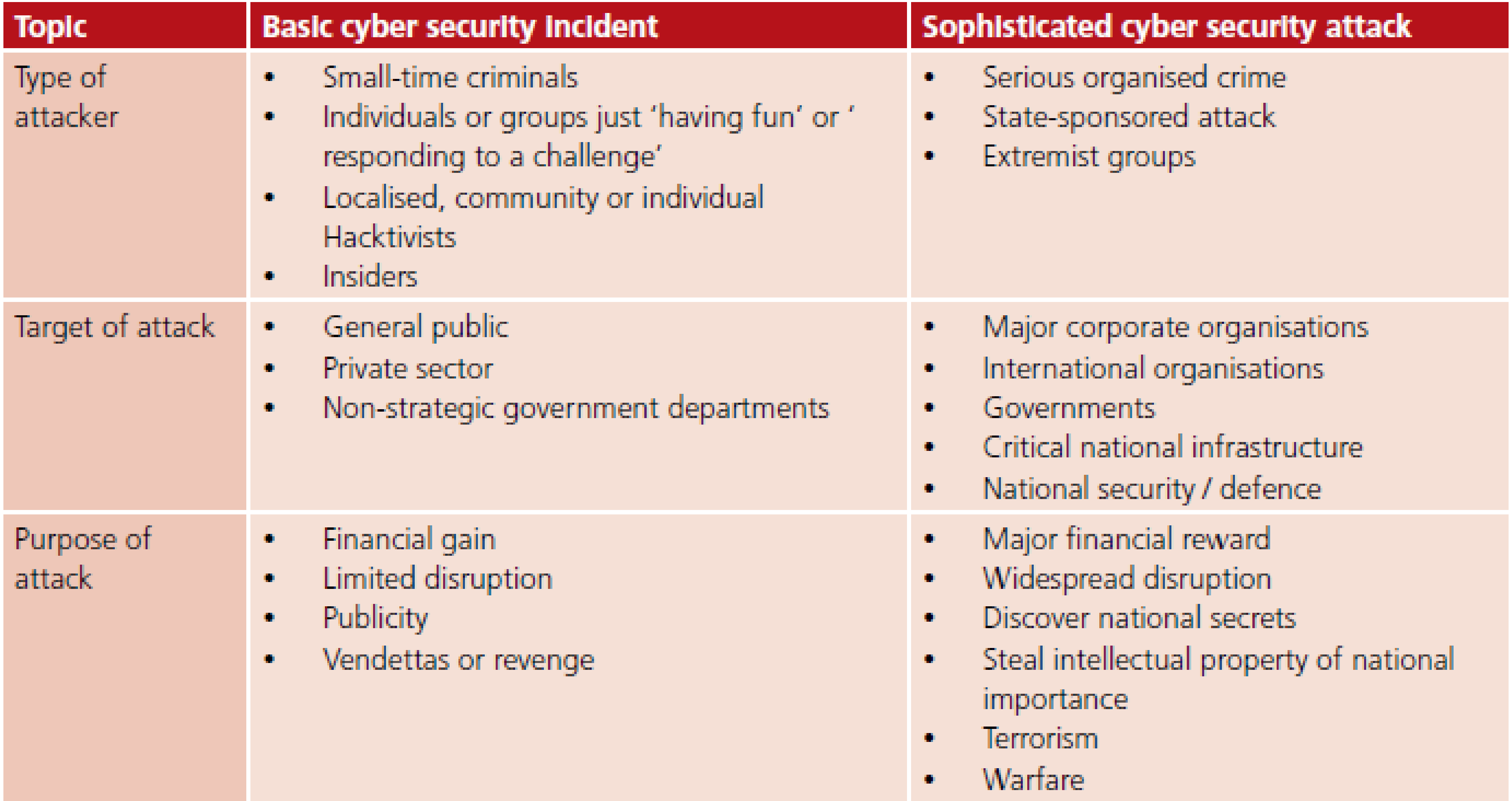
Data and IP loss

Cybersecurity Business Continuity Simulation

(EY)

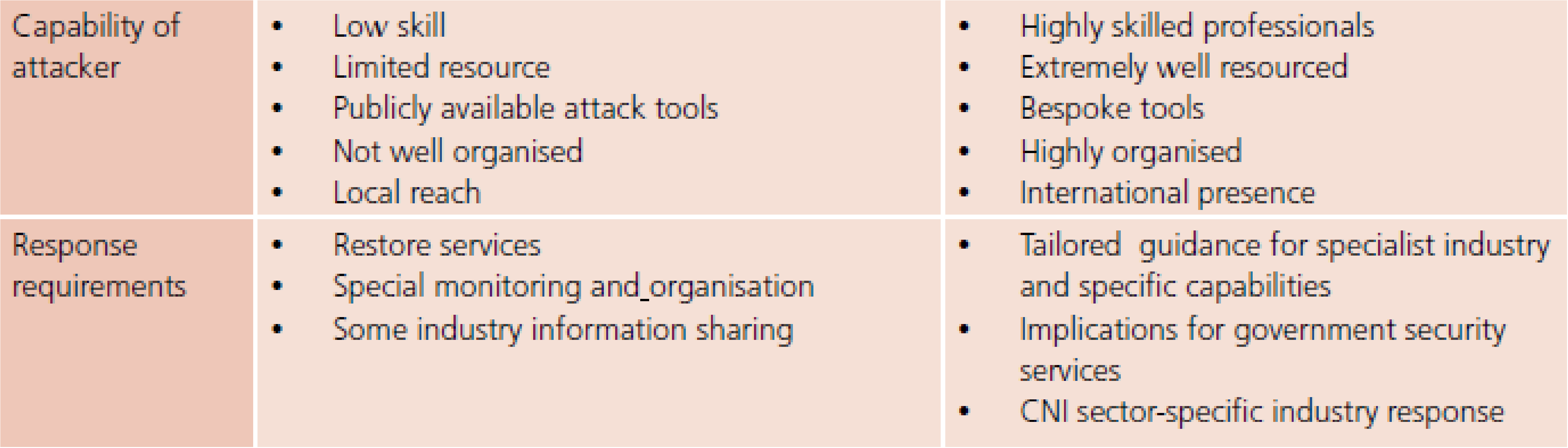
Attacker Models

Cyber Security Incident Response Guide (CREST)



