WEEK 3

INCORPORATING ITIL INTO BUSINESS MODEL

**Business Execution**

* This is based on the idea that business strategy is a driver of organizational design choice and IS infrastructure design.
* The top management formulate business strategy and IT managers design and implement ITIL for a better strategic alignment between IT and the business.

**Technology transformation**

* This evaluates the implementation of business strategy through appropriate IT strategy and IS infrastructure and processes.
* It examines the implementation of a chosen business strategy through IT strategy and the required IT infrastructure and ITIL processes.

**Competitive potential**

* It focuses on the utilisation of IT capabilities to impact on products and services (business scope), the key strategy attributes (distinctive competencies) and to create new forms of relationships (business governance).

**Service level**

* The strategic fit enables organizations to meet IS customers’ needs by implementing resources that can respond to their fast changing demands.

BENEFITS OF ALIGNING IT WITH BUSINESS OBJECTIVES USING ITIL

* Strategic alignment is achieved by **enhancing the communication between IT and business**, as well as **improving** **service** **delivery** to business.
* ITIL **breaks down barriers** and enables people in an organization to **share knowledge**.
* ITIL has the ability to **support business strategy, improve IT strategy and competency** and **impact significantly on organizational infrastructure**.
* It provides **consistency** in the way things can be done throughout the organization.
* It improves **quality** **of** **services** as well as **availability** of services, which results in having more **satisfied** **customers** and gaining competitive advantage

RISK MANAGEMENT

* Risk in the context of security is the **possibility of damage happening and the ramifications of such damage should it occur**.

***INFORMATION RISK MANAGEMENT (IRM)***

The process of **identifying** and **assessing** **risk**, **reducing** it to an **acceptable** **level**, and **implementing** the right **mechanisms** to **maintain** that **level**.

TYPES OF RISK

**PHYSICAL DAMAGE**  Fire, water, vandalism, power loss, and natural disasters.

**HUMAN INTERACTION** Accidental or intentional action or inaction that can disrupt productivity.

**EQUIPMENT MALFUNCTION** Failure of systems and peripheral devices.

**INSIDE AND OUTSIDE ATTACKS** Hacking, cracking, and attacking.

**MISUSE OF DATA** Sharing trade secrets, fraud, espionage, and theft.

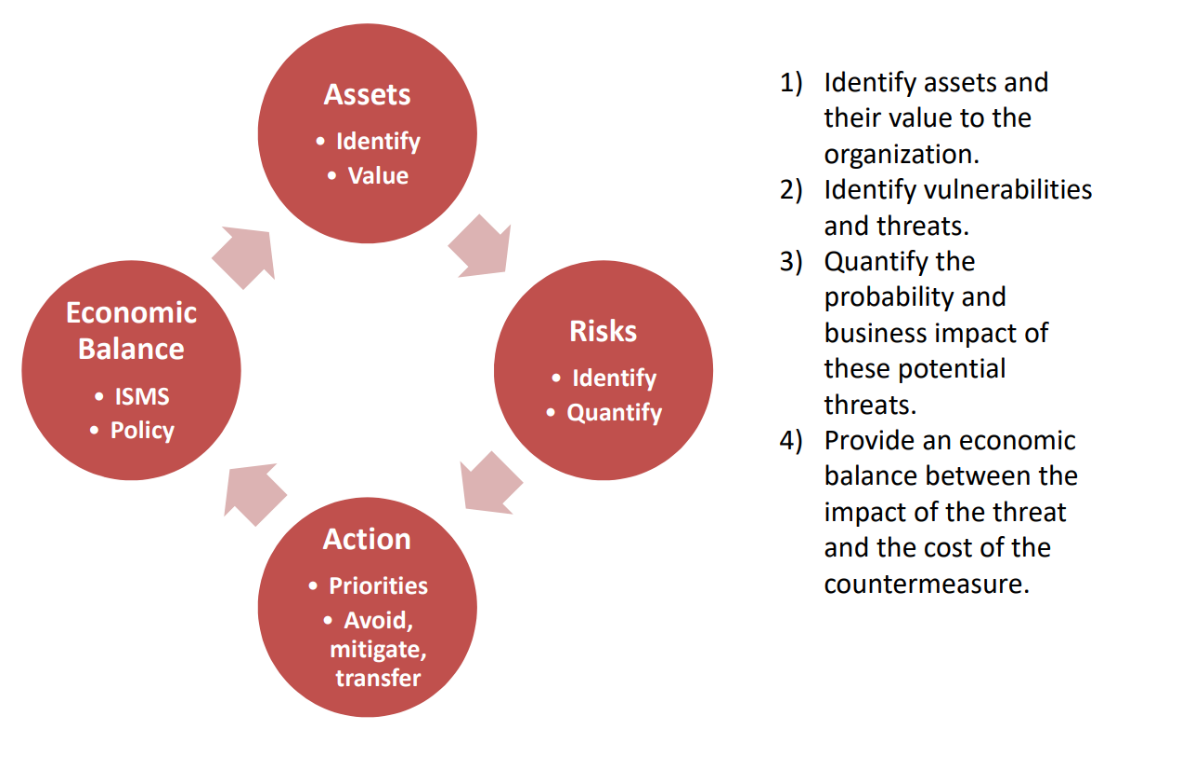
**LOSS OF DATA**  Intentional or unintentional loss of information to unauthorized receivers.

