Week 5-8 Notes

[**Week 5: Access Control Concepts**](#_ac399todsfga) **7**

[**Access Control**](#_woz2237svlnr) **7**

[What (Definition)](#_ko39iud0d5h9) 7

[Access Control Concepts:](#_quxu89ek2fs7) 8

[Identity](#_symwx6nul005) 9

[Uniqueness](#_mzvfjjfz96n) 9

[Non-descriptive](#_jccgdqynjf3q) 9

[Issuance](#_avu0el8o7fn2) 9

[Identification Component Requirements](#_ws7pd9q7dvz9) 10

[Identification and Authentication](#_ogz79olpz2pi) 10

[Example:](#_lz2fwj6ilznh) 11

[Authorization](#_ley657o9dqg5) 11

[Identity Management](#_ufs0nyimmxdo) 12

[Accountability](#_q11v87ipmemw) 12

[Password Management](#_8yre1813tph) 13

[Password security](#_grkqxjo5pff4) 14

[**Week 6: Access Control Practices**](#_cl31dftc7ac7) **14**

[Access Control Practices](#_rrp0o15mq86s) 14

[Security controls](#_ygjgqze2y7ct) 15

[Definition](#_cs40a83jq0d7) 15

[Advantages](#_bq16yqd3cysg) 15

[What is it for?](#_yibc5fyz5iko) 15

[There are Two ways of categorising Security Controls:](#_64t0gw6yul6i) 15

[1. Categorising according to nature of the control](#_hy360enh5wsf) 15

[2. Categorising according to the different phases of the control process](#_otmk2z31cxtd) 16

[1. Administrative Controls](#_umqf9m3t11ut) 16

[Definition](#_3niw6k74m17b) 16

[Categories of Administrative Controls:](#_qkm813po9h1f) 16

[Examples:](#_uqwz1meo04yz) 17

[2. Technical Controls (aka Logical Controls)](#_byo0gj41gyj2) 17

[Definition:](#_4mtknv9dva38) 17

[May refer to：](#_t9ydc0oq47xm) 17

[Examples：](#_1cj1mlvya8e9) 17

[Preventative](#_gz271g1krfyn) 18

[Detective](#_8pa4u6k9qm5x) 18

[Corrective/Recovery](#_i2h9r3x8rwrj) 18

[3. Physical Controls](#_lkzzuvk70wjo) 18

[Definition:](#_7wjl3726tktn) 18

[Examples:](#_oxeezjnvy8lb) 18

[Categorising according to the different phases of the control process](#_nx39cumxpyy0) 19

[1. Deterrent:](#_jatjz0kb1v69) 20

[2. Preventive:](#_uif8acdm3wve) 20

[3. Detective:](#_v8a3u1rjsplt) 20

[4. Corrective:](#_7dtqqr22jy5w) 21

[5. Recovery:](#_qxaotc5y6gh6) 21

[Real-life Example](#_snvel3otp90j) 21

[Speeding:](#_mt6g13mjpanv) 21

[Fire Hazards:](#_ed6nkgent82h) 21

[Commonly Used Security Methods](#_wyw02nq6fg6d) 22

[Least Privilege](#_mxv39hfbq1vi) 22

[Advantages:](#_hsucxmcjr03w) 23

[Disadvantages:](#_jgortzryj30x) 23

[Importance:](#_r7a7g06cief0) 24

[Defense in Depth (multiple types of security controls in different layers)](#_5p3joxvcbpif) 25

[● Advantage:](#_u5d75vhdn9jb) 25

[● Disadvantages:](#_qbkka0v3ppng) 25

[Eg.](#_vc9fkdl99cmc) 25

[Minimisation](#_pcyiyn3p2mxo) 26

[Purpose/Definition/Principle/States that:](#_eloe2sova8oy) 26

[● Advantages/Importance:](#_knc3cvysv7d3) 27

[Keep Things Simple](#_mmba7wlhgt11) 27

[Compartmentalisation](#_ywirg3lpfvc3) 28

[● Real life example:](#_1zu87ejlllme) 28

[● Definition:](#_rk9dzku1sfi0) 28

[● Advantages/Importance:](#_qj0opc1eq17r) 28

[Use Choke Points](#_ypz115t0171b) 29

[Purpose:](#_lbmza8jksxgg) 29

[Definition:](#_csniexbnvuce) 29

[Example:](#_qtmnawn3juev) 29

[Importance:](#_o12l2vuskcqg) 29

[Advantages:](#_d4ky3klntsnl) 29

[Disadvantages:](#_5jq6ok7ffeoh) 30

[Conclusion from advantages and disadvantages:](#_cv222n32qkvj) 30

[Fail Securely](#_2zuf3i27mx96) 30

[Definition:](#_or4zwvnvbwta) 30

[Principle:](#_5cewllujc9lw) 30

[Example:](#_wbywtevp4glt) 30

[Advantages/Importance:](#_c6b8iz5g3xcf) 31

[Disadvantage:](#_f6tgvgxo0y45) 31

[Secure the Weakest Link](#_umkj5exoarc6) 32

[Definition/Principle:](#_nwc10ztpv49n) 32

[Advantages/Importance:](#_41vtuex3vcmh) 32

[Examples:](#_depjqas77tq7) 32

[Real life examples:](#_mqn8hluuw0e3) 32

[Disadvantages:](#_f0hzg6wundjr) 32

[Leverage Unpredictability](#_mh305s1mrgf1) 33

[Definition/Principle:](#_uf4lw524luys) 33

[Example:](#_ti8iqfexhx42) 33

[FYI:](#_nf99vj3qnagq) 33

[Examples:](#_cow5dbhccxoq) 33

[Importance:](#_78aur3xg0cnp) 33

[Segregation of Duties](#_3gec1pd7vz22) 34

[Purpose/Definition:](#_me1keyn58v4m) 34

[Principle:](#_w7t3ryspyf2x) 34

[Most Cost Effective Method](#_hvo2l2hpr93v) 34

[Week 7: Busniess Continuity I](#_kc82rto971hi) 34

[Comprehensive approach to business continuity plan](#_93z1ih93s9zm) 34

[● Prevention:](#_3uj162s7papr) 34

[● Preparedness](#_738jteti9bcy) 34

[● Response:](#_4abkg8xviloq) 34

[● Recovery:](#_knv3yn9rbvp5) 35

[Risk](#_tpkw512b7x6a) 35

[● Definition:](#_jfif45h0b4kx) 35

[Risk Management](#_2e33o6kyrfxy) 35

[Risk management plan consists of three stages](#_4syd1eprzvzd) 36

[1. Plan](#_of1p5mgo4z0y) 36

[2. Collect information/perform risk analysis](#_vyp1njay8xaa) 36

[3. Define recommendations](#_tk7s24bv3a4a) 36

[How to determine risk](#_cjjmgbpysrcp) 37

[● Loss/damage](#_u9u3kaf2wxyu) 37

[● Likelihood](#_cvbae3ttgf1m) 37

[○ Definition:](#_l1k5nwhco1tx) 37

[● Effectiveness of existing controls](#_pr8xya9kukjc) 38

[● Uncertainty of vulnerability knowledge](#_i7bkjy1b7r74) 38

[Residual risk](#_yfksebsz9e9e) 38

[● Definition:](#_jdzfe9leb6b) 38

[Risk Management Plan](#_a8d81nfqi33n) 39

[Risk management involves three major undertakings:](#_hnwdtir5mf2x) 39

[Risk management: formal process](#_omvph8dzwa77) 39

[Who is to undertake this risk assessment, and How](#_ackf1qd9hfdo) 40

[Quantitative risk assessment](#_zb8pcqoo7dnq) 40

[Purpose:](#_2mp23webtg5k) 40

[Example:](#_8brapkw697sx) 40

[Limitations:](#_92h7vv8l41s2) 41

[Issues addressed:](#_wvxbmokn2k08) 41

[Limitations/ Disadvantages:](#_mm4qy35ecdf7) 41

[Qualitative Risk Assessment/Analysis:](#_rz7zs0q08wr9) 42

[Definition:](#_g3bvzkyntymm) 42

[Qualitative analysis techniques include:](#_82m9z5wyqw6r) 42

[Examples of qualitative techniques to gather data are:](#_4nyb7r4l65gv) 42

[The risk analysis team](#_wwy44cwqblhi) 42

[Concepts](#_ozo52mp38p4c) 42

[Single Loss Expectancy](#_krm5uso9sfyy) 43

[Example:](#_nhdo9vjkfnrv) 43

[Annualized rate of occurrence (ARO).](#_w3vd6ag7s7g4) 43

[Example:](#_osg780wdno31) 43

[The Cost Benefit Analysis (CBA) Formula:](#_dbjqtmizmeba) 44

[Risk Assesment](#_zcf2qccs7rkh) 44

[Disadvantages of Risk Assessment:](#_7c84u2x6rdyh) 44

[Tools to asses and handle threats](#_wk4smx4xn0gf) 44

[Purpose:](#_1kcj1v5jtlmy) 44

[Cons/Disadvantages of using RA tools:](#_v43vqq1sejfh) 45

[Alternatives if RA tools are not used:](#_6qofotsaqhk6) 45

[Risk Analysis](#_n3ogksuo8zoa) 45

[Importance:](#_ojkad6afkvc5) 45

[Purpose:](#_5nt74yhv9rcz) 46

[Definition:](#_im3oalwdwba) 46

[A risk analysis has four main goals:](#_k5gx4uleb7jq) 46

[What Risk Analysis do:](#_hf99qz4hwm8q) 46

[What should be done by a team:](#_piobizp5baz3) 47

[- Team:](#_wqili05pfe8e) 47

[- During discussions:](#_4j39ebxp7cmd) 47

[- Management:](#_f9m8el9s96hz) 47

[Importance and purpose:](#_i3e5uj8qyw5i) 48

[- Management:](#_6s60qkbwkdy2) 48

[Strategies to Address Risks](#_pd7o822v126m) 48

[Strategies to address risks:](#_i7ukk0mo6rj) 48

[Defend](#_rb631uoejhzm) 48

[Purpose:](#_9yz17okqwkw) 48

[How it is carried out:](#_moud9ed0oo75) 49

[Transfer](#_m1epm8vlvm6r) 49

[Purpose:](#_kuumoqrkyvd7) 49

[How it is carried out:](#_chsfqznssgwg) 49

[Example:](#_13ujifl7ivih) 49

[Mitigate](#_wjfr2cjhkovj) 50

[Terminate](#_iwnmu7n1jeei) 50

[Definition/Purpose:](#_edcl4obtwxkq) 50

[How it is done:](#_ups21qbd7who) 51

[Accept (Especially if the risk is relatively low)](#_b3rre5jclmg0) 51

[Purpose:](#_7dz7fjm10658) 51

[Example](#_2l5348e6nkc8) 51

[Asset Management](#_xfbpklq85191) 52

[Tangible Assets](#_4e3sv7q31lj1) 52

[Intangible Assets](#_pwtvhklvk324) 52

[How the value is derived](#_35qpvkc7ijfu) 52

[Example:](#_pnecz99kuygs) 52

[The following issues should be considered when assigning values to assets:](#_b29kozf9c3qt) 53

[Change Management](#_8lmyemr6aphf) 53

[Definition:](#_x21q5dxs5137) 53

[Importance:](#_oze6u0g6ku4z) 53

[There are different kinds of changes.](#_j7lxbv90dcve) 54

[Examples](#_xiq9pa0juie) 54

[Disadvantages/ Limitations/ Downsides:](#_ysx6v9qmw2e5) 54

[Purpose:](#_epjt0efbu2ze) 54

[Recommended auditing change management in following areas:](#_evjgm6i9wimc) 55

[Change Procedure](#_q71zadop9pql) 56

[1. Requests:](#_qsbe66w9mthk) 56

[2. Impact Assessment:](#_8jcy3plj06z3) 56

[3. Approval/Disapproval:](#_ftqgue3gdfkh) 56

[4. Build and Test:](#_909lsron0v38) 57

[5. Notification:](#_hdz7zxrgcygs) 57

[6. Implementation:](#_ttxty61a5bdq) 57

[7. Validation:](#_avmgptvtmnpt) 57

[8. Documentation:](#_g4jhbi354b38) 58

[Basic Change Management Workflow](#_hiy9ppr3swzn) 58

[Change Review](#_3ga80ka4eswk) 58

[1. Change Monitoring](#_qm3m6fyc781c) 58

[Importance of CM:](#_q1107uoq5p4z) 58

[2. Measuring success of the change:](#_ytnj0il5omx4) 59

[Technical objectives:](#_nlc3sl9jazb2) 59

[Business objectives:](#_17wml3l9xxhg) 59

[3. Change Management Assessment](#_lyn6wuys8dm9) 59

[4. Business Continuity](#_82du5roe9z29) 59

[What Change Management should include](#_d30jnem47kim) 60

[Documented Change](#_wdriukkd7dko) 61

[Documented audit trail](#_m7a2y2vv86yg) 61

[Risk Management](#_qwrx9xspwbyi) 61

[Change Classification](#_t884tpnr8vap) 61

[SLA’s (Service Level Agreements)](#_xby914kc0cgd) 61

[Version Control](#_q030q0hcraxl) 62

[Testing](#_u3egtrbdo5e1) 62

[Approval](#_8f4cufj7k9en) 62

[Communicating changes (and involve the users!)](#_at26oa7mh9ea) 62

[Implementation](#_ymcr3n5copyu) 62

[Fall back](#_3ad5bkb7oa5y) 62

[Documentation](#_ol8dhjhbvv0y) 62

[Business Continuity Plans (BCP)](#_yynur2y6rq69) 63

[Emergency Changes](#_eec9ng3pwfmu) 63

[Change Monitoring](#_m61617sqpvr1) 63

[Roles and responsibilities(From highest rank to lowest)](#_wcd6vchcgnr8) 63

[Members of the Board](#_1g2b73qmjn8l) 63

[Information Security Manager](#_cefvj1rn2gw9) 64

[Operations Manager](#_nyqsg38av98w) 64

[IT Service Provider](#_2qn8z9piyqf5) 65

[Solution Owners](#_25f3ziuncfxp) 65

[IT Governance Value statement](#_pg3umt5z33vq) 65

[Policy Access Considerations](#_jyjc82e2sr9j) 65

[Week 8: Business Continuity Planning II](#_im9sdj2mo1mg) 66

[Business Continuity Planning](#_y1e2vtrj7r33) 66

[Definition:](#_mgdh5vgo3vr8) 66

[BCP purposes:](#_9m1cfhp6b3d2) 66

[Advantages:](#_axqakvt4n6jb) 66

[Importance:](#_qtjr3joj8uz9) 66

[Disaster Recovery Planning](#_7g890851sj9) 67

[DRP purposes: (part of RBCP) aka Contingency Plans](#_wdvwbwuy8ajp) 67

[Importance:](#_dsq19gtth4zm) 67

[Advantages:](#_91qhj9xtj4wx) 68

[Difference between BCP and DRP](#_ht0adfezctjn) 68

[Disasters](#_xsmi7d2ynljt) 68

[● Natural](#_3jgh1q89sk44) 68

[● Environmental](#_milagh2l2pzx) 68

[● Human](#_nub4q2p6tkt1) 68

[BCP Process](#_ncqnev8cazj9) 68

[Initiation Process of BCP](#_70cumv7suaep) 69

[Business Impact Analysis](#_sdxzljl1aoju) 70

[<Recovery Parameters>](#_fbyuu2crq9g5) 72

[Maximum tolerable downtime (MTD)](#_crzx6ovpnqcw) 72

[Examples](#_66d5wlqm4guj) 73

[The recovery point objective (RPO)](#_hl94kcq132dp) 74

[The recovery time objective (RTO)](#_uotwo95a2f01) 74

[Work Recovery Time](#_eq7qqodnowxr) 75

[Examples of Recovery Parameters](#_8jitmsgokpdy) 75

[Recovery Parameters Timeline](#_k88k3d9hqqb4) 77

[Recover Time over Complexity of Method](#_x97de3uvgpco) 78

[Optimum time to set RPO, MTD and RTO](#_twq5p3ld5gho) 78

[Offsite Facilities (related to RTO)](#_w6vyfo61wx2x) 79

[Alternate Processing Facilities](#_44uv73s0970y) 79

[1. Hot site](#_8hrogmexc67y) 80

[2. Warm site](#_t3q7921ga9kp) 80

[3. Cold site](#_avhwkk6phw0g) 80

[Conclusion](#_kdui59bnydi7) 81

[The following provides a quick overview of the differences between offsite facilities:](#_oj2tiwm8uho1) 82

[Hot Site Advantages](#_ivsa3rlglhem) 82

[Hot Site Disadvantages](#_vuzznqpvut2v) 82

[Warm and Cold Site Advantages](#_5dt6fcv2hg25) 82

[Warm and Cold Site Disadvantages](#_pu5tsra6amgc) 82

[4. Tertiary Sites](#_8oevlo84j45l) 82

[5. Reciprocal Agreements](#_at71aobnzzeb) 83

[Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:](#_dspolnzgkz75) 83

[Offsite Location](#_s9k8h2e8sjsr) 84

[Redundant Sites](#_n3kiiivph3ob) 84

[Contingency Plans ( Discovery Recovery Planning: DRP)](#_cxt0oez06nyf) 85

[Supporting information & Appendices](#_aqtkkd5b1s86) 85

[Main phases](#_5270u6kn9h1a) 85

[1. Supporting information and Appendices](#_3dmzo9hk02ni) 85

[2. Activation and Notification Phase](#_a2oyztvd9dly) 86

[Recovery Phase](#_sw0dsbjpt9j3) 87

[Reconstitution Phase](#_zhyeq837gq5i) 89

[**Tutorial**](#_xjnxb2rb5dja) **91**

[Tutorial: Week 5 Access Controls](#_tw8ujvih0yq) 91

[Tutorial: Week 6 Security Controls](#_251nrqvgbso) 96

[Tutorial: Week 7 Business Continuity 1](#_qzbqzib4uxo3) 104

[Tutorial: Week 8 Business Continuity II](#_q1o1iqadfq7k) 115

## Week 5: Access Control Concepts

### Access Control

#### What (Definition)

* ***Access controls*** are security features that control how users and systems communicate and interact with other systems and resources.
* They protect the systems and resources from unauthorized access and can be components that participate in determining the level of authorization after an authentication procedure has successfully completed.
* Access control is a broad term that covers several different types of mechanisms that enforce access control features on computer systems, networks, and information.
* Access control is extremely important because it is one of the first lines of defense in battling unauthorized access to systems and network resources.