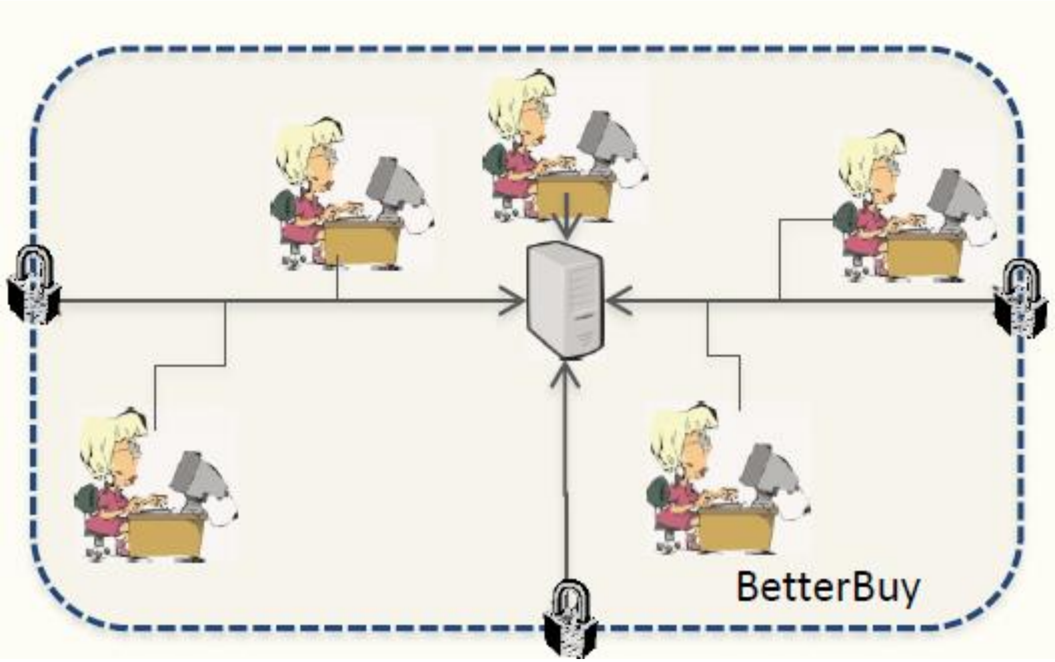
Topic	Basic cyber security incident	Sophisticated cyber security attack
Type of attacker	• Small-time criminals • Individuals or groups just ‘having fun’ or ‘ responding to a challenge’ • Localised, community or individual Hacktivists • Insiders	• Serious organised crime • State-sponsored attack • Extremist groups
Target of attack	• General public • Private sector • Non-strategic government departments	• Major corporate organisations • International organisations • Governments • Critical national infrastructure • National security / defence
Purpose of attack	• Financial gain • Limited disruption • Publicity • Vendettas or revenge	• Major financial reward • Widespread disruption • Discover national secrets • Steal intellectual property of national importance • Terrorism • Warfare

Attacker Models (CREST)