**APPLICATION ERROR**  Computation errors, input errors, and buffer overflows.

INFORMATION RISK MANAGEMENT POLICY

* The objectives of the IRM team.
* The level of risk the organization will accept and what is considered an acceptable level of risk.
* Formal processes of risk identification.
* The connection between the IRM policy and the organization’s strategic planning processes.
* Responsibilities that fall under IRM and the roles to fulfil them.
* The mapping of risk to internal controls.
* The approach toward changing staff behaviours and resource allocation in response to risk analysis.
* The mapping of risks to performance targets and budgets.
* Key indicators to monitor the effectiveness of controls.

RISK ASSESSMENT AND ANALYSIS

****

RISK MANAGEMENT - IN CONTEXT

****

***IDENTIFY***

* Not just the data
* Network mapping
  + What assets? Who owns them?

***VALUE***

* Valued in terms of their importance to the business operation (*low, medium, high*).

***COSTS THAT MAKE UP THE VALUE***

* Cost to acquire or develop the asset.
* Maintenance cost.
* Value of asset to owners.

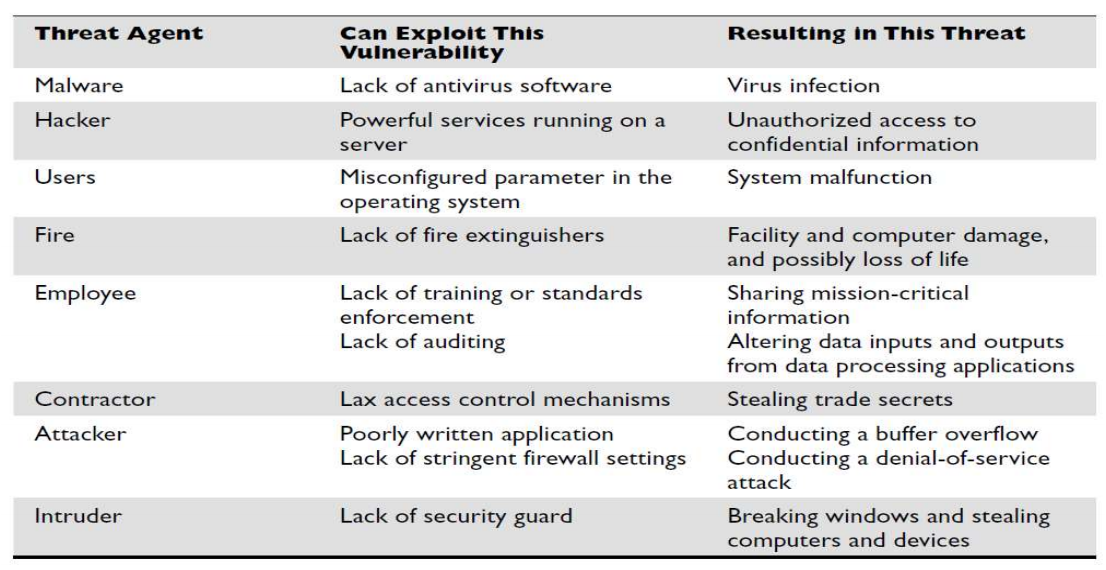
***BENEFIT OF IDENTIFYING VALUE OF ASSETS***

* To perform effective cost/benefit analysis.
* To understand what exactly is at risk.