Access Control：

Identification

• Subjects supplying identification information

• Username, user ID, account number

• Authentication

• Verifying the identification information

• Passphrase, PIN value, biometric, one-time password, password

• Authorization

• Using criteria to make a determination of operations that subjects can carry out on objects

• Accountability

• Audit logs and monitoring to track subject activities with objects

#### Access Control Concepts:

* Identity
* Identification and authentication
* Authorization
* Accountability
* Password management

##### Identity

Creating or issuing secure identities should include three key aspects

* Uniqueness
* Non-descriptive
* Issuance

###### Uniqueness

Definition

* Uniqueness refers to the identifiers that are specific to an individual, meaning every user must have a unique ID for accountability.

Examples

* Retina scan
* Fingerprints
* Iris scan

###### Non-descriptive

Definition

* Non-descriptive means that neither piece of the credential set should indicate the purpose of that account.

Examples

* For example, a user ID should not be “administrator,” “backup\_operator,” or “CEO.”

###### Issuance

Definition

* These elements are the ones that have been provided by another authority as a means of proving identity.

Examples

* ID cards are a kind of security element that would be considered an issuance form of identification.

###### Identification Component Requirements

When issuing identification values to users, the following should be in place:

* Each value should be unique, for user accountability
* A standard naming scheme should be followed.
* The value should be non-descriptive of the user’s position or tasks.
* The value should not be shared between users.

##### Identification and Authentication

* **Identification** describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. Once a person has been identified through the user ID or a similar value, she must be **authenticated**, which means she must prove she is who she says she is.

* Three general factors can be used for authentication:
* something a person knows/ authentication by knowledge
* something a person has/ authentication by ownership
* something a person is/ authentication by characteristic
* Strong authentication contains two out of these three methods: something a person knows, has, or is.
* Strong authentication is also sometimes referred to as **multi-authentication**, which just means that more than one authentication method is used. **Three-factor authentication** is possible, which includes all authentication approaches.

###### Example:

* User ID,
* MAC address,
* IP address,
* Personal Identification Number (PIN),
* Identification Badges,
* Email Address

##### Authorization

* Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions.

Eg. Different positions will have different rights and privileges to carry out the requested actions

* For example, a teacher and a student in school will have different rights to access different platforms on a school system. A teacher will be able to carry out certain tasks that a student cannot.
* The system will look at some type of access control matrix or **compare security labels** to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

###### Identity Management

* Identity management is a broad and loaded term that encompasses the use of different products to identify, authenticate, and authorize users through automated means.
* The following are many of the common questions enterprises deal with today in controlling access to assets:
* What should each user have access to?
* Who approves and allows access?
* How do the access decisions map to policies?
* Do former employees still have access?
* How do we keep up with our dynamic and ever-changing environment?
* What is the process of revoking access?
* How is access controlled and monitored centrally?
* Why do employees have eight passwords to remember?

##### Accountability

* Auditing capabilities ensure users are accountable for their actions, verify that the security policies are enforced, and can be used as investigation tools.
* There are several reasons why network administrators and security professionals want to make sure accountability mechanisms are in place and configured properly:
* to be able to track bad deeds back to individuals
* detect intrusions
* reconstruct events and system conditions
* provide legal recourse material
* produce problem reports
* Audit documentation and log files hold a mountain of information—the trick is usually deciphering it and presenting it in a useful and understandable format.
* Accountability is tracked by recording user, system, and application activities. This recording is done through auditing functions and mechanisms within an operating system or application.
* Audit trails contain information about operating system activities, application events, and user actions.
* Audit trails can be used to verify the health of a system by checking performance information or certain types of errors and conditions.
* After a system crashes, a network administrator often will review audit logs to try and piece together the status of the system and attempt to understand what events could be attributed to the disruption.

What to keep in mind when dealing with auditing

1. Store the audits securely.
2. The right audit tools will keep the size of the logs under control.
3. The logs must be protected from any unauthorized changes in order to safeguard data.
4. Train the right people to review the data in the right manner.
5. Make sure the ability to delete logs is only available to administrators.
6. Logs should contain activities of all high-privileged accounts (root, administrator).

##### Password Management

* Different types of password management technologies have been developed to get these pesky users off the backs of IT and the help desk by providing a more secure and automated password management system. The most common password management approaches are listed next:
* **Password Synchronization -** Reduces the complexity of keeping up with different passwords for different systems. eg. The password of our Axis, Moodle and Computer system accounts are the same.
* **Self-Service Password Reset** - Reduces help-desk call volumes by allowing users to reset their own passwords.
* **Assisted Password Reset** - Reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens).

###### Password security

* Password generation: system vs user
* Password strength: length, complexity, dynamic…
* Password ageing & rotation
* Limit login attempts

## Week 6: Access Control Practices

### Access Control Practices

* Deny access to systems to undefined users or anonymous accounts.
* Limit and monitor the usage of administrator and other powerful accounts.
* Suspend or delay access capability after a specific number of unsuccessful logon attempts
* Remove obsolete user accounts as soon as the user leaves the company
* Suspend inactive accounts after 30 to 60 days.
* Enforce strict access criteria.
* Enforce the need-to-know and least-privilege practices. （least privilege : giving an employee the only enough rights and privilege to carry out what they are supposed to do and nothing more)
* Disable unneeded system features, services and ports.
* Replace default password settings on accounts.
* Limit and monitor global access rules.
* Remove redundant resource rules from accounts and group memberships.
* Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
* Enforce password rotation.
* Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
* Audit system and user events and actions, and review reports periodically.
* Protect audit logs.

### Security controls

* Safeguards to prevent, detect, correct or minimise security risks.
* Set of actions for data security

#### Definition

Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

#### **Advantages**

* A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.
* The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

#### What is it for?

* They were created to answer the question, "what do we need to do to stop known attacks."
* The key to the continued value is that the Controls are updated based on new attacks that are identified and analysed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

### There are Two ways of categorising Security Controls:

#### 1. Categorising according to nature of the control

* Administrative Controls
* Technical Controls/ Logical Controls
* Physical Controls

#### 2. Categorising according to the different phases of the control process

* Deterrent
* Preventative
* Detective
* Corrective
* Recovery/ Compensatory

Categorising according to nature of the control

### Administrative Controls

These include the developing and publishing of policies, standards, procedures, and guidelines; risk management; the screening of personnel; conducting security-awareness training; and implementing change control procedures.

#### Definition

* Administrative controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organisation's security goals.
* Administrative controls are the process of developing and ensuring compliance with policy and procedures.
* They tend to be things that employees may do, or must always do, or cannot do.

#### Categories of Administrative Controls:

* Policies
* Standards
* Procedures
* Guidelines

#### Examples:

* Policies(Eg. Business Continuity Plan, Access Control Policy, Disaster Recovery Plan）
* Procedures
* Personnel Controls ( Def: Personnel controlling indicates strengths and weaknesses of the company. Its purpose is to effectively exploit the potential of all employees to achieve the maximum benefit within the organisation.）
* Supervisory structure (Def: a board of management of which nonmanagerial workers are members, having supervisory powers over some aspects of management decision-making.)
* Testing ( Eg. Vulnerability Scanning, Penetration Testing, Security Audit/Review, Risk Assessment, Security Scanning)

### Technical Controls (aka Logical Controls)

These consist of implementing and maintaining access control mechanisms, password and resource management, identification and authentication methods, security devices, and the configuration of the infrastructure.

#### Definition:

Technical controls are the hardware and software components that protect a system against cyberattacks. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

#### May refer to：

* identification and authentication methods
* security devices
* configuration of the infrastructure

#### Examples：

##### Preventative

* Encryption
* Smart cards
* Network authentication
* Access control lists (ACLs)
* File integrity auditing software
* patching
* IPS

##### Detective

* Security logs
* NIDS
* HIDS

##### Corrective/Recovery

* IPS
* Restore from backups
* patching

### Physical Controls

Depending on the organization physical security countermeasures will vary. A government agency such as the Department of Defense may have armed guards at the door of the building. Many organizations are not in the position of breaching national security so armed guards are not a necessity. In many cases a receptionist greets any new visitors and makes the appropriate arrangements for an on-site visit.

#### Definition:

These entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls.

#### Examples:

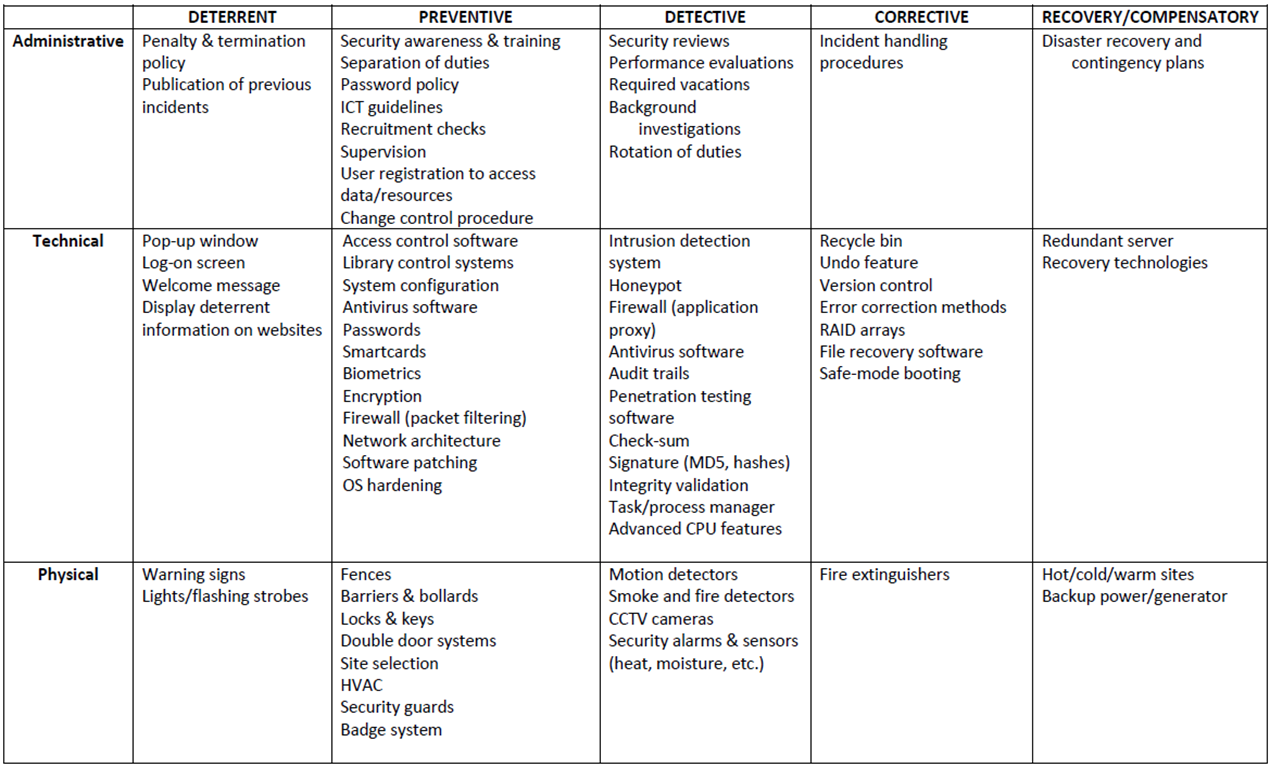
* Automated barriers & bollards
* Building management systems like Heating, HVAC, lifts/elevators control, etc.
* CCTV- Closed Circuit TV
* Electronic article surveillance - EAS
* Fire detection
* GIS mapping systems
* Intercom & IP phone
* Lighting control system
* Perimeter intrusion detection system
* Radar based detection & Perimeter surveillance radar
* Security alarm
* Video wall
* Power monitoring system
* Laptop Locks

### Categorising according to the different phases of the control process

* Deterrent: controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected
* Preventive: controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors
* Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network
* Corrective: corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)
* Recovery: controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

A general example:

Speeding (have fines and punishment, and preventive controls like speed bumps, detection – security cameras)



#### Deterrent:

controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected

#### Preventive:

controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors

#### Detective:

controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network

#### Corrective:

corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)

#### Recovery:

controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

#### Real-life Example

##### Speeding:

deterrent - having fines and punishment, preventive controls like speed bumps, detection security cameras, corrective - enforcement of fines and punishments, recovery -

##### Fire Hazards:

*deterrent* - flyers or advertisements how to prevent fire hazards from happening, *preventive* - making sure no open stoves are left unattended, power sockets are turned off when not in use, *detective* - smoke detectors, cctv at home, *corrective -* fire extinguishers, *recovery -* insurance and funds kept for a rainy day

### Commonly Used Security Methods

To address the key requirements of the AIC triad, one can employ a number of commonly used security methods:

* Least privilege
* Defense-in-depth
* Minimization
* Keep things simple
* Compartmentalization
* Use choke points
* Fail securely/safely
* Leverage unpredictability
* Separation of duties

#### Least Privilege

**States that:** do not provide more privileges than are required. This applies to both users and applications.

* Example: No administrative rights to guests accounts, unidentified applications should not be able to have the power to change the system file etc.)
* This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization’s staff.
* The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage.
* Some examples of application of this principle include the following:
* Giving users only read access to shared files if that’s what they need, and making sure write access is disabled
* Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password
* Not allowing software developers to move software from development servers to production servers
* Privilege : The ability to access data to run processes and applications
* Product: keep system more stable by giving less privilege to untrustworthy users

##### Advantages:

* Minimizes the attack surface, diminishing avenues a malicious actor can use to access sensitive data or carry out an attack by protecting superuser and administrator privileges.
* Reduces malware propagation by not allowing users to install unauthorized applications. The principle of least privilege also stops lateral network movement that can launch an attack against other connected devices by limiting malware to the entry point.
* Improves operational performance with reductions in system downtime that might otherwise occur as a result of a breach, malware spread or incompatibility issues between applications.
* Safeguards against human error that can happen through mistake, malice or negligence.

##### Disadvantages:

The two big problems with least privilege are minimal access and expiration of access.

* Minimal access

When assigning or providing access, in many cases an admin is not sure whether or not someone needs access. In the past, if an admin was not sure if a user needed access, the default rule was to go ahead and provide the user with access. While this potentially minimized support desk calls and user frustration, it introduced considerable risk.

If you provide additional access and it is not needed, no one ever notifies the help desk. Ultimately, providing access to a user beyond what he or she needs to perform his/her role leads to a massively increased attack surface that leaves organizations wide open to damage from hackers and insiders.

* Expiration of access

The second big problem with data access is expiration. In most organizations, once access is provided to a piece of information, it is never removed.Over the course of employment at an organization, as a user’s role and responsibilities change (or the technologies they need to access grow), more access is granted to the user. However, rarely is the previous access, when no longer relevant to a user’s role, removed.

##### Importance:

* The principle of least privilege is an important information security construct for organizations operating in today’s hybrid workplace to help protect them from cyberattacks and the financial, data and reputational losses that follow when ransomware, malware and other malicious threats impact their operations.
* The principle of least privilege strikes a balance between usability and security to safeguard critical data and systems by minimizing the attack surface, limiting cyberattacks, enhancing operational performance and reducing the impact of human error.

#### **Defense in Depth** (multiple types of security controls in different layers)

* The principle of defense in depth is about having more than one layer or type of defense.

##### **Advantage**:

The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach.

##### Disadvantages:

It is usually more costly and time consuming to implement many layers of security.

* Defense in depth works best when you combine two or more different types of defense mechanisms—
* such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

##### Eg.

1st layer – Deterrent control (easy to implement, use it to warn hackers to not attack, breaching policies may not be legal)

2nd layer – Preventive control (Firewall installed on server that monitors all the traffic gg btw the internet and internal network and intercept any suspicious activities)

3rd layer – Detective layer (Network monitoring tools like intrusion detection systems that will alert ppl on any attacks being made on the system)

4th layer – Corrective layer (software installed like antivirus that could get rid of virus that the computer has been infected)

5th layer – Recovery layer (Data backup, another image of the system software for recovery in the event that the system breaks)

Generally, different types of controls should be used together:

* first, preventive controls should be in place to try and prevent security incidents from happening at all;
* second, detective controls are necessary so that you can know whether preventive controls are working or have failed;
* and third, corrective controls are needed to help you respond effectively to security incidents and contain damage.
* However, the defense in depth principle does not mean that you should indiscriminately apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

#### Minimisation

##### ***Purpose/Definition/Principle/****States that:*

the system should not run any applications that are not strictly required to complete its assigned task

* The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration.
* For **example**, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse.

##### **Advantages/Importance**:

* Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.
* Minimisation is also one of the cheapest methods as no additional costs are needed and it can help an organisation save cost on storage as well.
* Data minimization can help you reduce data theft by decreasing your data footprint that requires security. The principle also allows you to limit the number of records that may be affected in case of a data breach, thereby protecting your business against costly fines.

#### Keep Things Simple

Definition/ Principle： a security system should be kept simple as any complexity introduced leads to insecurity in the overall system

* Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure.
* The more complex a system, the less assurance we may have that it will function as expected.
* Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later.
* When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.