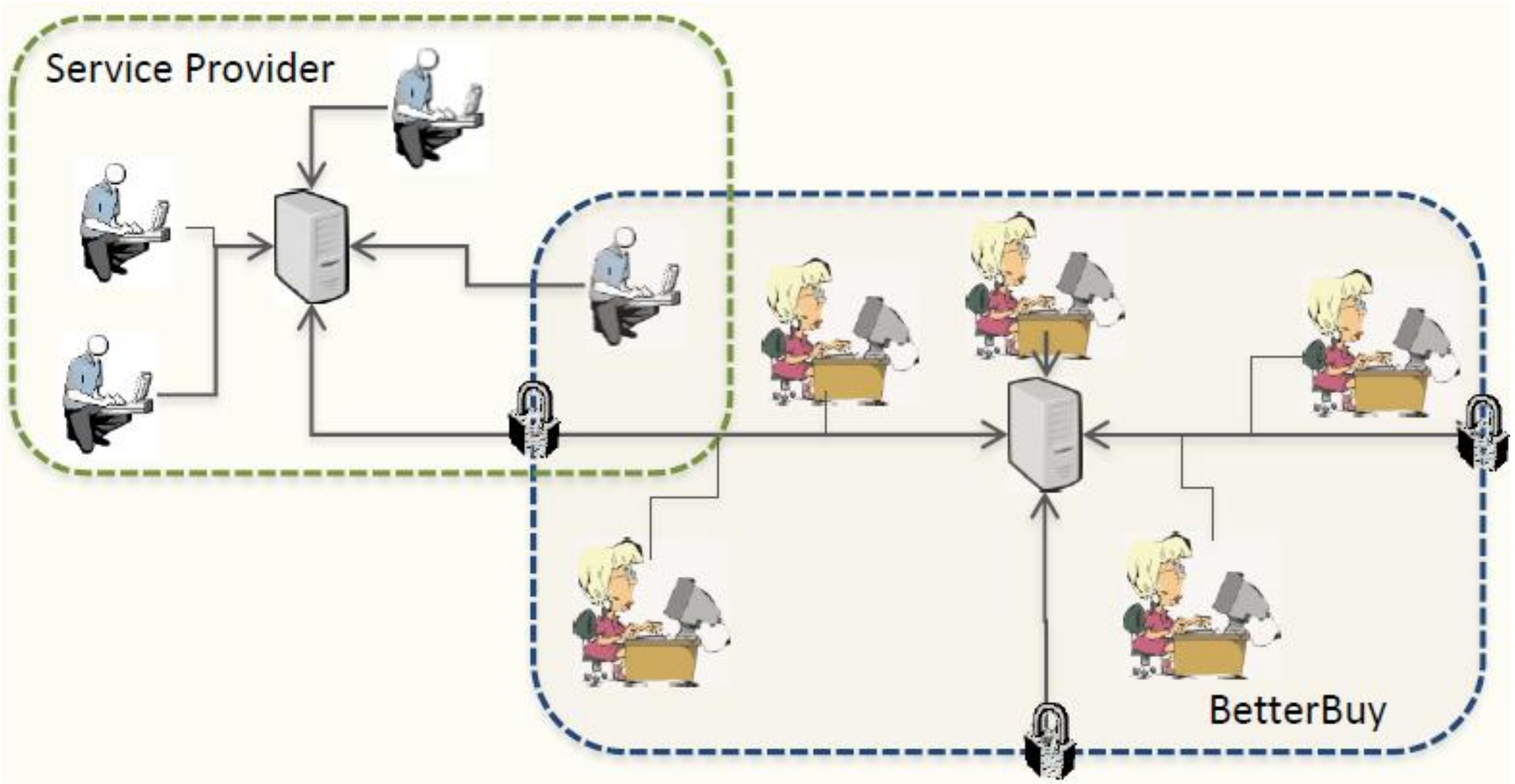


Capability of attacker	• Low skill • Limited resource • Publicly available attack tools • Not well organised • Local reach	• Highly skilled professionals • Extremely well resourced • Bespoke tools • Highly organised • International presence
Response requirements	• Restore services • Special monitoring and_organisation • Some industry information sharing	• Tailored guidance for specialist industry and specific capabilities • Implications for government security services • CNI sector-specific industry response

Perimeterised (Closed) Environments



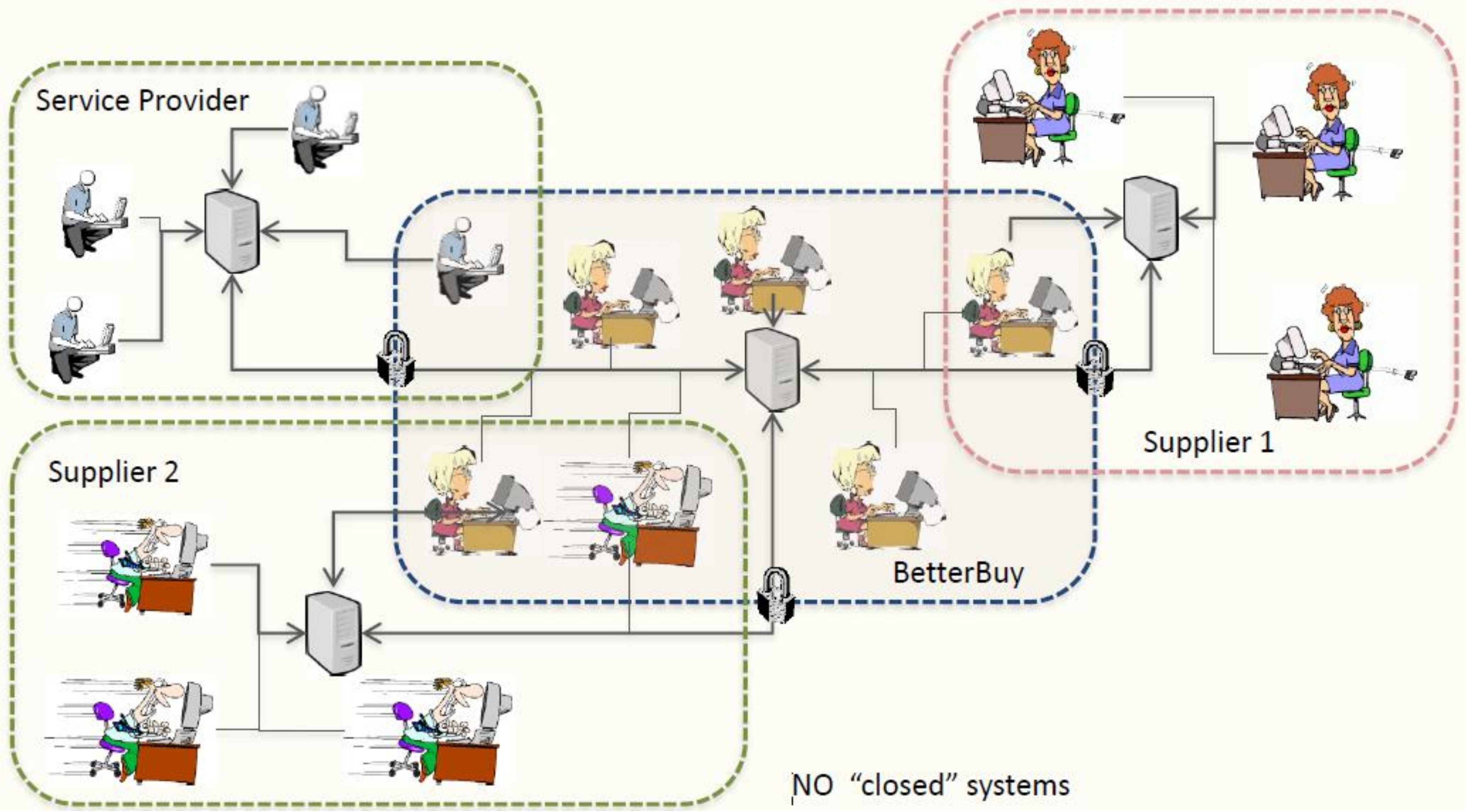
De-perimeterised Environments



- Introduction of additional attack surface – introduction of an external service provider
- Mode of engagement with the external provider is key