***IDENTIFY THREATS***

* *Network mapping, who has access to what?*



***A RISK IS:***

* The Likelihood of an event combined with its consequence.
* For something the be a risk there needs to be a vulnerability and a threat.
* Represented as **IMPACT / LIKELIHOOD = RISK**
* Must look at delayed loss when assessing the damages that can occur.



***PRIORITISE BY DOING RISK ANALYSIS***

* Rank risks f(likelihood, impact).
* Residual risk.
* Legal compliance.
* Company priorities.

***HANDLE RISK***

* Mitigate - Put a firewall in place.
* Transfer - Get insured.
* Accept - Do nothing.

***RISK ANALYSIS***

***QUANTITATIVE RISK***

* Used to **assign** **monetary** and **numeric** **values** to all **elements** of the risk analysis process.

***QUALITATIVE RISK***

* Analysis uses a “***softer***” **approach** to the data elements of a risk analysis. It does **not quantify** that **data**, which means that it **does not assign numeric values to the data** so that they can be used in equations.

QUANTITATIVE RISK ANALYSIS

1. We have identified the assets that are to be assessed.
2. Associated a value to each asset
3. Identified the vulnerabilities and threats that could affect these assets.

*Important terms to calculate*

The **Single Loss Expectancy (SLE)** is the **amount** that is **assigned** to a **single event** that **represents** the **company’s potential loss amount** **if** a specific **threat** were to **take** **place**.

**Asset Value × Exposure Factor (EF) = SLE**

Where, the **exposure factor (EF)** represents the percentage of loss a realized threat could have on a certain asset.

***EXAMPLE:***

If a data warehouse has the asset value of £150,000, it can be estimated that if a fire were to occur, 25 percent of the warehouse would be damaged, in which case the SLE would be:

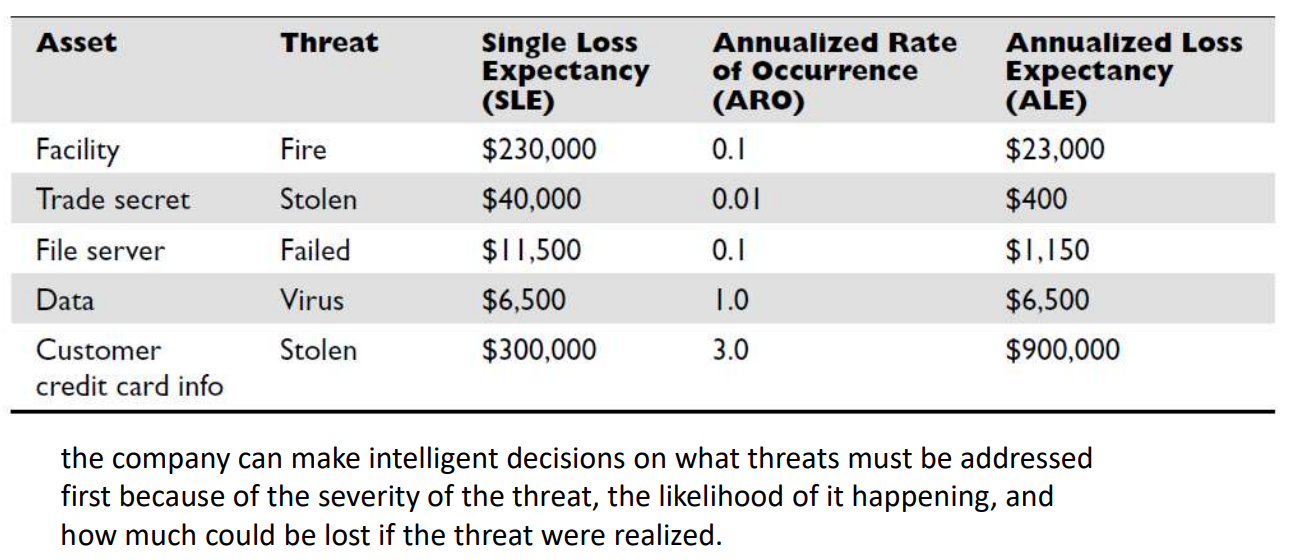
* *Asset Value × Exposure Factor (EF) = SLE*
* *Asset Value (£150,000) × Exposure Factor (25%) = £37,500*

The **annualized rate of occurrence (ARO)** is the **value** that represents the **estimated frequency** of a **specific threat taking place within a 12-month timeframe**.