#### Compartmentalisation

to prevent the compromise of the entire system, use a compartment approach to the system design and implementation

* Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment is malfunctioning or compromised.

##### Real life example:

It can be best compared to compartments on ships and submarines, where a disaster in one compartment does not necessarily mean that the entire ship or submarine is lost.

##### **Definition**:

Compartmentalization in the information security context means that applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment.

##### Advantages/Importance:

In information security, compartmentalization is equally about spreading the risk so if there’s any impact (breach) we’ve limited the damage to our personal information and the harm and recovery effort are far less.

#### Use Choke Points

##### Purpose:

the traffic can be easier to analyse and control by using choke points

Security is very much about control, and control is so much more effective and efficient when you know all ways in and out of your systems or networks.

##### Definition:

Choke points are logical “narrow channels” that can be easily monitored and controlled.

##### Example:

An example of a choke point is a firewall—unless traffic can travel only via the firewall, the firewall’s utility is reduced to zero. Consider the example of controlled entrances to buildings or facilities of high importance, such as perimeter fencing and guard posts.

##### Importance:

Enforcing choke points increases efficiency.

Attackers typically must go through a series of steps to steal assets. They will often breach defenses, move laterally, escalate privileges, evade detection, then exfiltrate data.

Mapping and prioritizing the choke points that attackers move though when launching attacks is a key approach for ensuring that critical assets stay safe. This strategy can also solve resource constraints — an important advantage for perennially understaffed/under-provisioned IT departments.

##### Advantages:

The greatest advantage of the Choke-Point architecture is its single point of installation. This provides simple installation and reduced IT management. In the case of a Web Proxy Server, access performance may be enhanced due to the caching nature of the proxy.

##### Disadvantages:

There are, however, a number of disadvantages to this architecture. The benefits of having a single point of installation also create a potential single point of failure that must be addressed with redundancy. Since the web filtering and reporting functionality in a Choke-Point environment requires all Web access to occur through a single point, the workstations in the managed environment must be configured to direct Web access to the Choke-Point. It is therefore possible for a user to change their configuration or use alternate means to access the Web. This could include a readily available WiFi connection or a portable Internet access device. In addition, monitoring and filtering remote or mobile users that are not in the managed environment requires the remote workstations to be directed back into the Choke-Point – a highly inefficient means to manage traffic.

##### Conclusion from advantages and disadvantages:

Although somewhat offset by its caching capabilities, Choke-Point installations create a bottleneck to Internet content which, depending on traffic dynamics, may actually cause performance to suffer. In general, with respect to filtering, Choke-Point architectures are used primarily for Web content and typically do not address other Internet communication protocols such as content exposed in email, chat, IM and dark web postings.

Not cost effective as one would need to hire people and funds might be needed to install Choke-points.

#### Fail Securely

##### Definition:

Failing securely means that if a security measure or control has failed for whatever reason, the system is not rendered to an insecure state.

##### Principle:

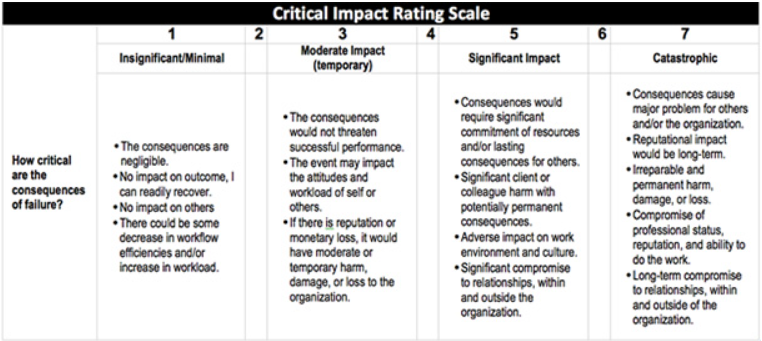
Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied.

##### Example:

For example, when a firewall fails, it should default to a “deny all” rule, not a “permit all.” However, fail securely does not mean “close everything” in all cases; if we are talking about a computer-controlled building access control system, for example, in case of a fire the system should default to “open doors” if humans are trapped in the building. In this case, human life takes priority over the risk of unauthorized access, which may be dealt with using some other form of control that does not endanger the lives of people during emergency situations.

##### Advantages/Importance:

Fail securely is especially important for systems that are accessible to everyone as the traffic flow of such systems would be high, leading to an increase in probability of error or malicious attacks. Failing securely gives operators more time to figure out what went wrong and prevent any undetectable damage.



##### Disadvantage:

Fail securely should not be used for systems where the impact of failure is significant or catastrophic. The consequences of failure, no matter how secure, could cause other major and significant damage such as reputational impact or adverse impact on work environment and culture for some organisations. Thus an organisation should weigh their impacts on the consequences of failure before using the Fail Securely method.

May not be the most expensive option, but is not cheap either because of the cost of such software and human resources to detect errors whenever fail securely happens.

#### Secure the Weakest Link

Many information security principles and approaches may sound like little more than common sense. Although that may well be the case, it doesn’t help us much, because very often we still fail to act with common sense.

##### **Definition/Principle:**

Securing the weakest means to spend your security budget securing the biggest problems and the largest vulnerabilities.

##### **Advantages/Importance:**

Instead of securing the weakest link, whatever it may be, resources are spent on reinforcing already adequate defences. The weakest link is the one most likely to be compromised by a hacker. An organisation's security model should not fall apart just because a part of the business, or a business partner, has weak security. Therefore securing the weakest link is important to decrease the chances of hackers exploiting the flaws of an organisation.

##### Examples:

For example, there are technological solutions already employed to protect the system but no training on how to handle attachments in email messages. Securing the weakest link is the training of employees to handle attachment in email messages.

##### Real life examples:

Addressing the weakest link means you avoid a strategy similar to erecting a gate and expecting an attacker to run straight for it while there are no walls around the gate to limit their access. With a focus on the weakest link, you expend your time and energy on the risks that matter most.

##### Disadvantages:

Should be paired with other methods as well as may not work as well alone.

#### Leverage Unpredictability

##### Definition/Principle:

Do not provide any information about the system's security setup - users and clients can know that a system is in place but they do not need any specific details

##### Example:

Don’t publicise the specifics of their armaments, exact locations, or numbers of armed forces, you should not publicize the details of your security measures and defenses.

##### FYI:

This principle should not be seen as contradicting deterrent security controls—controls that basically notify everyone that security mechanisms are in place and that violations will be resisted, detected, and acted upon. The important difference here is that deterrent controls don’t provide details of the defenses but merely announce their existence so as to deter potential attackers without giving them detailed information that later may be used against the defenders.

##### **Examples:**

In practical terms, this means you can, for example, announce that you are using a firewall that, in particular, logs all traffic to and from your network, and these logs are reviewed by the organisation—there is no need to disclose the type, vendor, or version number of the firewall; where it is located; how often logs are reviewed; and whether any backup firewalls or network intrusion detection systems are in place.

##### Importance:

Providing excessive information about a system’s security set up can lead to key information being lost or stolen, create a poor experience for customers and reputational harm.

#### Segregation of Duties

##### Purpose/Definition:

The purpose of the segregation (or separation) of duties is to avoid the possibility of a single person being responsible for different functions within an organisation, which when combined may result in a security violation that may go undetected. Segregation of duties can prevent or discourage security violations and should be practised when possible.

##### Principle:

Although the actual job titles and organizational hierarchies may differ greatly, the idea behind the principle of separation of duties stays the same: no single person should be able to violate security and get away with it. Rotation of duties is a similar control that is intended to detect abuse of privileges or fraud and is a practice to help your organization avoid becoming overly dependent on a single member of the staff. By rotating staff, the organization has more chances of discovering violations or fraud.

#### Most Cost Effective Method

"Keep things simple" would be the one that would be the cheapest and easiest to implement as its aim is to have less complex solutions and reduce attack surface area and potential vulnerabilities. This can be achieved by reducing the number of components, protocols and systems in a network and reducing the amount of customization. Having a simple design makes it easier to secure, monitor, and maintain.

## Week 7: Busniess Continuity I

### Comprehensive approach to business continuity plan

#### **Prevention**:

risk management plan (this lecture) – what to do to prevent incidents

#### Preparedness

business impact analysis – if incidents do happen, what would be the impact

#### **Response**:

incident response plan – what to do when incidents happen

#### **Recovery**:

recovery plan – how to recover after an incident/disaster

****

Risk Management

### Risk

#### Definition:

An uncertain event that, if it occurs, has a positive or negative effect on objectives

### Risk Management

* A proactive attempt to recognize and manage internal events and external threats that affect the likelihood of success
* What can go wrong (risk event)
* How to minimize the risk event’s impact (consequences)
* What can be done before an event occurs (anticipation)
* What to do when an event occurs (contingency plans)

### Risk management plan consists of three stages

#### Plan

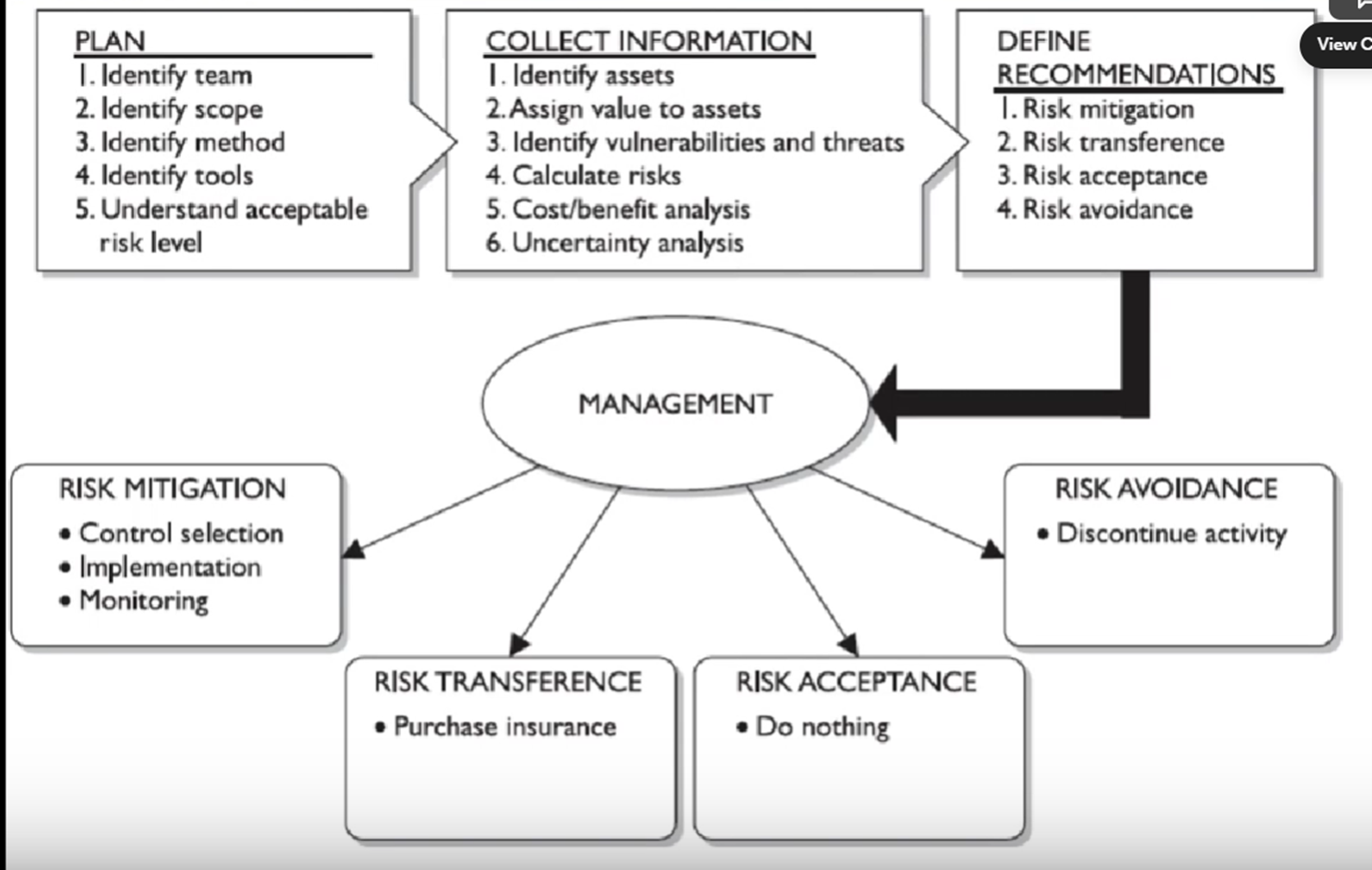
* 1. Identify team
  2. Identify scope
  3. Identify method
  4. Identify tools
  5. Understand acceptable risk level

#### Collect information/perform risk analysis

* 1. Identify assets
  2. Assign value to assets
  3. Identify vulnerabilities and threats
  4. Calculate risks
  5. Cost/benefit analysis
  6. Uncertainty analysis

#### Define recommendations

* 1. Defend the risk: lock the door, install IDS, block specific ports associated with specific attacks
  2. Mitigate the risk: incident response, disaster recovery, and business continuity plans
  3. Transfer the risk: outsource
  4. Avoid/terminate the risk: disable USB port
  5. Accept the risk: do nothing



### How to determine risk

#### Loss/damage

#### Likelihood

##### Definition:

Likelihood is the probability that a specific vulnerability will be the object of a successful attack.

* + In risk assessment, you assign a numeric value to likelihood. The National Institute of Standards and Technology recommends in Special Publication 800-30 assigning a number between 0.1 (low) and 1.0 (high).
  + For example, the likelihood of an asset being struck by a meteorite while indoors would be rated 0.1. At the other extreme, receiving at least one e-mail containing a virus or worm in the next year would be rated 1.0. You could also choose to use a number between 1 and 100 (zero is not used, since vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list). Whichever rating system you choose, use professionalism, experience, and judgment—and use the rating model you select consistently. Whenever possible, use external references for likelihood values that have been reviewed and adjusted for your specific circumstances. Many asset/vulnerability combinations have sources for likelihood, for **Example**:
    - The likelihood of a fire has been estimated actuarially for each type of structure.
    - The likelihood that any given e-mail contains a virus or worm has been researched.
    - The number of network attacks can be forecast based on how many assigned network addresses the organization has.

#### Effectiveness of existing controls

#### Uncertainty of vulnerability knowledge

### Residual risk

For each threat and its associated vulnerabilities that have residual risk, you must create a preliminary list of potential controls. Residual risk is the risk to the information asset that remains even after the application of controls.

#### Definition:

Risk not yet addressed by existing controls

* Residual risk=Total risk x Control gap

If a company addresses 20% of the risk, then the control gap will be 80%

For each threat and its associated vulnerabilities that have residual risk, you must create a preliminary list of potential controls. Residual risk is the risk to the information asset that remains even after the application of controls.

Risk is

the *likelihood* of the occurrence of a vulnerability

**multiplied by**

the *value* of the information asset

**Minus**

The percentage of risk mitigated by *current controls*

**Plus**

The *uncertainty* of current knowledge of the vulnerability

### Risk Management Plan

Risk management plans usually have four, linked, objectives. These are:

1. to eliminate risks;
2. to reduce to ‘acceptable’ levels those that cannot be eliminated; and then either
3. to live with them, exercising carefully the controls that keep them ‘acceptable’; or
4. to transfer them, by means of insurance, to some other organization.

**Risk Management**

Risk management is the process of identifying risk, as represented by vulnerabilities, to an organization’s information assets and infrastructure, and taking steps to reduce this risk to an acceptable level. Each of the three elements in the C.I.A. triad, is an essential part of every IT organization’s ability to sustain long-term competitiveness.

#### Risk management involves three major undertakings*:*

* **Risk identification** is the examination and documentation of the security posture of an organization’s information technology and the risks it faces.
* **Risk assessment** is the determination of the extent to which the organization’s information assets are exposed or at risk.
* **Risk control** is the application of controls to reduce the risks to an organization’s data and information systems

#### Risk management: formal process

The risk assessment must be a formal process. In other words, the process must be planned, and the input data, their analysis and the results should all be recorded.

The process must be planned, and the input data, their analysis and the results should all be recorded.

* Planning
* Documentation
* Assurance

#### Who is to undertake this risk assessment, and How

* Periodic review

The first is that the standard expects that **periodic reviews** of security risks and related controls will be carried out –taking account of new threats and vulnerabilities, assessing the impact of changes in the business, its goals or processes, technology and/or its external environment (such as legislation, regulation or society) and simply to confirm that controls remain effective and appropriate. Periodic review is a fundamental requirement of any risk assessment or risk management strategy.

* Appropriately qualified and experienced person

The second is that it is an assumption of the standard ‘that the execution of its provisions is entrusted to appropriately qualified and experienced people’. It is essential that risk assessment – the core competency of information security management – is conducted by **an appropriately qualified and experienced person**. This is logical; the key step on which the entire ISMS will be built needs, itself, to be solid. The ISO27001 auditor will therefore want to see documentary evidence of the formal qualifications and experience of this person.

**Risk Assessment**

### Quantitative risk assessment

#### Purpose:

Quantitative risk analysis attempts to assign real and meaningful numbers to all elements of the risk analysis process.

#### Example:

These elements may include safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, and so on.

When all of these are quantified, the process is said to be quantitative.

Quantitative risk analysis also provides concrete probability percentages when determining the likelihood of threats. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

#### Limitations:

Purely quantitative risk analysis is not possible because the method attempts to quantify qualitative items, and there are always uncertainties in quantitative values.

#### Issues addressed:

1. the probability of an event occurring and
2. the likely loss should it occur.

