WEEK 3

Introduction

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

* Modelling and Analysis

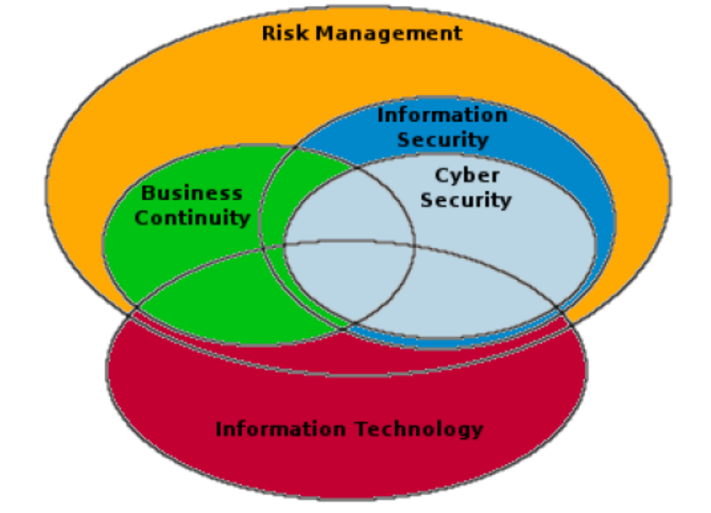
*Focusing on different aspects of business continuity:*

* 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**

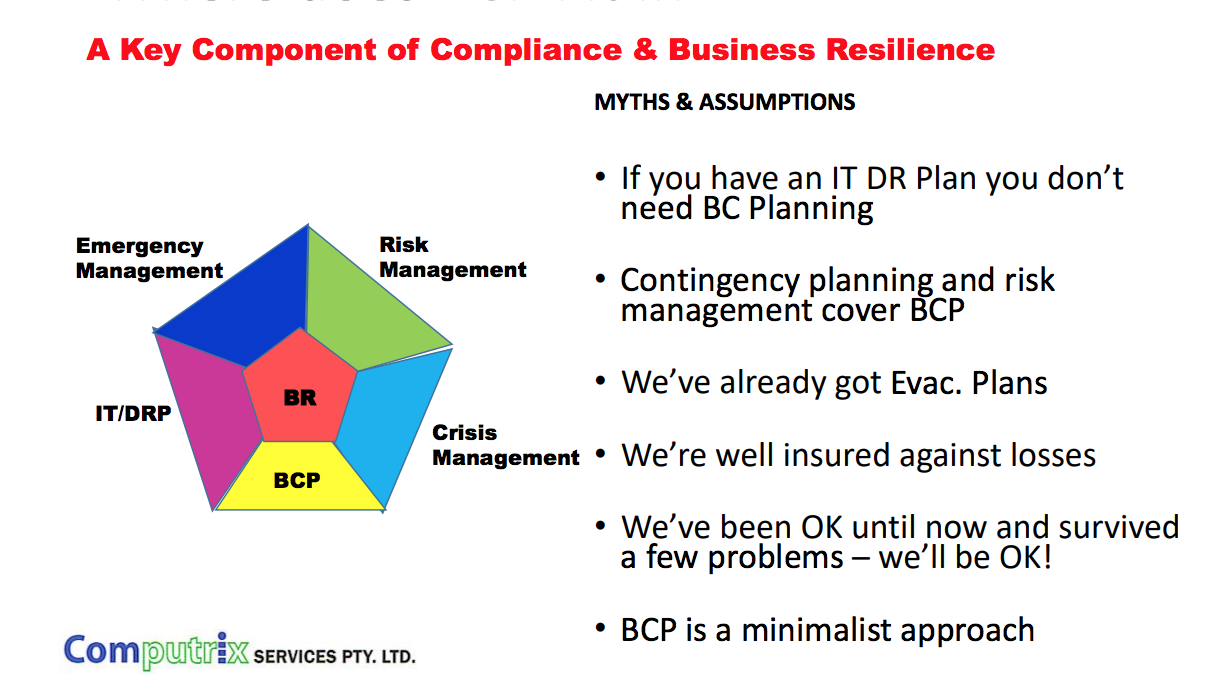
The physical or process alternative to a single point of failure *e.g. back up generator for power failures*.

**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**
6. 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.

1. 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.

1. 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.

1. 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.