The range can be from 0.0 (never) to 1.0 (once a year) to greater than 1 (several times a year) and anywhere in between.

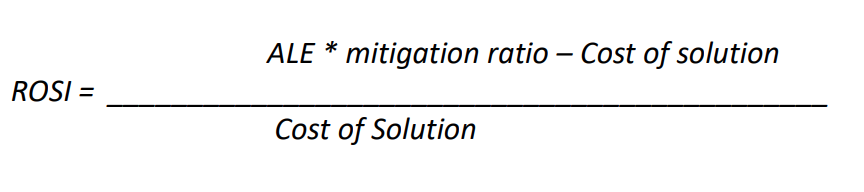
**SLE × Annualized Rate of Occurrence (ARO) = ALE**

For example, if the probability of a fire taking place and damaging our data warehouse is once every five years, the ARO value is 1/5= 0.2 Then the ALE value is £7,500 (£37,500 × 0.2 = £7,500).



***Return on Security Investments (ROSI)***

The ROSI equation integrates the risks and costs associated with a security incident, and combines that with the impact of a security solution.



***ROSI Example:***

* Echo Inc. has been suffering from increased security breaches for the last few years and is considering investing in a user behaviour analytics (UBA) solution. However, the executive suite is not convinced the investment is worth it. The new CIO has decided to run some numbers.
* Echo’s CIO estimates that Echo has been suffering about 10 (ARO=10) security incidents per year for the last three years. These incidents seem to cost about $20,000 (SLE=20,000) in data loss, fine, and productivity. The UBA solution is projected to block about 90% (mitigation ratio = 90%) of the attacks. However, the costs are causing the solution is an estimated $50,000 per year.

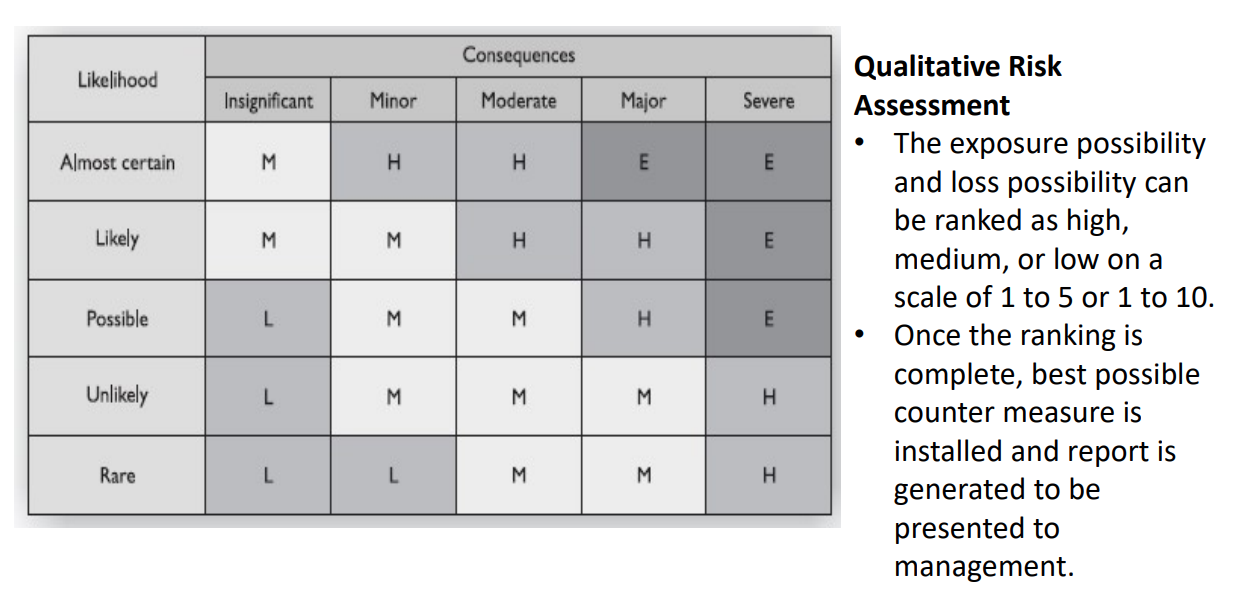
**ARO=10, SLE=20,000,mitigation ratio = 90, Cost of Solution $50,000 per year.**

