**Module 5 Risk Management**

**5.2 Business Impact Analysis**

**Business Impact Analysis Concepts**

* Business impact
* Mission-essential functions
* Identification of critical systems
* Single point of failure
* RTO/RPO
* MTBF
* MTTR
* Privacy impact assessment
* Privacy threshold assessment

**Business Impact Analysis (BIA)**

* Process of evaluating all critical systems (important to core business functions) in organisation to define impact & recovery plans
* Determining potential impacts (costs, resources, time) resulting from interruption of time-sensitive/critical business processes
* Identify critical business functions, systems, services & technologies along with cost associated with their loss & max acceptable outage period
* See NIST definition

**Critical Functions**

* Mission-essential functions, roles, services, systems, apps or data required to sustain business
* Steps

1. Identification & analysis
2. Prioritisation
3. Calculating timeframe for critical system loss
4. Estimating the tangible & intangible impact on organisation

**Single Point of Failure**

* 1 fault/malfunction can compromise entire system/enterprise
* Can be people/technology
* Avoided with redundancy & fault-tolerant protocols/procedures (HA – High Availability)

**Recovery Objectives**

* RTO (Recovery Time Objective) – max amount of time that process/service allowed to be down & consequences still considered acceptable
* RPO (Recovery Point Objective) – point last known good data prior to outage that is used to recover systems

1. As general rule, closer RPO matches time of crash, more expensive it is to obtain

**MTBF (Mean Time Between Failures) & MTTF (Mean Time To Failure)**

* Mean Time To Failure (MTTF)

1. Average time to failure for non-repairable system
2. Represents how long product can reasonably be expected to perform based on specific testing

* Mean Time Between Failures (MTBF)

1. Measurement of anticipated incidence of failure for system/component
2. Measurement determines component’s anticipated lifetime

**Mean Time To Recovery/Restore/Repair (MTTR)**

* Average time required to repair failed system/device/component & return it to operational status
* Calculation includes preparation time, active maintenance time & delay time
* Often part of maintenance contract

**Privacy Assessments**

* Personally Identifiable Information (PII) – information that can be used to distinguish/trace individual’s identity (Eg. Name, social security number, biometric records, etc.) alone/combined with other personal/identifying information that is linked/linkable to specific individual (Eg. Data & place of birth, mother’s maiden name etc.) (NIST)
* Personal Health Information (PHI)
* See section 5.8 for privacy best practices
* Privacy Impact Assessment (PIA)

1. Identifies adverse impacts that can be associated with destruction, loss, corruption or accidental disclosure of sensitive/personal/private data for organisation
2. Required for any organisation that collects/uses/stores/processes PII/PHI

* Privacy Threshold Assessment (PTA) – determines whether system contains PII/PHI