A single figure is produced from these two elements, by simply multiplying the potential loss (measured in monetary terms) by its probability (measured as a percentage). This is sometimes called the ‘annual loss expectancy’ (ALE) or the ‘estimated annual cost’ (EAC).

**(ALE) = potential loss ($) x probability (%)**

Clearly, **the higher the number** that an event or risk has, **the more serious** it is for the organization. It is then possible to rank events in order of risk (ALE) and to make decisions based upon this.

#### Limitations/ Disadvantages:

The problems with this type of risk analysis are usually associated with the **unreliability and inaccuracy of the data**. Probability is usually assessed subjectively and is rarely precise. In some cases, this approach can promote or reflect complacency about the real significance of particular risks.

The monetary value of the potential loss is also often assessed subjectively, and when the two components are multiplied together, the answer is equally subjective.

In addition, controls and countermeasures often have to tackle a number of potential events, and the events themselves are frequently interrelated. A detailed ranking in order of ALE can make it difficult to identify these interrelationships and lead to poor decisions about controls, and this approach is not, therefore, recommended.

### Qualitative Risk Assessment/Analysis:

#### **Definition**:

does not assign numbers and monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions.

#### Qualitative analysis techniques include:

1. judgment,
2. best practices,
3. intuition, and
4. experience.

#### Examples of qualitative techniques to gather data are:

Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews.

#### **The risk analysis team**

will determine the best technique for the threats that need to be assessed, as well as the culture of the company and individuals involved with the analysis.

The team that is performing the risk analysis gathers personnel who have experience and education on the threats being evaluated. When this group is presented with a scenario that describes threats and loss potential, each member responds with their gut feeling and experience on the likelihood of the threat and the extent of damage that may result.

### Concepts

#### Single Loss Expectancy

is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the exposure factor (EF), which is the expected percentage of loss that would occur from a particular attack, as follows**:**

**SLE = asset value x exposure factor (EF%)**

where **EF equals the percentage loss** that would occur from a given vulnerability being exploited.

##### Example:

For example, if a Web site has an estimated value of $1,000,000 (value determined by asset valuation), and a deliberate act of sabotage or vandalism (hacker defacement) scenario indicates that 10 percent of the Web site would be damaged or destroyed after such an attack, then the SLE for this Web site would be $1,000,000 0.10 $100,000.

#### **Annualized rate of occurrence (ARO).**

This calculates how often an organisation expects an event. It is simply how often you expect a specific type of attack to occur per year.

##### Example:

a successful deliberate act of sabotage or vandalism might occur about once every two years, in which case the ARO would be 50 percent (0.50), whereas some kinds of network attacks can occur multiple times per second. To standardize calculations, you convert the rate to a yearly (annualized) value. This is expressed as the probability of a threat occurrence.

Once each asset’s worth is known, the next step is to ascertain how much loss is expected from a single expected attack, and how often these attacks occur. Once those values are established, the equation can be completed to determine the overall lost potential per risk. **This is usually determined through an annualized loss expectancy (ALE), which is calculated from the ARO and SLE, as shown here:**

**ALE = SLE x ARO**

Using the example of the Web site that might suffer a deliberate act of sabotage or vandalism and thus has an SLE of $100,000 and an ARO of 0.50, the ALE would be calculated as follows:

ALE = $100,000 x 0.50 = $50,000

#### **The Cost Benefit Analysis (CBA) Formula**:

Subtract the revised ALE, estimated based on the control being in place, known as **ALE(post)**. Complete the calculation by subtracting the **annualized cost of the safeguard (ACS).**

**CBA = ALE(prior) - ALE(post) - ACS**

### Risk Assesment

#### Disadvantages of Risk Assessment:

Risk assessment can be a time-consuming process to meet standards

#### Tools to asses and handle threats

There are an increasing number of software tools available that can, to a varying extent, automate the risk assessment process and generate the statement of applicability.

Use of tools is optional, organisations need to examine their pros & cons

#### Purpose:

In theory, such a tool ought to encourage the user to perform a thorough and comprehensive security audit on the organization’s information systems, and ought not to produce too much paperwork as a result.

The organization will need to compare tools before making a selection and should concentrate, in the comparison process, on the extent to which the tool really does easily and effectively automate the risk assessment and statement of applicability development process; the amount of additional paperwork it generates; the flexibility it offers for dealing with changing circumstances and frequent, smaller-scale risk assessments; and the meaningfulness of the results it generates. Of course, normal due diligence should also be done into the status of the supplier and manufacturer of the product to ensure that it is properly supported and likely to continue to be. References might also be sought from happy customers. ( Tools could generate and plot graphs or templates for risk assessment from surveys)

#### Cons/Disadvantages of using RA tools:

* Organisation would be too dependent on these risk assessment tools
* Everytime an organisation hires new people they would have to train the new people on how to use these softwares

#### Alternatives if RA tools are not used:

Risk assessments can, with difficulty, be done without using such tools.

A thorough risk assessment of any significant business will be very time- consuming, and even more so if a software tool is not used.

‘Time-consuming’ means up to three months, or even longer for larger organizations. The use of a software tool will depend on the culture of the organization and the preferences of the information security adviser and manager.

Practically speaking, once the organization has decided to purchase such a tool, it becomes dependent on that tool and on the staff members who are trained to use it. In considering the appropriate route forward, consideration should be given to the speed with which incoming staff can become familiar with the chosen risk assessment tool; practicality and ease of use are likely to be key attributes

### Risk Analysis

#### Importance:

* Controls usually should not cost more than the amount of damage that is being reduced. Thus an organisation should compare the cost of the control and the benefit that you reap from the control in terms of reducing the quantitative risk. Implement the control if the benefit outweighs the cost. If the cost is too high then the control is not worth it, an organisation can then choose to accept the risk. Through risk analysis, an organisation could compare and rank the risk based on which is important and address the important threat first.
* Security can be quite complex, even for well- versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security components, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of money that should be applied to protecting against those risks in a sensible manner.

#### Purpose:

identify weaknesses, potential attacks and estimate potential damage

#### Definition:

Risk analysis, which is really a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security safeguards. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

#### **A risk analysis has four main goals**:

1. Identify assets and their value to the organization.
2. Identify vulnerabilities and threats.
3. Quantify the probability and business impact of these potential threats.
4. Provide an economic balance between the impact of the threat and the cost of the countermeasure.

#### What Risk Analysis do:

Risk analysis provides a cost/benefit comparison, which compares the annualized cost of safeguards to the potential cost of loss. A safeguard, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the safe- guard itself.

Example: This means that if a facility is worth $100,000, it does not make sense to spend $150,000 trying to protect it. It is important to figure out what you are supposed to be doing before you dig right in and start working.

Anyone who has worked on a project without a properly defined scope can attest to the truth of this statement. Before an assessment and analysis is started, the team must carry out project sizing to understand what assets and threats should be evaluated. Most assessments are focused on physical security, technology security, or personnel security. Trying to assess all of them at the same time can be quite an undertaking.

#### What should be done by a team:

##### Team:

The team’s tasks is to create a report that details the asset valuations. Senior management should review and accept the lists, and make them the scope of the IRM project. If management determines at this early stage that some assets are not important, the risk assessment team should not spend additional time or resources evaluating those assets.

##### **During discussions**:

With management, everyone involved must have a firmunderstanding of the value of the security AIC triad (availability, integrity, and confidentiality) and how it directly relates to business needs.

##### Management:

should outline the scope, which most likely will be dictated by organizational governance, risk management, and compliance as well as budgetary constraints. Many projects have run out of funds, and consequently stopped, because proper project sizing was not conducted at the onset of the project.

##### Importance and purpose:

A risk analysis helps integrate the security program objectives with the company’s business objectives and requirements. The more the business and security objectives are in alignment, the more successful the two will be. The analysis also helps the company draft a proper budget for a security program and its constituent security components. Once a company knows how much its assets are worth and the possible threats they are exposed to, it can make intelligent decisions about how much money to spend protecting those assets.

##### Management:

A risk analysis must be supported and directed by senior management if it is to be successful. Management must define the purpose and scope of the analysis, appoint a team to carry out the assessment, and allocate the necessary time and funds to conduct the analysis. ***It is essential for senior management to review the outcome of the risk assessment and analysis and to act on its findings.***

### Strategies to Address Risks

#### Strategies to address risks:

1. Defend
2. Transfer
3. Mitigate
4. Terminate/Avoid
5. Accept

##### Defend

###### **Purpose**:

* To reduce the likelihood of the risk coming through.

###### How it is carried out:

1. **The defend control strategy attempts to prevent the exploitation of the vulnerability.**

* This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards.
* Organizations can mitigate risk to an asset by countering the threats it faces or by eliminating its exposure. It is difficult, but possible, to eliminate a threat.

For example, in 2002 McDonalds Corporation, which had been subject to attacks by animal rights cyberactivists, sought to reduce risks by imposing stricter conditions on egg suppliers regarding the health and welfare of chickens. This strategy was consistent with other changes made by McDonalds to meet demands from animal rights activists and improve relationships with these groups.

1. **Another defend strategy is the implementation of security controls and safeguards to deflect attacks on systems and therefore minimize the probability that an attack will be successful.**

* An organization with dial-in access vulnerability, for example, may choose to implement a control or safeguard for that service. An authentication procedure based on a cryptographic technology, such as RADIUS (Remote Authentication Dial-In User Service), or another protocol or product, would provide sufficient control. On the other hand, the organization may choose to eliminate the dial-in system and service to avoid the potential risk

##### Transfer

###### Purpose:

The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations.

###### How it is carried out:

Contact the other party if the risk comes through. This can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

###### Example:

many organizations want Web services, including Web presences, domain name registration, and domain and Web hosting. Rather than implementing their own servers and hiring their own Webmasters, Web systems administrators, and specialized security experts, savvy organizations hire an ISP or a consulting organization to provide these products and services for them. This allows the organization to transfer the risks associated with the management of these complex systems to another organization that has experience in dealing with those risks. A side benefit of specific contract arrangements is that the provider is responsible for disaster recovery, and through service level agreements is responsible for guaranteeing server and Web site availability.

##### Mitigate

The mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

**This approach requires the creation of three types of plans**:

* the incident response plan,
* the disaster recovery plan, and
* the business continuity plan.

##### Terminate

###### Definition/Purpose:

The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. (Terminate what you are doing that causes the risk)

###### How it is done:

If an organization studies the risks from implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential benefits, the organization may seek an alternate mechanism to meet customer needs perhaps developing new channels for productdistribution or new partner- ship opportunities. By terminating the questionable activity, the organization reduces the risk exposure.

##### Accept (Especially if the risk is relatively low)

###### Purpose:

The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation. This may or may not be a conscious business decision.

**The only industry-recognized valid use of this strategy occurs when the organization has done the following:**

1. Determined the level of risk
2. Assessed the probability of attack
3. Estimated the potential damage that could occur from attacks
4. Performed a thorough cost benefit analysis
5. Evaluated controls using each appropriate type of feasibility
6. Decided that the particular function, service, information, or asset did not justify the cost of protection

**This strategy is based on the conclusion that the cost of protecting an asset does not justify the security expenditure.**

###### Example

suppose it would cost an organization $100,000 per year to protect a server. The security assessment determined that for $10,000 the organization could replace the information contained in the server, replace the server itself, and cover associated recovery costs. In this case, management may be satisfied with taking its chances and saving the money that would normally be spent on protecting this asset. If every vulnerability in the organization is handled by means of acceptance, it may reflect an inability to conduct proactive security activities and an apathetic approach to security in general. It is not acceptable for an organization to adopt a policy that ignorance is bliss and hope to avoid litigation by pleading ignorance of its obligation to protect employee and customer information. It is also unacceptable for management to hope that if they do not try to protect information, the opposition will assume that there is little to be gained by an attack. The risks far outweigh the benefits of this approach.

**Acceptance as a strategy is often mistakenly chosen based on the school of fish’s justification that sharks will not come after a small fish in a school of other small fish. But this reasoning can be very risky.**

### Asset Management

Assets may be **tangible (computers, facilities, supplies) or intangible (reputation,** data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change over time.

#### Tangible Assets

Definition: Physical form, assets that can be sell in the market for fixed value

#### Intangible Assets

Definition: Non-physical form

An asset can have both quantitative and qualitative measurements assigned to it, but these measurements need to be derived.

#### How the value is derived

* The actual value of an asset is determined by the **cost** it takes to **acquire, develop, and maintain it.**
* The value is determined by the importance it has to the owners, authorized users, and unauthorized users. Some information is important enough to a company to go through the steps of making it a trade secret.
* The value of an asset should reflect all identifiable costs that would arise if the asset were actually impaired.

#### Example:

If a server cost $4,000 to purchase, this value should not be input as the value of the asset in a risk assessment. Rather, the cost of replacing or re- pairing it, the loss of productivity, and the value of any data that may be corrupted or lost must be accounted for to properly capture the amount the company would lose if the

server were to fail for one reason or another.

#### The following issues should be considered when assigning values to assets:

1. Cost to acquire or develop the asset
2. Cost to maintain and protect the asset
3. Value of the asset to owners and users
4. Value of the asset to adversaries
5. Value of intellectual property that went into developing the information
6. Price others are willing to pay for the asset
7. Cost to replace the asset if lost
8. Operational and production activities affected if the asset is unavailable
9. Liability issues if the asset is compromised
10. Usefulness and role of the asset in the organization

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the company to not protect the asset.

### Change Management

#### Definition:

process of implementing changes in a controlled manner for e.g. maintaining information integrity.

#### Importance:

* Changes often happen on a very frequent basis e.g. I few are writing a piece of program, we are writing it incrementally, everytime a change ais made we have to push for those changes. That’s why we need standard procedures for pushing changes.
* Unmanaged changes to IT systems and networks can recklessly increase risk to enterprises. The key is rolling out an accepted change management process, and sticking to it.

#### There are different kinds of changes.

* Standard changes: low risk, follow standard procedure
* Approved by top-management : should follow the process of change management

#### Examples

Changes can be in the hardware or software of the system, patches or updates, new technology like facial recognition. Updates in the policy or when businesses are acquired by other businesses. All these changes need to go through change management. **For minor changes such as adding a user or changing some non-critical user configurations, may not need to follow change management procedures.**

Unmanaged changes to IT systems and networks can recklessly increase risk to enterprises. The key is rolling out an accepted change management process, and sticking to it.

#### Disadvantages/ Limitations/ Downsides:

Many of the exposures associated with lack of change management are more complex and subtle than in the example. This is due to the complex nature of today's network environments. Networks are complicated ecosystems and dependencies are not always clear, especially to someone who only sees part of the whole system at a time. A database administrator changing an IP address could lead to a critical service outage. A router administrator that configures a new static route may inadvertently redirect or block traffic from hundreds of remote offices.

#### Purpose:

The purpose of change management is to prevent unintended consequences, such as the ones described, and ensure that changes or alterations to systems are implemented according to an approved framework or model. That's not something many employees would argue with. The problem occurs when an employee, such as the firewall admin in our example above, thinks that circumventing the system will allow things to work more efficiently--or feels that following the processes somehow detracts from getting "real work" done. So the challenge is not simply putting change management in place, but also gaining buy-in from all users of the system so that they're incented to follow the change management process rather than circumvent it.

#### Recommended auditing change management in following areas:

1. Acceptance
2. Awareness
3. Policies and Procedures
4. Tools and Automation
5. Skills and Expertise
6. Responsibility and Accountability
7. Measurement

Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is non-existent, it is incumbent on IS’s senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organisations can demonstrate increased agility in responding predictably and reliably to new business demands.

<Organisation> (hereafter called ‘the company’) management has recognised the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks.

This policy applies to all parties operating within the company’s network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company’s data networks. No employee is exempt from this policy.

### Change Procedure

The change management structure should be codified as an organization policy. Procedures for the operational aspects of the change management process should also be created. Change management policies and procedures are forms of directive controls. The following subsections outline a recommended structure for a change management process.

#### Requests:

Proposed changes should be formally presented to the committee in writing. The request should include a detailed justification in the form of a business case argument for the change, focusing on the benefits of implementation and costs of not implementing. Can assign priority to these changes.

#### Impact Assessment:

Members of the committee should determine the impacts to operations regarding the decision to implement or reject the change.

#### Approval/Disapproval:

Requests should be answered officially regarding their acceptance or rejection.

#### Build and Test:

Once the proposal has been approved, the software would have to be put in an isolated environment but one that iss similar to the production system to test whether if everything works. Subsequent approvals are provided to operations support for test and integration development. A fallback plan should be in place such that the organisation would be able to recover from those unsuccessful changes. Go back to the previous working stage. The fallback has to be put in place before the testings are carried out.

The necessary software and hardware should be tested in a nonproduction environment. All configuration changes associated with a deployment must be fully tested and documented. The security team should be invited to perform a final review of the proposed change within the test environment to ensure that no vulnerabilities are introduced into the production system. Change requests involving the removal of a software or a system component require a similar approach. The item should be removed from the test environment and have a determination made regarding any negative impacts.

#### Notification:

System users and stakeholders are notified of the proposed change and the schedule of deployment.

#### Implementation:

The change is deployed incrementally, when possible, and monitored for issues during the process.