**ROSI = ((10 \* 20000) \* 0.9 - 50,000) / 50,000 = 260%**

*The investment in this example of $50,000 per year would save Echo Inc. an estimated $130,000 per year. Put simply the saving produced from the investment would provide a 260% payback on the security investment*

QUALITATIVE RISK ANALYSIS

* Qualitative analysis techniques include **judgment, best practices, intuition,** and **experience**.
* Examples of qualitative techniques to gather data are **Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings,** and **interviews**.
* A scenario of each identified vulnerability and how it would be exploited is explored.
* The “**expert**” in the group, who is **most** **familiar** with this **type** of **threat**, should **review** the **scenario** to ensure it reflects how an actual threat would be carried out.
* **Safeguards** that would **diminish** the **damage** of this threat are then **evaluated**, and the scenario is played out for each safeguard.



***Qualitative Risk Assessment Example***

**Scenario**

The risk analysis team presents a scenario explaining the threat of a hacker exploiting a web vulnerability in the website of the company and accessing confidential information held on the five file servers within the company.

Steps

1. The risk analysis team then distributes the scenario in a written format to a team of five people that would be affected by the threat example
   1. *IT manager*
   2. *Database administrator*
   3. *Application programmer*
   4. *System operator*
   5. *Operational manager*
2. They are also given a sheet to rank the threat’s severity, loss potential, and each safeguard’s effectiveness, with a rating of 1 to 5, 1 being the least severe, effective, or probable

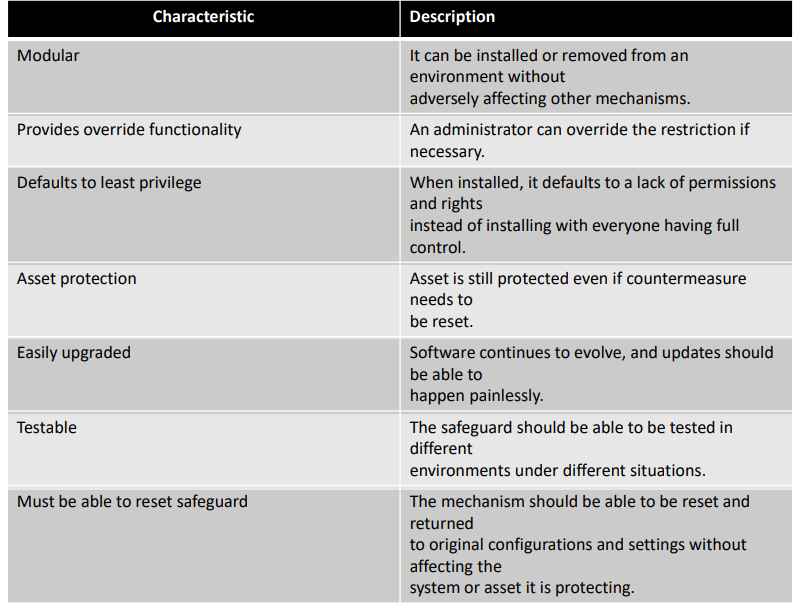


* Update the **ISMS** ***(Information Security Management System).***
* **Provide** an **economic balance** between the **impact** of the **threat** and the **cost** of the **countermeasure**.
* **Recommend counter measures** to the board.

Control Selection

* Things to consider while calculating cost for countermeasures:
* *Product costs*
* *Design/planning costs*
* *Implementation costs*
* *Environment modifications*
* *Compatibility with other countermeasures*
* *Maintenance requirements*
* *Testing requirements*
* *Repair, replacement, or update costs*
* *Operating and support costs*
* *Effects on productivity*
* *Subscription costs*
* *Extra man-hours for monitoring and responding to alerts*

Assessing Functionality and Effectiveness of Control



Risk company is exposed to

**Total Risk** is the risk the company faces if it chooses not to apply control

* **TOTAL RISK = THREATS \* VULNERABILITY \* ASSET VALUE**
* Which is possibility of a vulnerability being exploited multiply by assets value.