De-perimeterised Environments

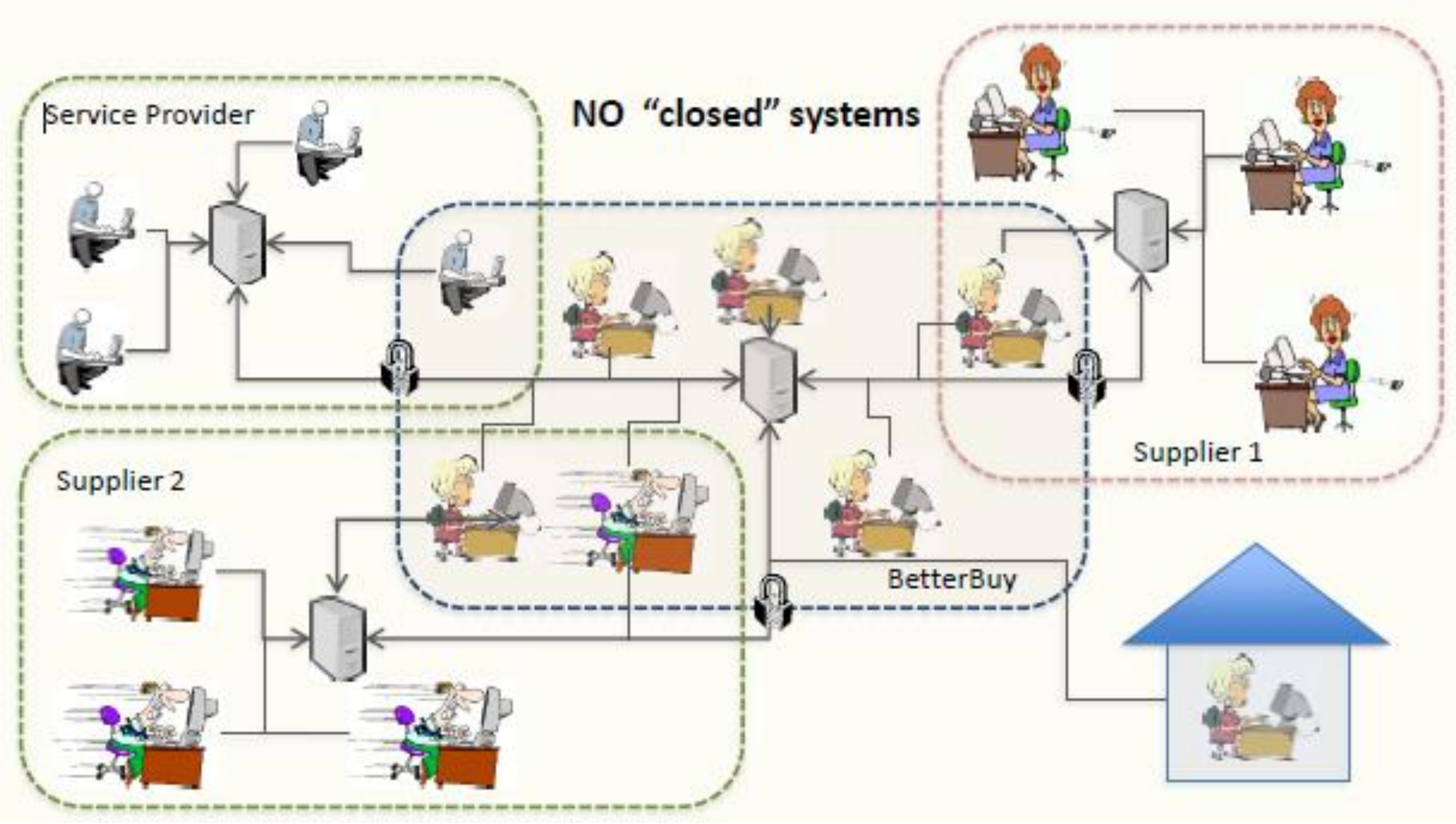
(Open vs. Closed systems)



DR YULIA CHERDANTSEVA

De-perimeterised Environments

(Open vs. Closed systems)



DR YULIA CHERDANTSEVA

Small Business Guide: Response & Recovery

https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-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
  - Are you being attacked?
  - Identify what happened
  - Stop the incident getting worse

  (antivirus alerts & server/audit logs)

- computers running slowly
- users being locked out of their accounts
- users being unable to access documents
- messages demanding a ransom for the release of your files
- people informing you of strange emails coming out of your domain
- redirected internet searches
- requests for unauthorised payments
- unusual account activity

10 Crucial Questions …

- What problem has been reported, and by who?
- What services, programs and/or hardware aren’t working?
- 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?
- What information (if any) has been disclosed to unauthorised parties, deleted or corrupted?
- Have your customers noticed any problems? Can they use your services?
- Who designed the affected system, and who maintains it?
- When did the problem occur or first come to your attention?
- What is the scope of the problem, what areas of the organisation are affected?
- Have there been any signs as to whether the problem has occurred internally within your organisation or externally through your supply chain?
- What is the potential business impact of the incident?

Small Business Guide: Response & Recovery

https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

- Step 3: Resolve the incident
    - IT system managed externally or internally

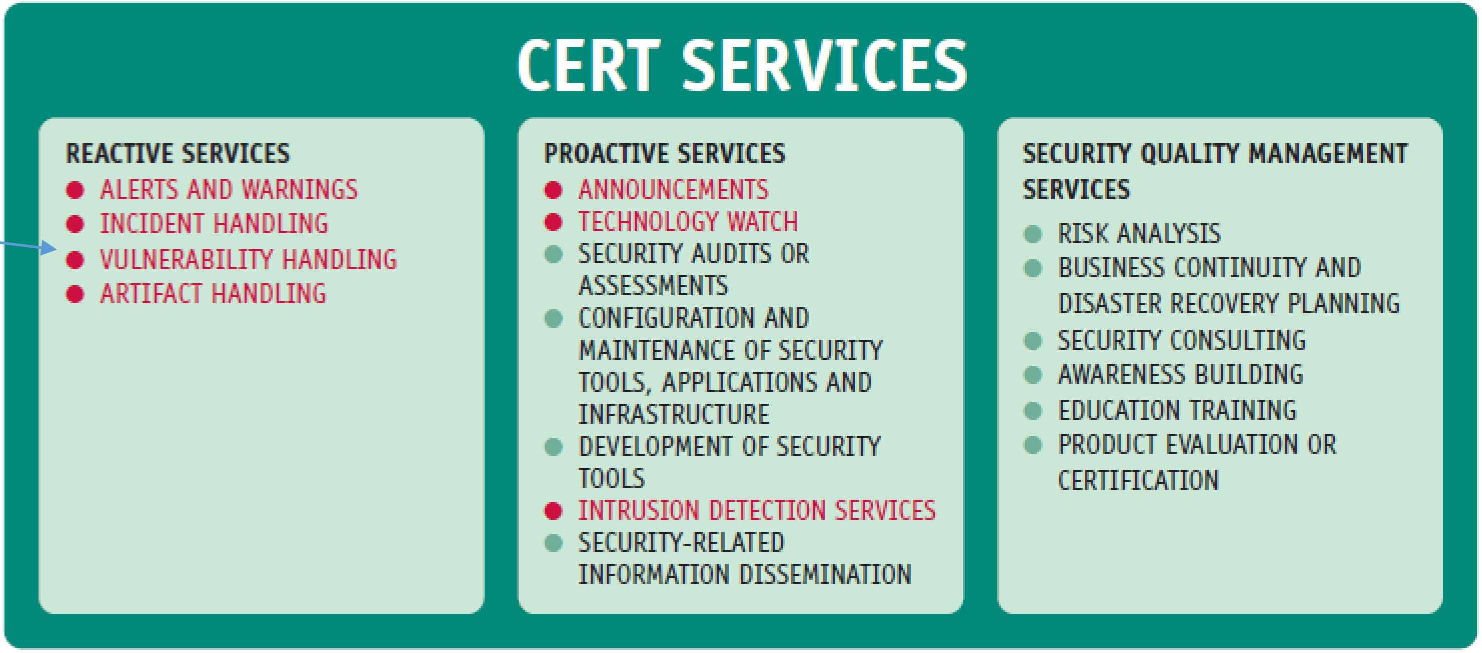
- Step 4: Report incident to wider stakeholders
    - Report to law enforcement – e.g. Information Commissioner's Office (ICO) (https://ico.org.uk/for-organisations/report-a-breach/)
    - Keep everyone informed (staff & customers) – time that is proportionate to the effect of the incident
    - Consider 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)