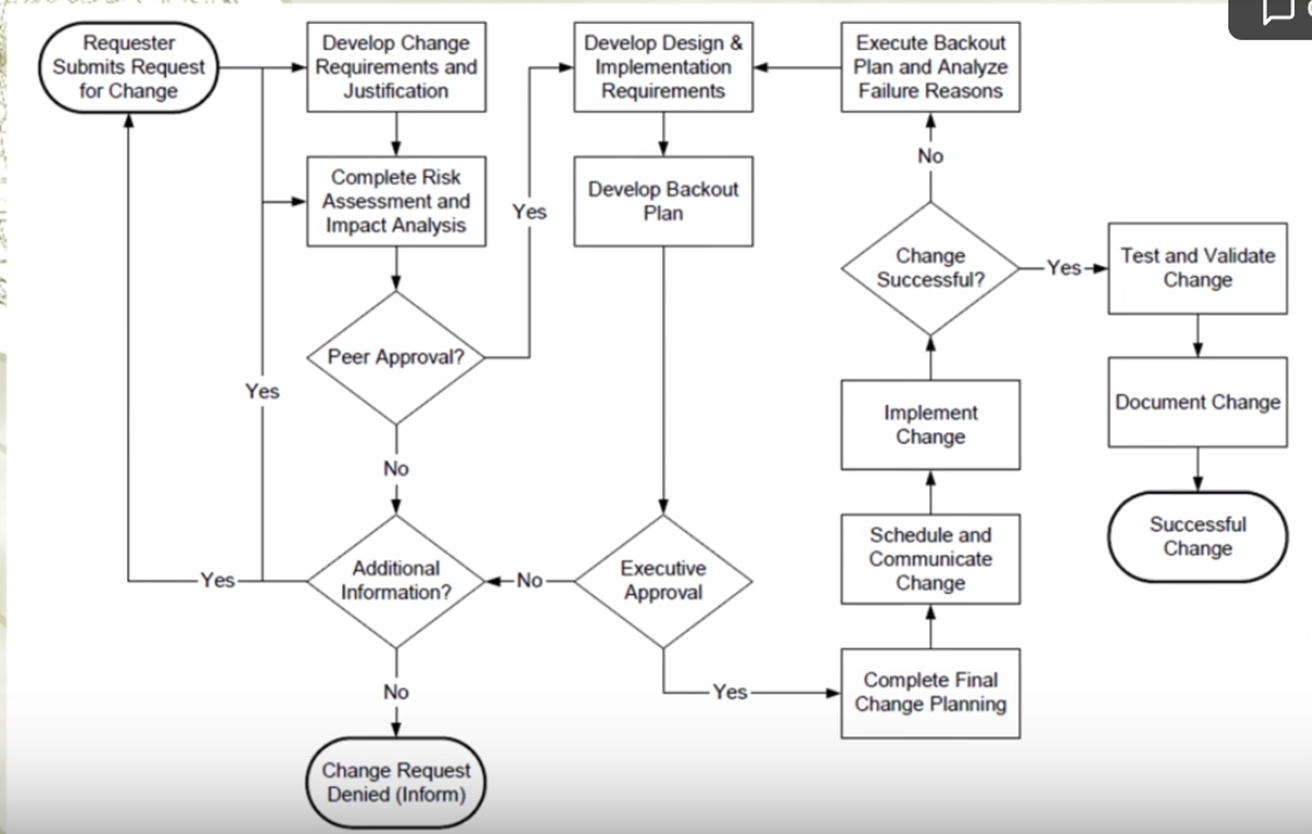
#### Validation:

The change is validated by the operations staff to ensure that the intended machines received the deployment package. The security staff performs a security scan or review of the affected machines to ensure that new vulnerabilities are not introduced. Changes should be included in the problem tracking system until operations has ensured that no problems have been introduced.

#### Documentation:

The outcome of the system change, to include system modifications and lessons learned, should be recorded in the appropriate records. This is the way that change management typically interfaces with configuration management.

### Basic Change Management Workflow

****

#### Change Review

##### Change Monitoring

* Checking the desired functionality
* Monitoring network, server, performance

###### Importance of CM:

After a period of time, if a bug suddenly comes up, the organisation would still have to document the issue and escalate it.

**How:**

Different tools could be used to monitor these changes.

##### Measuring success of the change:

###### Technical objectives:

whether the changes accomplishes everything that it is set to accomplish, and that there are no technical issues.

###### Business objectives:

ensure that the changes that are made meet business objectives e.g. if it is set to increase productivity, ensure that is being met. Or if it is set to have solve certain issues, whether that goal is being met.

##### Change Management Assessment

Assessing change management as a culture, whether it has been properly adhered to or whether the employees are not aware of it or accept the change management procedures. The organisation can run audits on the change management process to see if it is working.

##### Business Continuity

If any changes are made, business continuity plans should be maintained accordingly.

**This policy applies to all parties operating within the company’s network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company’s data networks. No employee is exempt from this policy.**

**In order to fulfil this policy, the following statements shall be adhered to:**

**Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.**

**Operational Procedures**

**Operational Procedures**

The change control process shall be formally **defined and documented**. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures).

This documented process shall **include management responsibilities and procedures**. Wherever practicable, operational and application change control procedures should be integrated.

##### What Change Management should include

**Should include (at the least) the following phases:**

1. Logged Change Requests;
2. Identification, prioritisation and initiation of change;
3. Proper authorisation of change;
4. Requirements analysis;
5. Inter-dependency and compliance analysis;
6. Impact Assessment;
7. Change approach;
8. Change testing;
9. User acceptance testing and approval;
10. Implementation and release planning;
11. Documentation;
12. Change monitoring;
13. Defined responsibilities and authorities of all users and IT personnel;
14. Emergency change classification parameters.

##### Documented Change

**All change requests shall be logged**

whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

###### Documented audit trail

A documented audit trail, **maintained at a Business Unit Level**, containing relevant information shall be maintained at all times. This should **include change request documentation, change authorisation and the outcome of the change.** No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

### Risk Management

* A risk assessment shall be performed for all changes and dependant on the outcome.
* An impact assessment should be performed.
* The impact assessment should include
* the potential effect on other information resources
* potential cost implications.
* consider compliance with legislative requirements and standards.

#### Change Classification

All change requests shall be prioritised in terms of

* benefits,
* urgency,
* effort required and
* potential impact on operations.

#### SLA’s (Service Level Agreements)

**Changes affecting SLA‘s**

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

#### Version Control

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

#### Testing

Changes shall be tested in an i**solated, controlled, and representative environment** (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

#### Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

#### Communicating changes (and involve the users!)

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

#### Implementation

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

#### Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

#### Documentation

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

#### Business Continuity Plans (BCP)

#### 

Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

#### Emergency Changes

Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

#### Change Monitoring

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

### Roles and responsibilities(From highest rank to lowest)

#### Members of the Board

* Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.

#### Information Security Manager

* Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries;
* Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards;
* Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;
* Co-ordinate the overall communication and awareness strategy for change management;
* Acts as the management champion for change management and control;
* Provide technical input to the service requirements and co-ordinate affected changes to SLA’s where applicable.
* Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and
* Co-ordinate the implementation of new or additional security controls for change management.

#### Operations Manager

* Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders;
* Approve and authorise change management and control measures on behalf of the <Organisation>;
* Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;
* Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums;
* Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control;
* Establish and revise the information security strategy, policy and standards for change management and control;
* Facilitate and co-ordinate the necessary change management and control initiatives within each company;
* Report and evaluate changes to change management and control policies and standards;
* Co-ordinate the overall communication and awareness strategy for change management and control;
* Co-ordinate the implementation of new or additional security controls for change management and control
* Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified;
* Provide regular updates on change management and control initiatives and the suitable application;
* Evaluate and recommend changes to change management/ version control solutions; and
* Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company.
* Establish and implement the necessary standards and procedures that conform to the Information Security policy;
* Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all <ORGANISATION> companies and divisions;
* Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control.
* Ensure the compliance of this policy and report deviations to the Information Manager.

#### IT Service Provider

* Shall comply with all change management and control statements of this policy.

#### Solution Owners

* Shall comply with all information security policies, standards and procedures for change management and control; and
* Report all deviations.

### IT Governance Value statement

Changes that materially affect the financial process must be evaluated and reported at some interval. Financial system upgrades or replacements will require new certification. The implication is that Sarbanes-Oxley compliance is reliant on the changes you make to the operational systems and procedures.

### Policy Access Considerations

All IT personnel

Business Unit Management teams

Executive Directors

## Week 8: Business Continuity Planning II

### Business Continuity Planning

#### Definition:

Business continuity planning (BCP) is a process designed to reduce the organisation’s business risk arising from an unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organisation.

#### BCP purposes:

* Reduce business risks
* Make sure that any disruptions and losses due to the incidents or disasters are minimised

#### Advantages:

* keep your business trading during and after an incident
* recover operations more quickly after interruptions
* reduce costs and duration of any disruption
* mitigate risks and financial exposure
* build customer confidence and trust
* safeguard company reputation
* develop confidence within the business
* comply with regulatory or legal requirements
* insure against otherwise unacceptable risks
* save lives, if dangerous events (such as a fire) occur

#### Importance:

A business continuity plan positions your organization to survive serious disruption. It eliminates confusion common to every disaster, providing a clear blueprint for what everyone should do.

### Disaster Recovery Planning

#### *DRP purposes:* (part of RBCP) aka Contingency Plans

* Coordinating recovery after a disaster
* Often referred to as restoring information system and operational facilities after a disaster.

A disaster recovery plan should have at least the following components:

* recovery coordinator
* recovery team
* recovery analysis and planning
* damage assessment and salvage operations
* recovery communications
* employee support and assistance.

Preparing for an emergency typically involves:

* Planning
* Practising
* Rehearsing
* Evaluating
* Adjusting

There should be well documented procedures, strategies etc. This requires setting up an Emergency Response Team and inclusion of that information in BCP.

Team should have general and local responsibilities.

They should for example facilitate evacuation and shut down, protect companies properties and potentially cooperate with local authorities such as fire department.

Depending on the type of disasters, there could be different plans.

#### Importance:

A DRP aims to help an organization resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimum level.

#### Advantages:

* Cost-Efficiency.
* Increased Employee Productivity.
* Greater Customer Retention.
* A Better Understanding of Scalability.

### Difference between BCP and DRP

BCP is a process designed to reduce the organizations business risk arising from and unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization, whilst DRP typically details the process IT personal still follow to restore the computer system and the operational facilities after a disaster.

### Disasters

Definition: Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting business operations.

There are three classifications of threats that can cause disasters:

#### Natural

* earthquakes, floods, tornados, severe thunderstorms and fire etc.

#### Environmental

* Power shortages, staff shortages, unavailability resources, electrical power, telecommunications, equipment failure and software error etc.

#### Human

* operator error, terrorist attacks, hacker attacks or viruses etc.

### BCP Process

The business continuity planning process can be divided into the following lifecycle phases:

1. *Develop the continuity planning policy statement.* Write a policy that provides the guidance necessary to develop a BCP, and that assigns authority to the necessary roles to carry out these tasks.
2. *Conduct the business impact analysis (BIA)*. Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities and threats, and calculate risks.
3. *Identify preventive controls.* Once threats are recognized, identify and implement controls and countermeasures to reduce the organization’s risk level in an economical manner.
4. *Develop recovery strategies.* Formulate methods to ensure systems and critical functions can be brought online quickly.
5. *Develop the contingency plan.* Write procedures and guidelines for how the organization can still stay functional in a crippled state.
6. *Test the plan and conduct training and exercises.* Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.
7. *Maintain the plan.* Put in place steps to ensure the BCP is a living document that is updated regularly.

#### Initiation Process of BCP

The BCP effort has to result in a sustainable, long-term program that serves its purpose—assisting the organization in the event of a disaster. The effort must be well thought out and methodically executed. It must not be perceived as a mere “public relations” effort to make it simply appear that the organization is concerned about disaster response. The **initiation process** for BCP might include the following:

* Setting up a budget and staff for the program before the BCP process begins. Dedicated personnel and dedicated hours are essential for executing something as labor-intensive as a BCP.
* Setting up the program would include assigning duties and responsibilities to the BCP coordinator and to representatives from all of the functional units of the organization.
* Senior management should kick off the BCP with a formal announcement or, better still, an organization-wide meeting to demonstrate high-level support. Awareness-raising activities to let employees know about the BCP program and to build internal support for it.
* Establishment of skills training for the support of the BCP effort.
* The start of data collection from throughout the organization to aid in crafting various continuity options.
* Putting into effect “quick wins” and gathering of “low-hanging fruit” to show tangible evidence of improvement in the organization’s readiness, as well as improving readiness.

### Business Impact Analysis

Business Impact Analysis is assisting the design of our contingency which is assuming that bad things will happen. BIA is in the Preparedness stage.

Risk Management includes controls that help the organisation prevent bad things from happening. Risk Management is in the Prevention stage.

*Three steps* are typically involved in accomplishing the BIA:

1. Determine mission/business processes and recovery criticality. Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.
2. Identify resource requirements.

Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

1. Identify recovery priorities for system resources.

Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources. **Evaluate the impact of ceasing to perform these activities and identify priorities/ assign priorities**

1. Identify an acceptable level of loss may pertain to recovery criticality (recovery parameters)

The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

* **Maximum Tolerable Downtime (MTD)**. The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
* **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
* **Recovery Point Objective (RPO).** The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

#### <Recovery Parameters>

##### Maximum tolerable downtime (MTD)

Definition: outage time that can be tolerated by the company as a result of various unfortunate events

The BIA identifies which of the company’s critical systems are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the maximum tolerable downtime (MTD) or maximum period time of disruption (MPTD)

The following are some MTD estimates that an organization may use. Note that these are sample estimates that will vary from organization to organization and from business unit to business unit:

* **Nonessential** 30 days
* **Normal** 7 days
* **Important** 72 hours
* **Urgent** 24 hours
* **Critical** Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the company can survive without it. These estimates will help the company determine what backup solutions are necessary to ensure the availability of these resources. The shorter the MTD, the higher priority of recovery for the function in question. Thus, the items classified as Urgent should be addressed before those classified as Normal.

###### Examples

* For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line could be considered Critical and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the Normal category, and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor’s service level agreement (SLA), which may promise to have it back online in eight days.
* Sometimes the MTD will depend in large measure on the type of business in question. For instance, a call center—a vital link to current and prospective clients—will have a short MTD, perhaps measured in minutes instead of weeks. A common solution is to split up the calls through multiple call centers placed in differing locales. If one call center is knocked out of service, the other one can temporarily pick up the load. Manufacturing can be handled in various ways. Examples include subcontracting the making of products to an outside vendor, manufacturing at multiple sites, and warehousing an extra supply of products to fill gaps in supply in case of disruptions to normal manufacturing.

##### The recovery point objective (RPO)

Definition: determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data.

The Recovery Point Objective (RPO) is the acceptable amount of data loss measured in time. This value represents the earliest point in time at which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster.

##### The recovery time objective (RTO)

Definition: determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume after disaster.

* The Recovery Time Objective (RTO) is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.
* The RTO value is smaller than the MTD value, because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization’s reputation or bottom line.
* The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is sinking too fast to properly recover.

##### Work Recovery Time

Definition: The Work Recovery Time (WRT) is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything “live” for production purposes.

—-------------------------------------------------------------------------------------------------------------------------------------

Both RPO and RTO are based on time parameters. **The lower the time requirements, the higher the cost of recovery strategies.**

* If the RPO is in minutes (lowest possible acceptable data loss) then data mirroring should be implemented as the recovery strategy.
* If the RTO is less, then the alternate site might be preferred over a hot-site contract.
* The lower the RTO, the lower the disaster tolerance. Disaster tolerance is a time gap within which the business can accept the non-availability of IT facilities.

##### Examples of Recovery Parameters

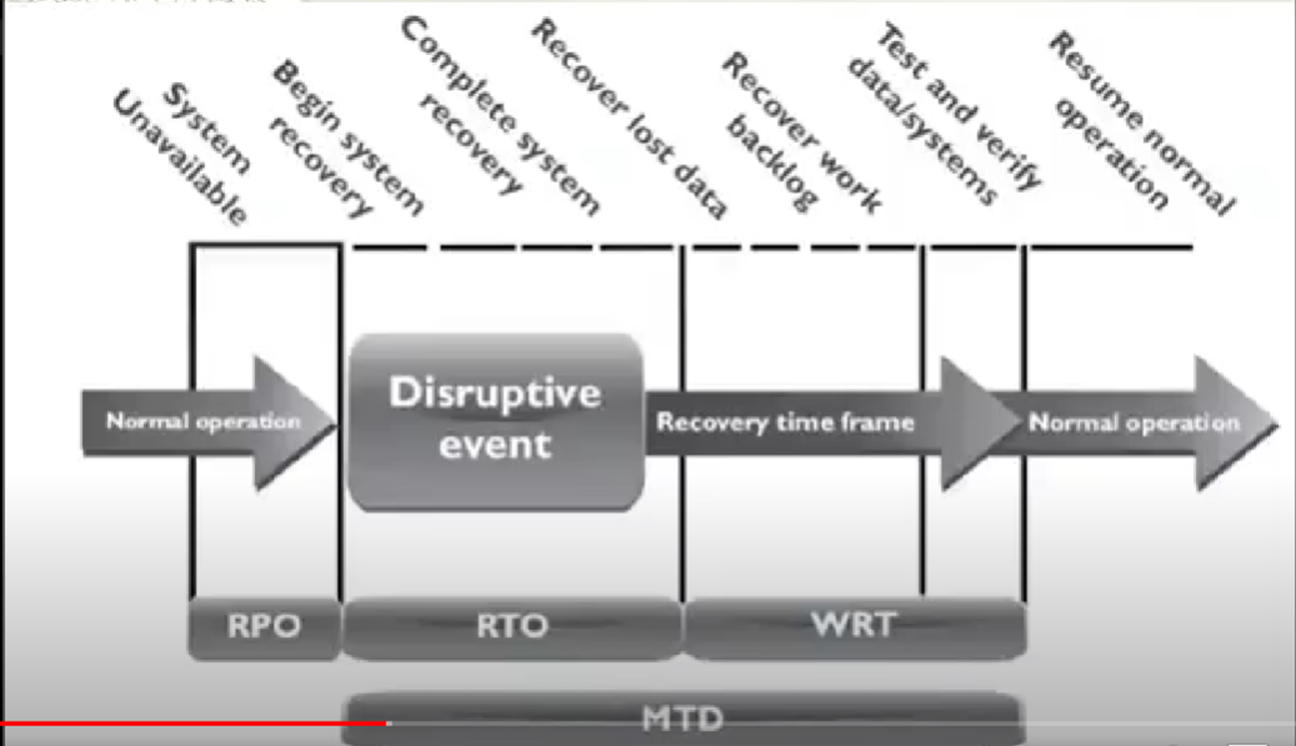
The RTO, RPO, and WRT values are critical to understand because they will be the basic foundational metrics used when determining the type of recovery solutions a company must put into place, so let’s dig a bit deeper into them.