**Residual Risk** is the risk left after control is places.

* **TOTAL RISK – COUNTERMEASURE = RESIDUAL RISK**

Handling Risk

* ***Risk Mitigation***
  + Control Selection
  + Implementation
  + Monitoring
* ***Risk Transference***
  + Purchase insurance
* ***Risk Acceptance***
  + Do nothing
* ***Risk Avoidance***
  + Discontinue Activity

Computer Misuse Act 1990

Background

* The law was introduced following the 1987 case of Regina v Gold and Schifreen.
* The hackers were charged and convicted under Frogery and Counterfeiting Act 1981 however, their conviction was overturned on appeal, where they demonstrated that they hadn’t attempted to profit from hacking.

*This lead to the design and introduction of Computer misuse act*

* **Unauthorised** **access** to **computer** **material**, **punishable** by **twelve** **months'** imprisonment (*or six months in Scotland*) and/or a fine "*not exceeding level 5 (unlimited) on the standard scale*"
* Unauthorised access with **intent to commit** or **facilitate** **commission** of **further** **offences**, punishable by twelve months/maximum fine (*or six months in Scotland*) on summary conviction and/or five years/fine on indictment;
* Unauthorised **modification** **of** **computer** **material**, punishable by twelve months/maximum fine (*or six months in Scotland*) on summary conviction and/or ten years/fine on indictment.

Data Protection Act 1998

* The Data Protection Act 1998 was a United Kingdom Act of Parliament designed toprotect personal data stored on computers or in an organised paper filing system.
* It was superseded by the Data Protection Act 2018 and supplements the GDPR which regulates the collection, storage and use of personal data significantly more strictly.

Data Protection Act 1998 Principles

1. Personal data shall be processed **fairly** and **lawfully** and shall **not** be **processed** unless
2. Personal data shall be **obtained** only for **one or more specified and lawful purposes** and **shall not be further processed in any manner incompatible** with that **purpose** or **those** **purposes**.
3. Personal data shall be **adequate**, **relevant** and not **excessive** in relation to the purpose or purposes for which they are processed.
4. Personal data shall be **accurate** and, where necessary, kept **up to date**.
5. Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes.
6. About the rights of individuals e.g. **personal data shall be processed in accordance with the rights of data subjects** (*individuals*).
7. Appropriate **technical** and **organisational** **measures** shall be taken against **unauthorised** or **unlawful processing of personal data** and against **accidental** **loss** or **destruction** of, or **damage** **to**, personal **data**.
8. Personal data shall **not be transferred to a country or territory outside the European Economic Area** **unless** that country or **territory ensures an adequate level of protection** for the rights and freedoms of data subjects in relation to the processing of personal data.

General Data Protection Regulation

* Companies must fully comply with GDPR from 25 May2018.
* **Personal Data**
  + Is defined as any information relation to a person that can be used to identify the person directly or indirectly.
  + Included online identifiers such as IP and cookies, if they are capable to be linked back to user.
  + There is no distinction between personal data about an individual in their private, public or work roles.
* **Penalties**
  + 10 million Euro’s or two percent of global gross turnover for violation of record keeping, security breach notification and privacy impact assessment obligation.
  + 20 million Euro’s or 4% of turnover for violation related to legal justification for processing, lack of consent, data subject rights and cross-border data transfer.
* **Companies are required to implement appropriate technical and organisational measures in relation to the nature, scope, context and purpose of handling and processing personal data.**
  + *These safeguards must be appropriate to the degree of risk and might include:*
    - **Encryption** of **personal** **data**
    - Ensuring **CIA** and **resilience** of **system**
    - **Restoring** **data** in a **timely** **manner**
    - Process to **test**, **assess** and **evaluate** the **effectiveness** of **system**.
  + Consent to be taken by individual whose data is held.
    - Organisation must be able to **show how consent was obtained**
    - Data obtained must be **specific**, **explicit** and of **legitimate** **purpose**
    - User must be able to withdraw consent
* Individual must have full access to information on how their data is processed.
* Companies must report breaches of security.
  + - In the event of personal data breach companies must notify the appropriate supervisory authority with **72 hours**.