https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?start=0&rows=20&productType=Cyber%20Incident%20Response%20(CIR)

ENISA (Incident Management)

Computer Emergency Response Teams (CERTS)
(those in red related to incident management)



CERT SERVICES

REACTIVE SERVICES

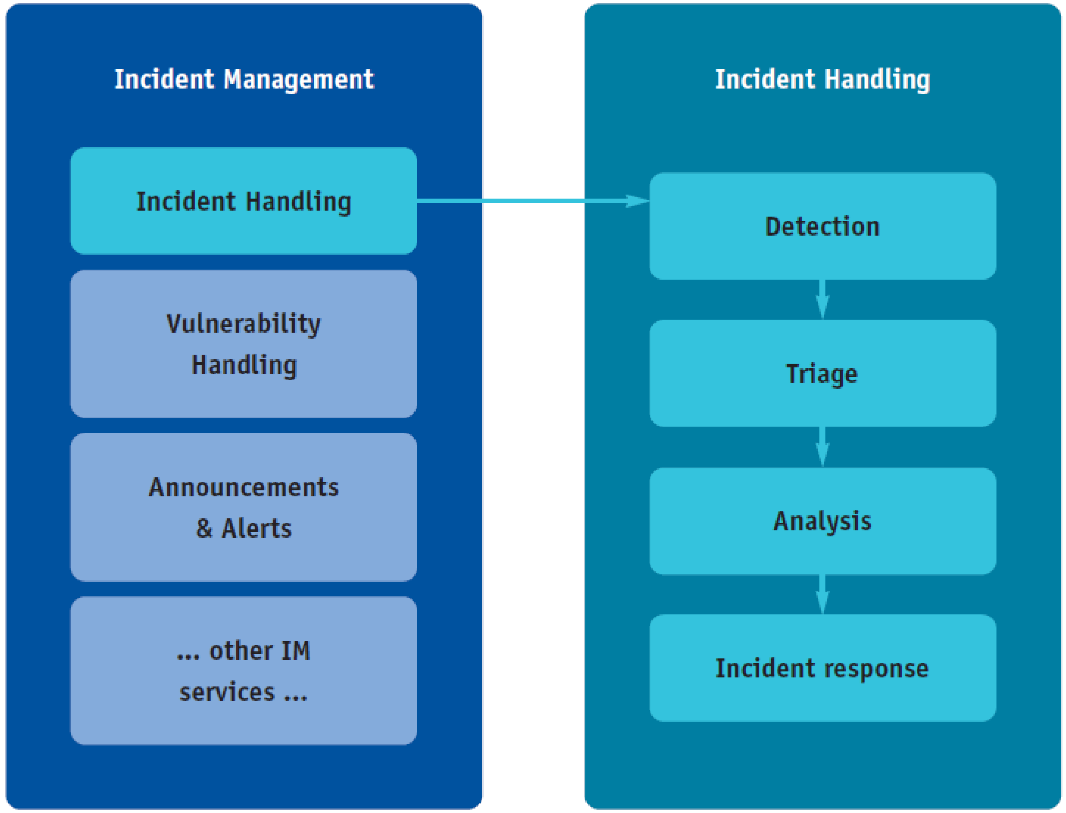
- ALERTS AND WARNINGS
- INCIDENT HANDLING
- VULNERABILITY HANDLING
- ARTIFACT HANDLING

PROACTIVE SERVICES

- ANNOUNCEMENTS
- TECHNOLOGY WATCH
- SECURITY AUDITS OR ASSESSMENTS
- CONFIGURATION AND MAINTENANCE OF SECURITY TOOLS, APPLICATIONS AND INFRASTRUCTURE
- DEVELOPMENT OF SECURITY TOOLS
- INTRUSION DETECTION SERVICES
- SECURITY-RELATED INFORMATION DISSEMINATION

SECURITY QUALITY MANAGEMENT SERVICES

- RISK ANALYSIS
- BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING
- SECURITY CONSULTING
- AWARENESS BUILDING
- EDUCATION TRAINING
- PRODUCT EVALUATION OR CERTIFICATION



CERT can be a virtual team with no formal members and with tasks distributed between different employees in various company departments such as the network operations centre, internal IT security team, legal department, PR department, help desk, etc. It can also be a department in a company’s organisational structure, with several core members but also with some members from different departments, who work part-time or only on a specific task. Finally it can be an organisation or department with only full-time members

ENISA (Incident Management)