* RTO is the duration of time and a service level that a business process must be restored to in order to ensure that unacceptable consequences associated with a disaster are not endured.
* Let’s say a company has determined that if it is unable to process product order requests for 12 hours, the financial hit will be too large for it to survive. So the company develops methods to ensure that orders can be processed manually if their automated technological solutions become unavailable. But if it takes the company 24 hours to actually stand up the manual processes, the company could be in a place operationally and financially where it can never fully recover. So RTO deals with “how long do we have to get everything up and working again?”
* Now let’s say that the same company experienced a disaster and got its manual processes up and running within two hours, so it met the RTO requirement.
* But just because business processes are back in place, we still might have a critical problem.
* The company has to restore the data it lost during the disaster. It does no good to restore data that is a week old. The employees need to have access to the data that was being processed right before the disaster hit.
* If the company can only restore data that is a week old, then all the orders that were in some stage of being fulfilled over the last seven days could be lost. If the company makes an average of $25,000 per day in orders and all the order data was lost for the last seven days, this can result in a loss of $175,000 and a lot of unhappy customers. So just getting things up and running (RTO) is part of the picture. Getting the necessary data in place so that business processes are up to date and relevant (RPO) is just as critical.

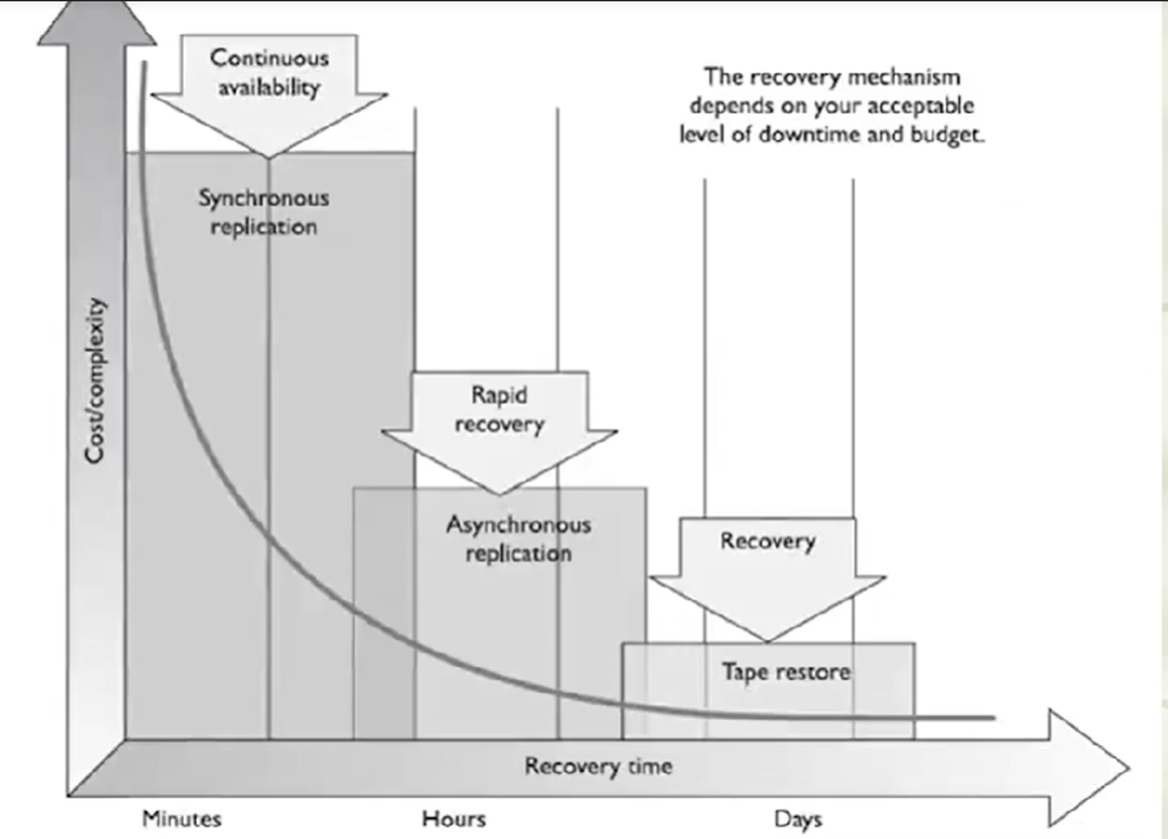
The actual MTD, RTO, and RPO values are derived during the BIA. The impact analysis is carried out to be able to apply criticality values to specific business functions, resources, and data types.

* The company must have data restoration capabilities in place to ensure that mission-critical data is never older than one minute. The company cannot rely on something as slow as backup tape restoration, but must have a high-availability data replication solution in place.
* The RTO value for mission-critical data processing is two minutes or less. This means that the technology that carries out the processing functionality for this type of data cannot be down for more than two minutes.
* The company may choose to have a cluster technology in place that will shift the load once it notices that a server goes offline.

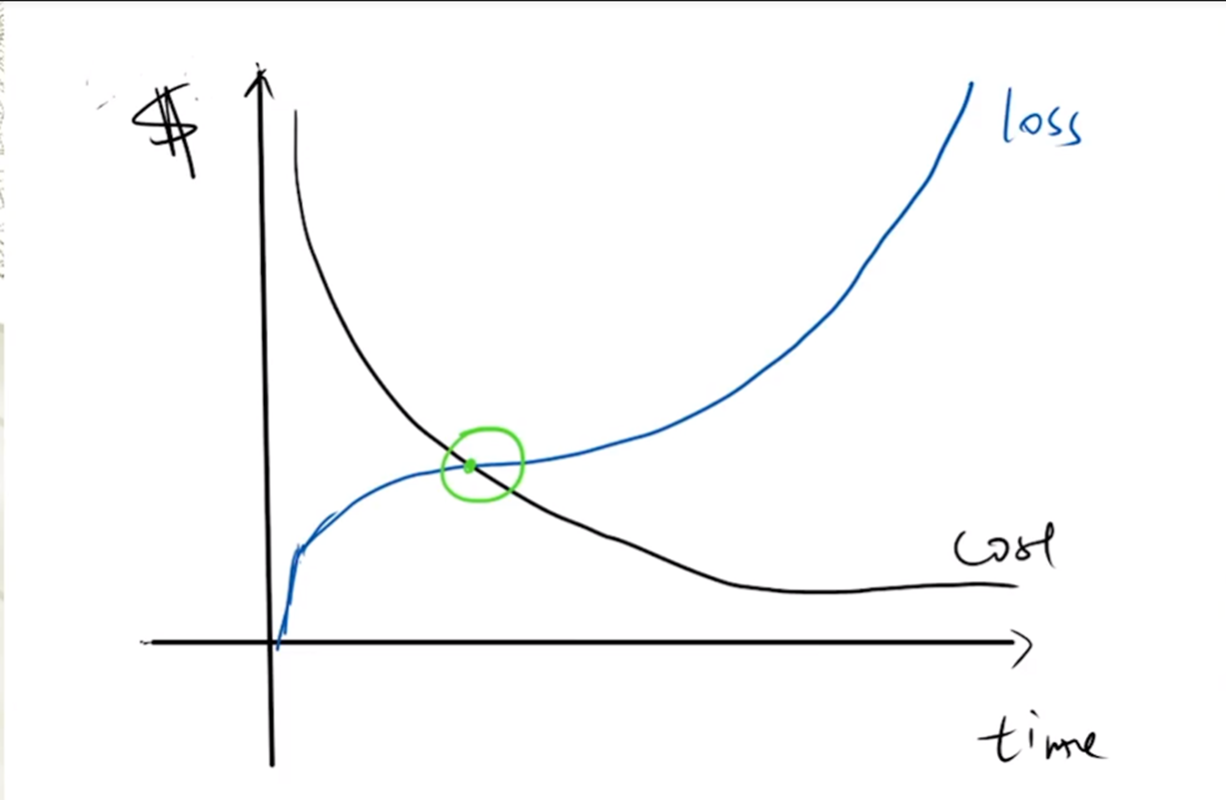
##### Recovery Parameters Timeline



##### Recover Time over Complexity of Method



##### Optimum time to set RPO, MTD and RTO

****

* Cost of recovering is more than the cost of loss with every unit of time that passes before the Optimum time. The method may not be worth its price.
* Cost of loss is more than the cost of recovery with every unit of time that passes after the Optimum time. Loss due to damage is too high.

### Offsite Facilities (related to RTO)

#### Alternate Processing Facilities

* Hot sites
* Warm sites
* Cold sites
* Mobile sites
* Reciprocal agreements

For larger disasters that affect the primary facility, an offsite backup facility must be accessible.

Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need, and then incurs an activation fee when the facility actually has to be used.

In addition, there would be a daily or hourly fee imposed for the duration of the stay. This is why subscription services for backup facilities should be considered a short-term solution, not a long-term solution.

It is important to note that most recovery site contracts do not promise to house the company in need at a specific location, but rather promise to provide what has been contracted for somewhere within the company’s locale. On, and subsequent to, September 11, 2001, many organizations with Manhattan offices were surprised when they were redirected by their backup site vendor not to sites located in New Jersey (which were already full), but rather to sites located in Boston, Chicago, or Atlanta. This adds yet another level of complexity to the recovery process, specifically the logistics of transporting people and equipment to unplanned locations.

**Companies can choose from three main types of leased or rented offsite facilities:**

##### Hot site

* A facility that is leased or rented and is fully configured and ready to operate within a few hours.
* The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data.
* The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues.
* Some facilities, for a fee, store data backups close to the hot site. These sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible.
* Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state of readiness.
* This is the most expensive of the three types of offsite facilities. It can pose problems if a company requires proprietary or unusual hardware or software.

##### Warm site

* A leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers.
* In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers.
* Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices.
* This is the most widely used model. It is less expensive than a hot site, and can be up and running within a reasonably acceptable time period. It may be a **better choice for companies that depend upon proprietary and unusual hardware and software**, because they will bring their own hardware and software with them to the site after the disaster hits. Drawbacks, however, are that much of the equipment has to be procured, delivered to, and configured at the warm site after the fact, and the annual testing available with hot-site contracts is not usually available with warm-site contracts. Thus, a company cannot be certain that it will in fact be able to return to an operating state within hours.

##### Cold site

* A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services.
* A cold site is essentially an empty data center.
* It may take weeks to get the site activated and ready for work.
* The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks. However, it would require the receipt of equipment from the client, since it does not provide any.
* **(Advantages vs Disadvantages)** The cold site is the least expensive option, but takes the most time and effort to actually get up and functioning right after a disaster, as the systems and software must be delivered, tweaked, and configured.
* Cold sites are often used as backups for call centers, manufacturing plants, and other services that can be moved lock, stock, and barrel in one shot.

#### Conclusion

Most companies use warm sites, which have some devices such as disk drives, tape drives, and controllers, but very little else.

These companies usually cannot afford a hot site, and the extra downtime would not be considered detrimental.

A warm site can provide a longer-term solution than a hot site. Companies that decide to go with a cold site must be able to be out of operation for a week or two. The cold site usually includes power, raised flooring, climate control, and wiring.

#### The following provides a quick overview of the differences between offsite facilities:

##### Hot Site Advantages

* Ready within hours for operation
* Highly available
* Usually used for short-term solutions, but available for longer stays
* Annual testing available

##### Hot Site Disadvantages

* Very expensive
* Limited on hardware and software choices

##### Warm and Cold Site Advantages

* Less expensive
* Available for longer timeframes because of the reduced costs
* Practical for proprietary hardware or software use

##### Warm and Cold Site Disadvantages

* Operational testing not usually available
* Resources for operations not immediately available

#### Tertiary Sites

* During the BIA phase, the team may recognize the danger of the primary backup facility not being available when needed, which could require a tertiary site.
* This is a secondary backup site, just in case the primary backup site is unavailable. The secondary backup site is sometimes referred to as a “backup to the backup.” This is basically plan B if plan A does not work out.

#### Reciprocal Agreements

* Another approach to alternate offsite facilities is to establish a reciprocal agreement with another company, usually one in a similar field or that that has similar technological infrastructure.
* This means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability.
* To allow another company to come in and work out of the same shop could prove to be detrimental to both companies. Whether it can assist the other company while tending effectively to its own business is an open question. The stress of two companies working in the same environment could cause tremendous levels of tension.
* If it did work out, it would only provide a short-term solution. Configuration management could be a nightmare. Does the other company upgrade to new technology and retire old systems and software? If not, one company’s systems may become incompatible with that of the other company?

##### Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

* How long will the facility be available to the company in need?
* How much assistance will the staff supply in integrating the two environments and ongoing support?
* How quickly can the company in need move into the facility?
* What are the issues pertaining to interoperability?
* How many of the resources will be available to the company in need?
* How will differences and conflicts be addressed?
* How does change control and configuration management take place?
* How often can drills and testing take place?
* How can critical assets of both companies be properly protected?

#### Offsite Location

* When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed.
* There is a rule of thumb that suggests that alternate facilities should be, at a bare minimum, at least 5 miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50 to 200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

#### Redundant Sites

* Some companies choose to have redundant sites, or mirrored sites, meaning one site is equipped and configured exactly like the primary site, which serves as a redundant environment.
* The business-processing capabilities between the two sites can be completely synchronized. These sites are owned by the company and are mirrors of the original production environment.
* A redundant site has clear advantages: it has full availability, is ready to go at a moment’s notice, and is under the organization’s complete control.
* This is, however, one of the most expensive backup facility options, because a full environment must be maintained even though it usually is not used for regular production activities until after a disaster takes place that triggers the relocation of services to the redundant site.
* But expensive is relative here. If the company would lose a million dollars if it were out of business for just a few hours, the loss potential would override the cost of this option. Many organizations are subjected to regulations that dictate they must have redundant sites in place, so expense is not an issue in these situations.

### Contingency Plans ( Discovery Recovery Planning: DRP)

#### Supporting information & Appendices

1. Business impact analysis
2. Emergency contacts
3. Recovery procedures

#### Main phases

1. Activation and notification
2. Recovery
3. Reconstitution

There are five main components of the information system contingency plan (ISCP). The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency.

##### Supporting information and Appendices

* (What it includes) The supporting information component includes an **introduction and concept of operations section** providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain.
* (What for) These details **aid in** understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.
* (What it includes) This section may contain the **roles and responsibilities** section and presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams.
* (What for) The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

##### Activation and Notification Phase

* The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan.
* At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.
* **Activation criteria**: The ISCP should be activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority should activate the plan
* **Notification procedures**: An outage or disruption may occur with or without prior notice.

For example, advance notice is often given that a hurricane is predicted to affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act.

Notification procedures should be documented in the plan for both types of situation.

The procedures should describe the methods used to notify recovery personnel during business and non business hours.

Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

Following the outage or disruption, notification should be sent to the Outage Assessment Team so that it may determine the status of the situation and appropriate next steps.

When outage assessment is complete, the appropriate recovery and system support personnel should be notified.

* **Outage assessment:** To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption.

The outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption.

Once impact to the system has been determined, the appropriate teams should be notified of updated information and the planned response to the situation

##### Recovery Phase

* Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.
* At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan.
* Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.
* **Sequence of Recovery Activities:** The sequence of activities should reflect the system’s MTD to avoid significant impacts to related systems.

Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner.

If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured.

These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records.

References to applicable appendices, such as equipment lists or vendor contact information, should be made in the plan where necessary.

Procedures should clearly describe requirements to package, transport, and purchase materials required to recover the system.

* **Recovery Procedures:** To facilitate Recovery Phase operations, the ISCP should provide detailed procedures to restore the information system or components to a known state. Procedures should be assigned to the appropriate recovery team and typically address the following actions**:**

1. Obtaining authorization to access damaged facilities and/or geographic area;
2. Notifying internal and external business partners associated with the system;
3. Obtaining necessary office supplies and work space;
4. Obtaining and installing necessary hardware components;
5. Obtaining and loading backup media;
6. Restoring critical operating system and application software;
7. Restoring system data to a known state;
8. Testing system functionality including security controls;
9. Connecting system to network or other external systems; and
10. Operating alternate equipment successfully.

Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly.

* **Recovery Escalation and Notification:** Effective escalation and notification procedures should define and describe the events, thresholds, or other types of triggers that are necessary for additional action.

Actions would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources.

Procedures should be included to establish a clear set of events, actions and results, and should be documented for teams or individuals as appropriate.

##### Reconstitution Phase

The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality.

During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements.

This phase consists of two major activities: validating successful recovery and deactivation of the plan.

* **Validation of recovery typically includes these steps:**
* **Concurrent Processing.** Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.
* **Validation Data Testing.** Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.
* **Validation Functionality Testing.** Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

At the successful completion of the validation testing, ISCP personnel will be prepared to declare that reconstitution efforts are complete and that the system is operating normally. The ISCP Coordinator must determine if the system has undergone significant change and will require reassessment and reauthorization.

* Deactivation of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:
* **Notifications.** Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.
* **Cleanup.** Cleanup is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.
* **Offsite Data Storage.** If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.
* **Data Backup.** As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.
* **Event Documentation.** All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts.