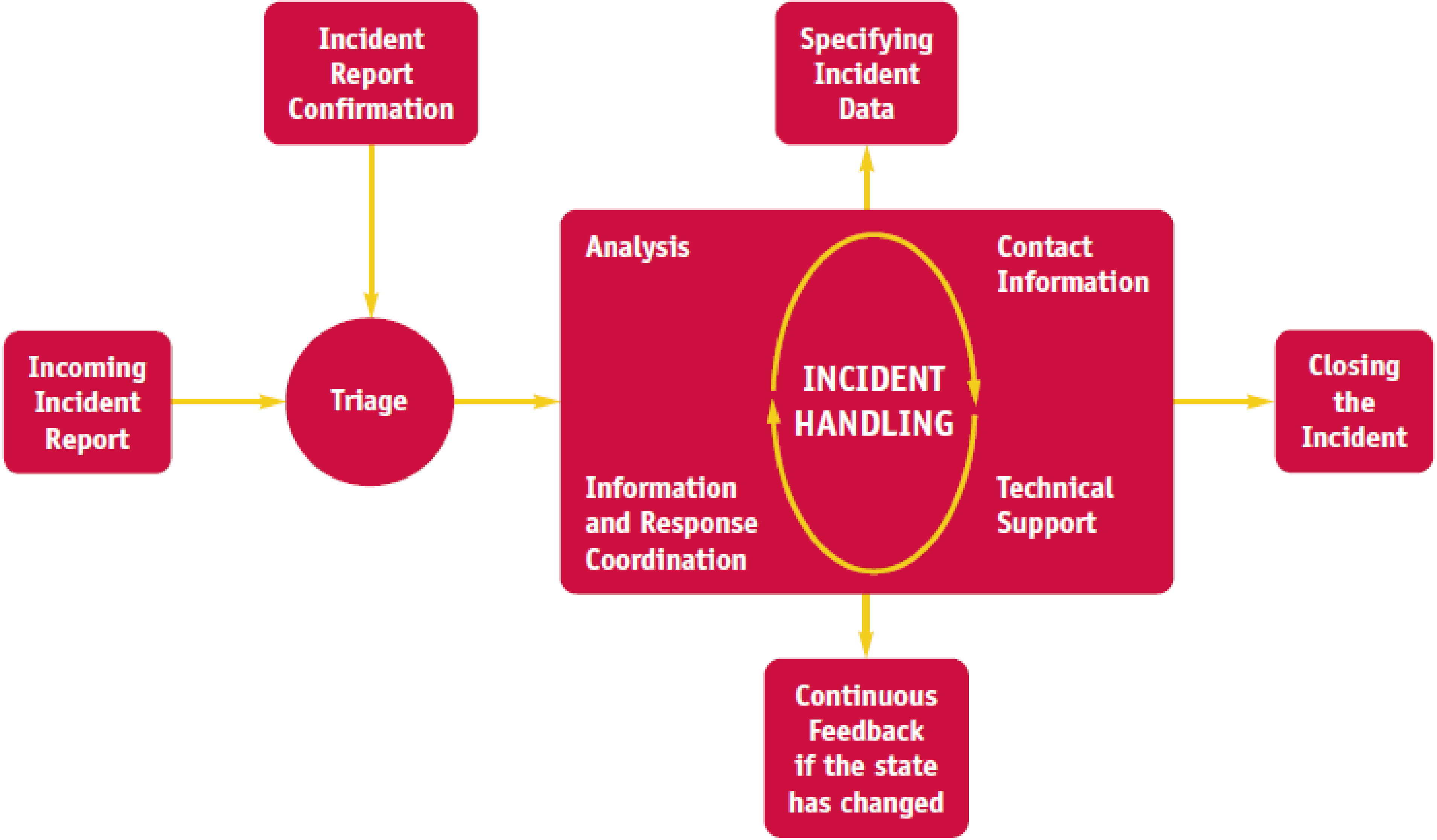
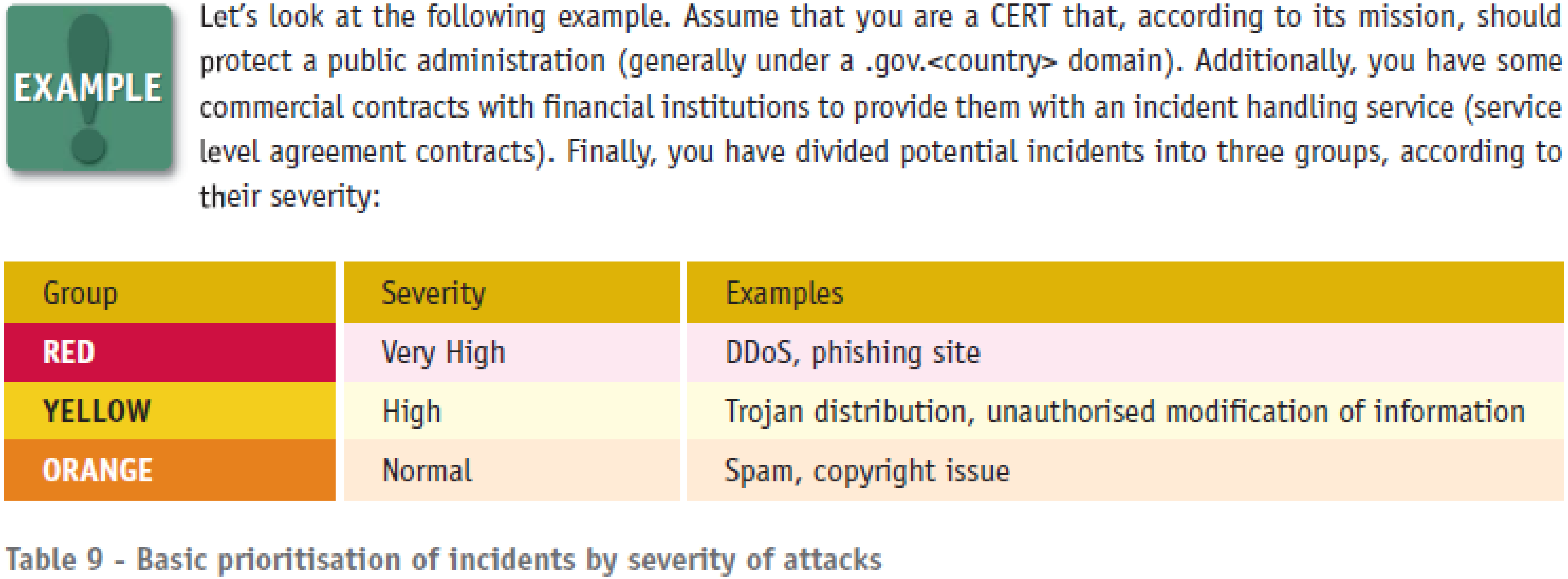


Figure 5 - Incident handling process flow (CERT Hungary example)

ENISA (Incident Management)