An after-action report with lessons learned should be documented and included for updating the ISCP. Once all activities and steps have been completed and documentation has been updated, the ISCP can be formally deactivated. An announcement with the declaration should be sent to all business and technical contacts.

# Tutorial

## Tutorial: Week 5 Access Controls

Question 1

What are the three (3) different factors that are used for authentication? For each factor, give an example. Finally, describe a situation where a combination of at least two factors is necessary and briefly explain why

Three diff factors

1. Sth a person knows (Pwd Pin)
2. Sth a person has (Token)
3. Sth a person is (Biometrics Thumbprint, Thumb, Iris)

Two Factors Necessary (Choose 2 from above)

* Companies Card access and Biometrics to verify identity
* Companies Pin and Thumbprint
* Internet Banking Pin and Message sent to phone

**Question 2**

One important requirement when assigning value to an identity is that the value must be non-descriptive.

Explain what it means by ‘‘non-descriptive” and why it is required so.

Neither piece of the cred set shld indicate the purpose of the acct

Eg. user id not (backup op, ceo, administrator) - does not show who it belongs to

**Question 3**

Describe two types of technical controls that can be used for building access and specify which one you would use for low-security set-up required to protect a generic PC lab against unauthorised entry.

Access cards, biometrics, Pin (personal id number)

Low security - Biometrics, Pin, Access Card,

\* Need to write what type of biometrics

**Question 4**

Describe two types of technical controls that can be used for building access and specify which one you would use for low-security set-up required to protect a generic PC lab against unauthorised entry.

To be able to

Detect intrusion

reconstruct events and system conditions

provide legal recourse material

**Question 5**

Physical controls are often neglected when security systems are developed but nonetheless they are a critical component of an effective security solution. Describe two physical preventive types of controls as well as two physical detective types of controls and specify a scenario in which a combination of the two is necessary.

Physical Preventives

* Turnstiles
* Automated barriers
* Bollards

Physical Detectives

* Cctv
* smoke detector

Scenario

CCTV and Biometrics (Data Centre)

Technical Real Life examples:

* Online banking includes the:
* technical preventive controls such as (Passwords)
* Technical deterrent (Message on website to prevent people from hacking
* Technical detective (Audit)
* School security system
* Technical preventive (Passwords)
* Technical deterrent (Message on website to prevent people from hacking)
* Technical detective (Antivirus software)
* Technical Corrective (Recycle bin)
* Technical Recovery (Recovery technologies)

Administrative Real life examples:

* Big organisations:
* Administrative deterrent (Penalty and termination policy)
* Administrative preventive (Security awareness and training)
* Administrative detective (Security reviews, performance evaluations)
* Administrative Corrective (Incident handling procedures)
* Administrative recovery (Contingency plans and Disaster recovery plans)

**Question 6**

When developing a security system, it is important to plan for cases which the preventive measures in place fail and, consequently, the system integrity is compromised. From a security perspective what are the two main avenues that are generally considered for continuity/restoration of services?

Access controls fail

If fail, integ comprom

(Backup - offsite storage backups(Offline)

Ensure restoration of services, test the backup so that the backup will not fail (once in 6 mths or once a yr)

**Question 7**

The integrity principle in the context of data security deals with the correctness of the data and the aim is to prevent damage from personnel inside or outside the organization. What is the first measure that needs to be put in place to help with the data integrity protection?

Implement access controls. Users will only have limited access, this reduces the chance that a basic mist can result in a maj damage to the data that is being protected.

**Question 8**

Explain the difference between corrective and recovery controls.

Recovery controls are for recovering more serious situations from damage.

**Corrective control**

Example:

Recycle bin in Windows helps to correct accidental deletion. When an item is accidentally deleted, it goes into the recycle bin and users are still able to retrieve the files within a specific amount of time.

**Recovery control**

Example:

Chkdsk which helps to recover files that have been erased.

**CHKDSK**

It is not a data recovery tool and will not recover lost or damaged files. CHKDSK will simply ensure the information currently on the disk is in a consistent and safe state. If files are damaged, the CHKDSK utility attempts to separate the damaged files and save the remnants as Filenn.chk. This reorganisation of bad sectors can cause further problems. There have been many discussions or forums whereby CHKDSK has failed to repair a file and made it worse! The best advice we can give is to never run CHKDSK with the automatic repair option enabled.

<http://www.datarecoveryspecialists.co.uk/blog/chkdsk-data-recovery#:~:text=Will%20CHKDSK%20recover%20data%3F,save%20the%20remnants%20as%20Filenn>.

**Question 9**

Many organizations develop security systems which are focused entirely on physical and technological security controls. Explain why this is insufficient and provide examples how the security could be compromised.

Cyber security has 3 main aspects: People, Process, Systems

We need **Administrative Controls** as well.

If overlooked, an experienced attacker will be able to breach the security set up because the issue of information ownership is properly handled.

Thus an attacker may not need to break into the better protector systems as the access to confidential information is unlikely to be thoroughly control.

Example of lack of **Administrative Control**

Email to all users instead of only those that should have access to it.

Disposal of older hardware is not done in a secure manner and harddrives are simply thrown into a bin in from which an attacker can extract critical information such as passwords or confidential records.

**Question 10**

What is CERT-Australia? What is AusCERT? What is ASD? Why is it important from a data security point of view to know about each of them?

**C.E.R.T -** Computer Emergency Response Team

**CERT Australia** is the national computer emergency response team. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

**AusCERT** is a non-profit organisation that provides advice and solutions to cybersecurity threats and vulnerabilities. The organisation covers their costs through member subscriptions, attendees to the annual AusCERT conference and service contracts.

CERT educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Knowing about each of them allows us to be better prepared in tackling cyber-security threats.

**Question 11**

What is sender policy framework (SPF)? Explain the type of attacks that SPF addresses.

The Sender Policy Framework (SPF) is an email authentication protocol and part of email cybersecurity used to stop phishing attacks. It allows your company to specify who is allowed to send email on behalf of your domain.

This is useful because in a typical phishing attack, the threat actor spoofs the sender address to look like an official business account or someone the victim may know.

**Targets**

* Email spoofing
* Phishing attacks

**How**

The protection of your outbound email is implemented by configuring a TXT record in your public DNS which lists the servers that are allowed to send email from your mail domain. Nothing is configured on the mail server itself.

The Sender Policy Framework (SPF) email authentication method aims to reduce spam and fraud by making it harder for email senders to hide their identity. SPF detects email spoofing by providing a process to verify who is permitted to send emails on your behalf.

## Tutorial: Week 6 Security Controls

**Question 1**

* Give an example of administrative preventive controls that addresses Confidentiality and briefly explain how.
* Give an example of technical corrective controls that addresses Integrity and briefly explain how.

Confidentiality - No leak (the secrecy of the data is maintained at all times)

Availability - Users must be able to use the system when they need to (The systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance.)

Integrity - No modifications and Accuracy( Accuracy and reliability of information

Prevent unauthorised and improper modifications)

Three types of control

* Administrative controls
* Technical (Software part eg. penetration testing) controls
* Physical controls

**Preventive controls**:

Training of employees about security awareness. Eg. enhances security awareness of phishing attacks.

How: With security awareness training, users will be able to identify and spot phishing emails that attempt to steal account information

**Technical Controls**:

Recycle bin in windows helps to recover files that are accidentally deleted by authorised users.

**Question 2**

Describe one (1) example of administrative preventive controls and one (1) example of physical recovery controls, both of which must address Availability. For each example, briefly explain how it helps address availability.

**Availability**

Definition: The systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance.

**Administrative**

(The soft part of things: Policy, trainings, procedures, software based)

* Policy that prevent unauthorised people from entering
* Change control procedure, change management ensure that new software development will not crash existing appication due to thorough testing.
* Penetration testing

**Physical**

(Physical part of things, Physical infrastructure)

Backup sites, Backup systems, Warm site, cold site, UPS (Uninterruptible Power Supply), Hot sites, Backup power so that when a system is down, data can be retrieved from the backup sites and will thus will make the data available as quickly as possible. (Example + how it addresses availability)

**Question 3**

A small health organization has asked for advice in regards to improving its security system. The organization is already implementing a defense-in-depth mechanism which combines a firewall with the encryption of traffic to prevent confidential information being accessed by unauthorised personnel. The company has very limited funding and you can only suggest two additional security mechanisms (security methods) to be considered. Describe the mechanism you have selected and justify your selection.

\* Defence in depth - Different layers of controls

Small organisation and limited funding (sugg solutions must address these constraints)

Touches on commonly used security methods

**Minimisation (similar to least privilege)**

* applies to system configuration
* States that one should not run any software, applications or services that are not strictly required to the entrusted job
* Eg. computer which only function is to serve as an email server, should only have the email server and software installed on the computer, all other services as per protocols should either be disabled or not installed at all to eliminate any possibility of the compromise or misuse
* Advantages: Increases security and improve performance, save storage space and is also a good system administration in practice.
* Principle: hardening the organisation server by disabling the services that are redundant or removing programs that are not necessary in order to reduce the attacks on the server
* Summary: able to harden org server, disable unnecessary services, restrict accesses, perform on a need to basis, use the least privilege principal
* Does not need require company to buy solutions, only need to use the current system that the organization has and enforce such principals

**Leverage unpredictability**

* Eg. announce on the organisation website web that using firewall that logs all traffic to and from the network and the logs are reviewed by the organisation
* No need to disclose the type and vendor of the firewall, where it is located, the frequency of use and any backup firewalls or network disruption detections are put in place
* Principle in this case: telling the public about the existence of such security controls, public able to get the gist of what is happening in the organisation and warn them about the effects of trying to compromise the security of the organisation

**Question 4**

A retailer is selling goods via both physical and online stores. The online store allows customers to create their own accounts, update personal and financial information, order goods, and track order status. It also links to the inventory management back-end. It has been suggested that three universal security methods; Least privileges, Compartmentalisation, and Defense-in-depth need to be used to enhance the security of the system. Describe your interpretation of these three (3) security methods in this particular scenario. (Definition, Example, Principle, Advantage and Disadvantages)

\*Physical and online store

**Least privileges**

Do not grant users or the staff more privilege than they should have. Only give them the privileges they need for their duties.

**Compartmentalisation**

Definition: Putting things into different categories

Parts

Web server ( in demilitarised zone DMZ)

Front end systems and Backend systems

**Compartmentalise :**

* segregation of front end systems from the back end systems
* If they are not in physical servers, they can be on virtual machines
* Users able to retrieve webpage from web servers without accessing any materials on the backend
* Pulling happens when information is transferred from one system to another (eg. info keyed in -> inventory -> management -> system -> person reads and sends order to warehouse -> ship)

**Defence in depth**

Multiple layers to the defence: Online stall has personal and financial information. In order to protect the info, multiple layers need to be used.

Layers : (Outer to inner layer) Firewall. Intrusion detection system (IDS). Secure data with encryption. Search for more information and examples on these layers

(two layer firewall: internet facing and internal facing firewall)

**Question 5**

With the help of an example, explain the principle Fail securely.

* Definition : If a security measure or control has failed, the system is not rendered to an insecure state.
* Eg. firewall fails, shld fall towards a deny all rule instead of permit all ( Firewall: There are many firewall rules. Person whos job is to key,delete, amend and add firewall rule. Eg. users cannot access the database servers and only the web servers. Because database server is in the internal network. Firewall rule states who can access what etc. on 80, there is http protocol bec access the webpage stored in web server. Firewall has a particular deny all rule : unless all rules are followed, deny all rule is activated)

\* Does not mean close everything in all cases

* Physical example: Building access control system: Doors should open when there is a fire should default to open doors when humans are trapped in the buildings instead of close as human lives takes priority over the risk of unauthorised access which may be dealt with using other forms of controls that does not endanger the lives of people during emergency situations.

**Question 6**

With the help of an example, explain why the principle of minimization is important from the point of view of system security. (Definition, Example, Principle, Advantage, Importance)

Minimisation Principle: Only run applications that are strictly necessary to perform its tasks and nothing more because when there are more applications running, the higher the chance for something to go wrong and the security will be compromised

A common approach to breach security is to attack services which are running on a host machine, such as Telnet.

TELNET is commonly used by terminal emulation programs that allow you to log into a remote host. However, TELNET can also be used for terminal-to-terminal communication and interprocess communication. TELNET is also used by other protocols (for example, FTP) for establishing a protocol control channel.

To limit the number of options for hackers, it is imperative to shut down all services that are not essential to improve the running of the system.

An application may have weaknesses that can be exploited and thus, if they are not running, the system will be more secure.

Disabling redundant services is a major task to server hardening. With minimisation principle, the priority is to have the least privileges as possible

Example:

In the case of the Firewall Rule in minimisation principle, port 80, HTTP is the protocol. Inside the firewall, there are alot of protocols and ports. For example:

* FTP(File Transfer Protocol: works on a client-server model, it is a standard communication protocol used for the transfer of computer files from a server to a client on a computer. FTP is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections.) protocol in port 21.
* TELNET is in port 23.
* SSH is another service is in port 22.
* SMTP (Simple Mail Transfer Protocol: for mail services) in port 25

Minimisation: disable services that you do not need, unnecessary services should be disabled eg. If an organisation does not need to use FTP, disable FTP bec FTP is not secure as FTP transfer files in clear files.

* Instead of having FTP, use SFTP (Secure File Transfer Protocol)
* Since TELNET is also not secure as TELNET also send files in clear text, disable TELNET and enable SSH (Secure Shell) instead.

**Ports and Protocols**

As per its word definition, a protocol is a set of rules. In computer networking, a protocol defines a standard way for computers to exchange information. Most common protocols used in computer networks and the internet are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and IP (Internet Protocol).

A port in computer networking is a logical access channel for communication between two devices. Bi-directional communications and more complex connections may use multiple ports (channels) simultaneously.

Data on the Internet is organised into standard TCP or UDP packets. Network clients use different ports (or channels) to transfer this data. Generally one port is used to send data and another to receive it, so packets don't collide. The port number (and the destination IP address) is included as part of the header each packet is given. Ports range from 1 to 65535 for the TCP and UDP protocols.

**Question 7**

You are asked to give an advice on the security set-up for a medical research laboratory which has computer terminals connected to a server that stores sensitive information. a) Suggest two physical preventive controls and two physical detective controls that can be used and explain your choice. b) The laboratory is going to provide an Internet presence to assist researchers in finding information online. However, this raises a serious concern that the sensitive information is accessed by intruders from the outside world. Under the defense-in-depth principle, suggest specific security solutions for at least two layers of defense that may be deployed to mitigate the risk.

**Physical Preventive:**

(Since it is in a medical research lab, assume that it is a physical site)

Security guards, Bollard, Biometrics Access Control

Backup Files (in case of an attack)

**Physical Detective** :

CCTV, Smoke Detectors, Fire alarm

**Defense-in-depth:**

**(**eg. having a preventive, detective and corrective control)

* Preventive - firewall (stops bad traffic before it enters the network)
* Detective - Intrusion detection system, Logging (helps to detect malicious activities)
* Corrective - Backups (helps to restore the data damaged or modified by intruders)

**Question 8**

It is often suggested to suspend or delay access capability after a number of unsuccessful login attempts. Describe the reason behind this suggestion and clearly indicate what security threat this recommended practice addresses.

This helps prevent hackers from carrying out Brute force attack, Password guessing when it is done automatically.

**Question 9**

With the help of examples explain the differences between three universal security principles/methods:

Least privilege, Minimization, and Keep things simple. (Definition, Advantages and Disadvantages, Principles, Importance)

**Least Privilege**

Normal users do not have the same level of power as compared to administrators. Normal users should not be able to change, view system critical files. Normal users are given as least privilege as possible.

**Minimisation**

Disable redundant services or services that are unnecessary for example FTP, TELNET.

**Keep things simple**

For making decisions between different choices, pick the one that does the job but simple. Not making things difficult.

**Question 10**

The logon screen of workstations in an organisation reads ”Warning: All activity is constantly monitored and logged, including hostname and IP address.”

Explain the purpose of this notice and determine the type of security control and the universal security method of this practice.

(Types of security control - Preventive, Deterrent, Detective, Corrective, Recovery)

(Universal security method - Commonly used security methods)

**Purpose: (based on this scenario)**

**Deterrent control**

This is used to discourage malicious activities by users. Users will know that people at the backend will be able to see their activities.This security method leverages unpredictability.

## Tutorial: Week 7 Business Continuity 1

Question 1

Risk analysis is an integral part of the process of developing a security system. What is risk analysis used for and how does it influence the overall security system?

Risk Management, Risk Assessment and Risk Analysis

Risk Management: Risk management is the overall management to manage risks. Risk Assessment is only part of risk management. Risk management also involves planning and monitoring/maintaining that are not covered in risk assessment.

Risk assessment: is part of risk management and is a framework to manage risk at a particular point in time.

Risk analysis is the actual step carried out to quantify impact, likelihood of different risk items in order to determine the risk levels and for making recommendations.

* Risk analysis is used primarily to identify the threats oto an organisation’s assets and to estimate the potential damage that ma need to be dealt with if any of the threats turned out to be real.
* For example, risk analysis may be used to determine what threats one needs to deal with when protecting a medical database and the cost associated with a case in which some patient records are accessed by unauthorised persons.

Question 2

An important step in risk analysis is to determine the value of an asset. Give five (5) different questions you think might help with the task of determining the asset value.

Questions:

How much is the cost to acquire

How much is the value of the asset to adversaries

How much is the price others are willing to pay for the assets.

Other questions:

* Cost to acquire or develop the asset
* Cost to maintain and protect the asset
* Value of the asset to owners and users
* Value of the asset to adversaries
* Price others are willing to pay fo the asset
* Cost to replace the asset if lost
* Operational and production activities affected if the asset is unavailablie
* Liability issues if the asset is compromised
* Usefulness and role of the asset in the organisation

Question 3

Give two (2) examples of intangible assets and explain why it is often more difficult to determine the value of an intangible asset than a tangible one.