EXAMPLE

Let's look at the following example. Assume that you are a CERT that, according to its mission, should protect a public administration (generally under a .gov.<country> domain). Additionally, you have some commercial contracts with financial institutions to provide them with an incident handling service (service level agreement contracts). Finally, you have divided potential incidents into three groups, according to their severity:

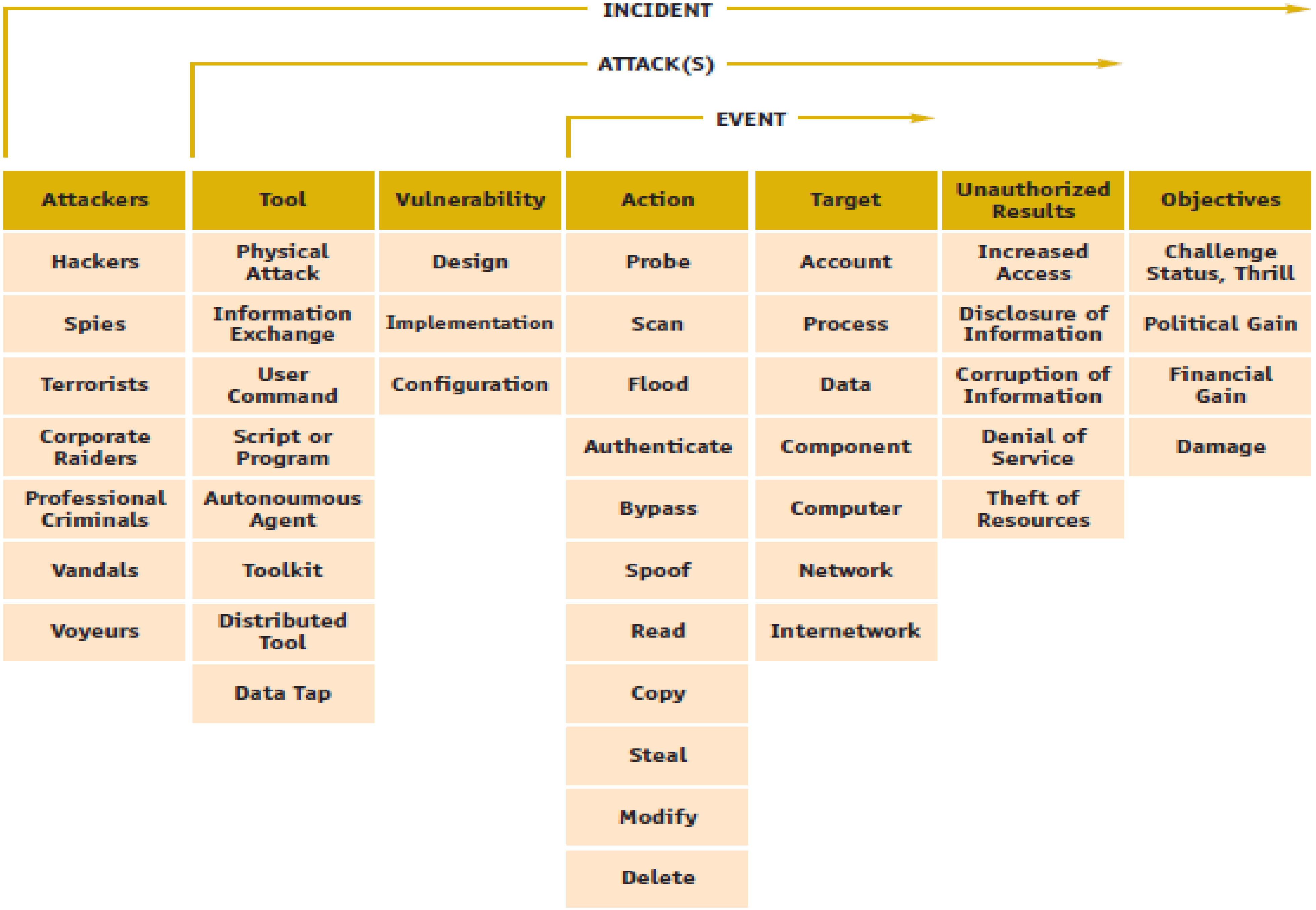
Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Table 9 - Basic prioritisation of incidents by severity of attacks

Incident Taxonomy (European CERT) – Latvian CERT

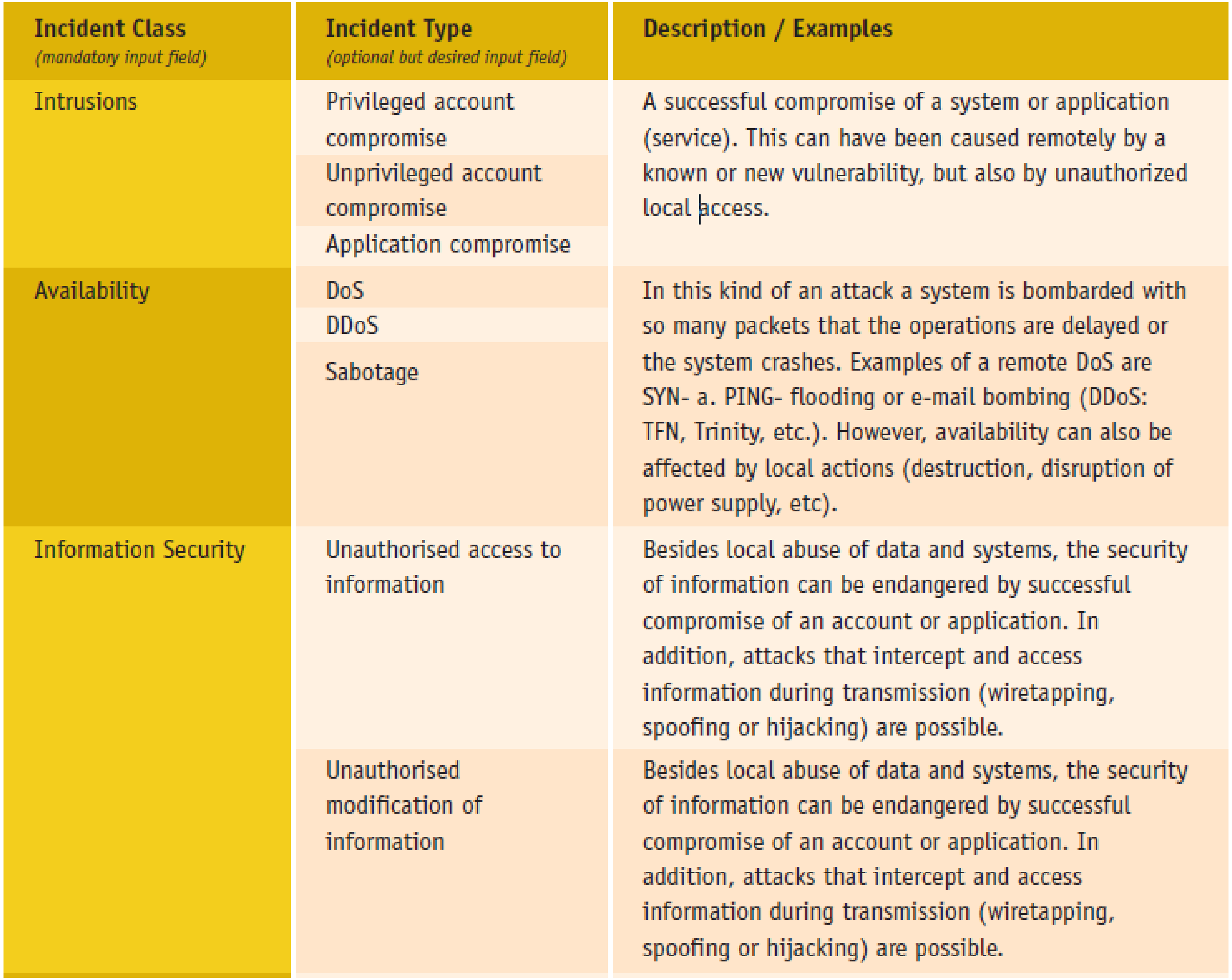
https://cert.lv/en/incidents

- Attacks on the critical infrastructure
- Attacks on the internet infrastructure, eg, 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

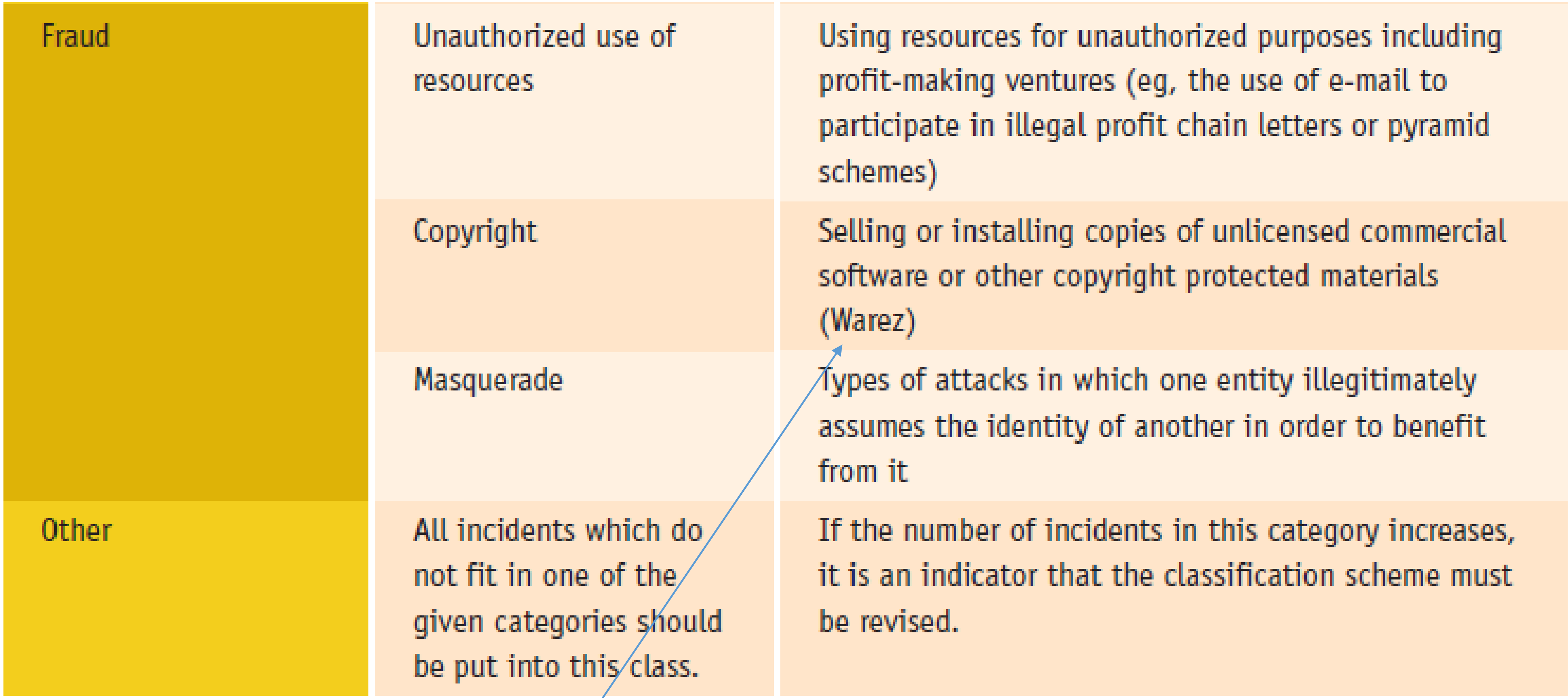


Attackers	Tool	Vulnerability	Action	Target	Unauthorized Results	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

Figure 11 – Common Language security incident taxonomy



Incident Class *(mandatory input field)*	**Incident Type** *(optional but desired input field)*	**Description / Examples**
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access.
	Unprivileged account compromise	
	Application compromise	
Availability	DoS	In this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYN- a. PING- flooding or e-mail bombing (DDoS: TFN, Trinity, etc.). However, availability can also be affected by local actions (destruction, disruption of power supply, etc).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorised modification of information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.



Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes)
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez)
	Masquerade	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Warez is a common computing and broader cultural term referring to pirated software (i.e. illegally copied, often after deactivation of anti-piracy measures) that is distributed via the Internet.

Incident Taxonomy (European CERT) – Latvian CERT … 2

https://cert.lv/en/incidents

- Botnets, ie, 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.