Eg. Rep and data

Hard to quantify values of intangible assets which may change over time.

Tangible: eg. computers, harddrive and facilities

Assets may be tangible(computers, facilities, supplies) or intangible (reputation, data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change overtime. How do you put a monetary value on a company’s reputation? This is not always an easy question to answer, but it is important to do so.

Question 4

A backup data centre is located in a remote area. It has been determined that in the event of a severe cyclone, which happened twice in the last 40 years, the backup data centre suffers 50% damage. The cost to rebuild the centre is currently $1 million. What is the single loss expectancy for the centre suffering from such a severe cyclone? What is the annualised loss expectancy? If the insurance premium for such events is $10,000 per annum, would it be wise to consider insuring the centre to address the risk? Explain your reasoning.

SLE = asset value x exposure factor

SLE is the loss that you experience to the asset due to the event, in this case is 1mil, therefore (1mil x 50%) , SLE = 500k

ALE = SLE x ARO

500k x (2/40) = 10k

Since, 10k<25k, lt is wise to pay an insurance premium of $10,000 to cover a potential damage of $25,000 from a cost-benefit perspective.

Other possible answer:

Last 40 years - Twice (Very ambiguous)

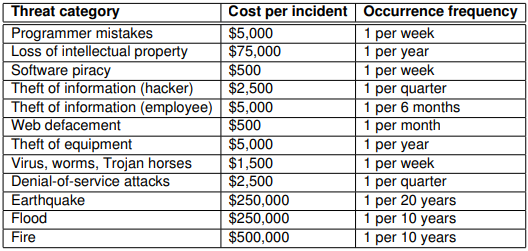
1 year -> (1/40)\*(2) = 0.5% (Exposure Factor)

SLE -> 500k

ALE = 500k x (1/20) = 25k (May be fixed or minimum or maximum)

Question 5

Consider the following risk analysis of a software company

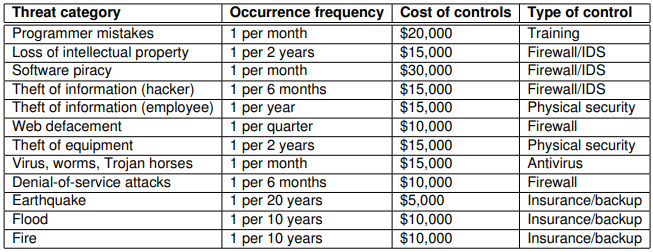


Calculate the SLE, ARO, and ALE for each threat category listed in the above table.

• How did the software company arrive at the values shown in the table?

• Assume that the company has implemented controls to address the risk shown in the analysis

and the new figures after one year are shown below. Assume that the cost per incident figures are still the same. Recalculate SLE, ARO, and ALE values for each category. Comment on the results.



SLE = Cost of the Incident x 1 (for all because it only takes into account one incident and the overall frequency for all is 1)

ARO

1. 52 = 1 x 52weeks
2. 1

ALE

1. $260 000= 52 x $5000

If ALE after is the same or more than the ALE before, the control is not effective

Answer:

| Threat Category | Cost/Incident  ($) | Occurence freq. | SLE | ARO | ALE |
| --- | --- | --- | --- | --- | --- |
| Programmer mistakes | 5,000 | 1 per week | 5,000 | 52.0 | 260,000 |
| Loss of intellectual property | 75,000 | 1 per year | 75,000 | 1.0 | 75,000 |
| Software piracy | 500 | 1 per week | 500 | 52.0 | 26,000 |
| Theft of information (hacker) | 2,500 | 1 per quarter | 2,500 | 4.0 | 10,000 |
| Theft of information (employee) | 5,000 | 1 per 6 months | 5,000 | 2.0 | 10,000 |
| Web defacement | 500 | 1 per month | 500 | 12.0 | 6,000 |
| Theft of equipment | 5,000 | 1 per year | 5,000 | 1.0 | 5,000 |
| Virus, worms, Trojan horses | 1,500 | 1 per week | 1,500 | 52.0 | 78,000 |
| Denial-of-service attacks | 2,500 | 1 per quarter | 2,500 | 4.0 | 10,000 |
| Earthquakes | 250,000 | 1 per 20 years | 250,000 | 0.05 | 12,500 |
| Flood | 250,000 | 1 per 10 years | 250,000 | 0.1 | 25,000 |
| Fire | 500,000 | 1 per 10 years | 500,000 | 0.1 | 50,000 |

The company may subjectively evaluate the cost per incident, and may have record of previous incidents to estimate frequency. Estimates from other sources may also be available.

Except for insured items (fully cover the damage), SLE generally does not change even when new controls are put in place, only ARO and ALE change.

| Threat category | SLE | ARO | ALE  (After) | ALE (before) | CC | Y/N |
| --- | --- | --- | --- | --- | --- | --- |
| Programmer mistakes | $5.000 | 12 | $60,000 | $260,000 | $20,000 | Y |
| Loss of intellectual property | $75,000 | 0.5 | $37,500 | $75,000 | $15,000 | Y |
| Software piracy | $500 | 12 | $6,000 | $26,000 | $30,000 | N |
| Theft of information (hacker) | $2,500 | 2 | $5,000 | $10,000 | $15,000 | N |
| Theft of information (employee) | $5,000 | 1 | $5,000 | $10,000 | $15,000 | N |
| Web defacement | $500 | 4 | $2,000 | $6,000 | $10,000 | N |
| Theft of equipment | $5,000 | 0.5 | $2,500 | $5,000 | $15,000 | N |
| Virus, worms, Trojan horses | $1,500 | 12 | $18,000 | $78,000 | $15,000 | Y |
| Denial-of-service attacks | $2,500 | 2 | $5,000 | $10,000 | $10,000 | N |
| Earthquakes | $0 | 0.05 | $0 | $12,500 | $5,000 | Y |
| Flood | $0 | 0.1 | $0 | $25,000 | $10,000 | Y |
| Fire | $0 | 0.1 | $0 | $50,000 | $10,000 | Y |

Question 6

A recent security audit at an organisation has revealed that the processor of an important internal server has a critical design flaw that could be exploited to reveal confidential system information. This is a hardware vulnerability and there are no current fixes. It is also determined that it is not cost effective to upgrade to a new server and the current server must continue its operation to serve users within the organisation. The organisation needs to address this particular risk immediately. Identify two (2) strategies that can be used to address the risk. For each strategy, give an example and briefly explain how it helps.

Transfer risk

Eg. Purchase insurance : Insurance provider pay for the damage if there are damage

Accept the risk

Shld know what will happen assuming the cost of the asset outweighs the risk and the benefits

Mitigate the risk

Put controls on the risk, put

Early detection and response

Create incident response plan to deal with such an attack

Answer:

It is not expected that Prevent or Avoid strategies can be used because of the constraints.

* Strategy 1 : Mitigate the risk. Monitor the server and ask users to monitor their accounts for any suspected activity so early detection and response can be performed. Encrypt user data and perform frequent backup to prevent data from being stolen or damaged. Create incident response plan to deal with such an attack.
* Strategy 2 : Accept the risk. This strategy accepts the risk, knowing that it could happen - assume that the cost much outweighs the benefits.
* Strategy 3: Transfer the risk. This means transfer the risk to another organisation. The simplest form being purchasing insurance. If there is any damage caused by such an attack, the insurance provider will pay the damage.

Question 7

List and briefly describe five sections which are usually found in a policy.

Choose four from the following:

* Purpose: Explains the reason for the policy
* Related documents: Lists any documents (or other policy) that affect the contents of this policy
* Cancellation: Identifies any existing policy that is cancelled when this policy becomes effective.
* Background: Provides amplifying information on the need for the policy
* Scope: States the range of coverage for the policy (to whom or what does the policy apply)
* Policy statement: Identifies the actual guiding principles or what is to be done
* Action: Specifies what actions are necessary and when they are to be accomplished
* Responsibility: States who is responsible for what
* Ownership: Identifies who sponsored the policy and from whom it derives its authority, as well as defines who may change the policy.

Question 8

Describe an example wherein unmanaged changes to IT systems and networks can increase risk to enterprises. Describe how the risk can be minimized if changes are managed carefully.

**Example**

1. Remote access to the internal server - opens the firewall port, introduces unauthorised hackers to also gain access to internal server remotely

**How**

1. Impl change management process whereby approval has to be granted by the superior before the firewall administrator can open the firewall port to allow access to the internal server. Only when he is granted access to open the access to the internal server, the firewall administrator should also monitor traffic from remote to internal server to make sure that the traffic is legitimate and not suspicious.

Question 9

Describe how you would measure the success of a change management program?

Compare the outcomes vs expectations the organisation has ( eg on time, on budget, meats tech and busin or human obj)

Answer

This is an open question: One obvious approach is to compare the delivered outcomes and the expectations before the change.

Some other examples can also include:

* Installation: It is on time
* Installation: It is on budget
* Installation: It meets the technical objective
* Implementation: The business objectives are met
* Implementation: The human objectives are met

Question 10

What are basic elements that you can expect to see in a change management and control policy. Briefly describe each of them.

Change Management is the discipline of understanding, adjusting and adapting to a new normal after an enterprise transformation.

Change control is the process of how changes to requirements are sourced, analyzed, managed, and included in the roadmap and implementation schedule.

Change Management is about molding hearts and minds. Change Control is about governing the requirements management.

Change Management is about not letting investment into a transformation come to naught. Change Control is about not letting the requirements runaway train derail a project or a program.

Change Management may or may not involve technology involvement. Change Control is a part of the overall IT enablement realm.

Change Management could impact an entire company. Typically, Change Control is about a specific project and a set of requirements.

Question 11

Using the quantitative risk assessment approach, a software company is assessing the risk due to programmer mistakes which happen five (5) times every four (4) weeks on average and cause a damage of $10,000 per incident.

* Calculate the current SLE, ARO and ALE values.
* The company is considering two possible controls described below to address this risk. Using the cost-benefit analysis (CBA) approach, derive the SLE, ARO, ALE, ACS and CBA values for each case and state clearly which control should be selected to address the risk due to the programmer mistakes.
* Control A (training staff) costs $150,000 per annum and reduces the frequency of mistakes to one (1) every fortnight.
* Control B (smart backup and version control) costs $100,000 per annum and reduces the damage to $5,000 per incident.
* Current values
* SLE = $10,000
* ARO = 52 x 5/4 = 65
* ALE = 65 x $10,000 = $260,000
* Control A
* SLE = $10,000
* ARO = 52 x ½ = 26
* ALE = 26 x $10,000 = $260,000
* ACS = $150,000
* CBA = $650,000 - $260,000 - $150,000 = $240,000
* Control B
* SLE = $5,000
* ARO = 65
* ALE = 65 x $5,000 = $325,000
* ACS = $100,000
* CBA = $650,000 - $325,000 - $100,000 = $225,000
* Conclusion: Control A should be selected because iths CBA is better than that of Control B by $15,000

Question 12

Describe an example wherein unmanaged changes to IT systems and networks can increase risk to enterprises. Describe how the risk can be minimised if changes are managed carefully.

Take for example, a team of developers that has just written a much better looking and easier to use version of the organisation’s website. The only problem is that it cant be tested by the remote QA team because the firewall is blocking access. Waiting for change management approval could take weeks, so as the firewall admin, it may be very tempting to want to help out the development team by temporarily opening a port on the firewall. Sadly, we’ve all seen some variation of how that story ends: a worm or Trojan is introduced onto the internal network, a sniffer is planted on a server and credentials are stolen, or a previously protected database is exposed to attackers.

Question 13

Explain the differences between the two roles in a change management process: Change Manager vs Change Coordinator

* Hierarchy: as far as the hierarchy is concerned, Change Manager sits above Change Coordinator, Change Manager actually appoints Change Coordinatior(s). There could be multiple Change Coordinators for multiple business IT units, each looking after their own area. However, usually there is only one Change Manager.
* Responsibilities: Change Manager has the overall responsibility for the organisation and acts at a high level. A Change Coordinator on the other hand is usually appointed for a particular change, and “responsible for planning and coordinating all of the phases of the change from initiation through acceptance and documentation” . Change Coordinators will provide updates to Change Manager on a regular basis. That is to say that Change Coordinators assist Change Manager.

## Tutorial: Week 8 Business Continuity II

Question 1

Explain the fundamental difference between business continuity planning (BCP) and disaster recovery planning (DRP).

Student should consult lecture slides on BCP to recognise that DRP is a sub-component of BCP (BCP consists of: BIA, COOP + DRP, Testing, and Maintenance). BCP is a process designed to reduce the organizations business risk arising from and unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization, whilst DRP typically details the process IT personal still follow to restore the computer system and the operational facilities after a disaster

.

Question 2

What is business impact analysis (BIA), and what is it used for?

The BIA is the first phase of BCP. A crucial component of the initial planning stages, it serves as an investigation and assessment of the impact that various event can have on the organization. It includes

Determine core business processes and recover criticality

Identify resource requirements

Identify recover priorities for system resources

Question 3

What is the fundamental difference between BIA and risk assessment?

Risk management focuses on identifying threats, vulnerabilities, and attacks in order to determine controls that can protect data. BIA on the other hand assumes that these controls have FAILED/BY-PASSED/INEFFECTIVE, and the attacks have been successful. BIA therefore addresses worst-case scenarios.

Question 4

The comprehensive approach to emergency or disaster management typically consists of four phases: Prevention, Preparedness, Response, and Recovery (PPRR). Which phase does Business Impact Analysis (BIA) belong to? Describe two (2) examples of critical activities of a typical software firm that need to be established as part of business impact analysis.

BIA belongs to: Preparedness

A software firm is similar to manufacturing firm as in the QLD BCP Guide, so example can be found similarly as follows

Securing contracts with clients

Developing software

Delivering and supporting developed software products

Question 5

Explain why it is important for large organisations to have a proper BCP in place? What is the implication if a lack of BCP is found?

Legal and regulatory req: many industries may find themselves bound by federal, state and local laws or regulations that require them to implement various degrees of Business Continuity Planning. For example, the officers and directors of publicly traded firms have a fiduciary responsibility to exercise due diligence in the execution of their business continuity duties. In other circumstances, the requirements(and consequence of failure) might be more severe. Emergency services, such as police, fire, and emergency medical operations, have a responsibility to the community to continue operations in the event of a disaster. Indeed, their services become even more critical in an emergency when public safety is threatened. Failure on their part to implement a solid BCP could result in the loss of life and/or property and the decreased confidence of the population in their government.

In many countries, financial institutions, such as banks, brokerages,and the firms that process their data, are governed by strict government and international banking a d securities regulations designed to facilitate their continued operation to ensure the viability of the national economy. Why pharmaceutical manufacturers must produce products in less-than-optimal circumstances following a disaster, they are required to certify the purity of their products to government regulators. There are countless other examples of industries that are required to continue operating in the event of an emergency by various laws and regulations.

Question 6

Consider the statement ‘‘Business continuity planning is only about recovery of computer systems.” Is it true or false? Explain your reasoning.

In the past, continuity planning was frequently thought of as the recovery of computer or information technology systems and nothing more. This discipline is often referred to as disaster recovery planning. Experience in the field of continuity planning has shown that the recovery of IT functions alone does not ensure survival of the enterprise following a serious disruption or disaster. Complete recovery requires thorough knowledge of all aspects of the enterprise.

Question 7

Does business continuity planning provide any additional benefits to an organisation apart from providing the ability to recover from major disruptive events.

There are other, less obvious benefits of continuity planning. In developing a comprehensive continuity planning infrastructure, the continuity planner must understand the business processes of his enterprise, and how information, goods, and services move within the organization. Equally important is knowing how information, goods, services, and cash flow in and out of the enterprise.

The collection and analysis of this knowledge could identify potential cost reductions by improving or creating operating efficiencies. The planner may also find opportunities for cost savings in business interruption insurance and directors and officer's coverage. These examples show that continuity planning could provide an advantage over competitors. As the importance of continuity planning becomes more well known, the lack of planning could even disqualify a company from consideration for new business.

The continuity planning process also forces a review of various other components of the organization's infrastructure. Vital records management, data backup and storage, and physical, environmental, and information security controls must also be scrutinized when addressing continuity planning, and efficiencies may be discovered during the process

Question 8

Describe the advantages and disadvantages of hot sites

Hot Sites' Advantages

* Ready within hours for operation
* Highly available
* Usually used for short-term solutions, but available for longer stays
* Annual testing available

Hot Sites’ Disadvantages

* Very expensive
* Limited on hardware and software choices

Question 9

Describe the advantages and disadvantages of cold and warm sites.

Warm and Cold Sites' Advantages

• Less expensive

• Available for longer time frames because of the reduced costs

• Practical for proprietary hardware or software use

Warm and Cold Sites' Disadvantages

• Operational testing not usually available

• Resources for operations not immediately available

Question 10

What is the fundamental difference between recovery time objective (RTO) and maximum tolerable downtime (MTD)? Suppose that RTO has been fixed, which aspects of data backup could be influenced by MTD? Discuss.

Difference: RTO is the specified time frame for recovering critical infrastructure/core functions of an organization, for example the website is up but with only limited/core features. In contrast, MTD is the specified time frame for bringing back the whole system to normal, which means all features should be available just like before the disaster strikes.

• Discussion: The data recovery is actually done in the second stage and is governed by WRT, which is MTD-RTO. When RTO is fixed, the time for recovering data is directly dependent on MTD:

- If MTD is large, the data recovery time is large, hence any backup method, such as incremental backup is ok as we can take several steps to actually recover the data

- If MTD is small, the data recovery time is small, we need to recover data quickly, so differential backup might be preferred as it takes less time

- If MTD is very small, just sufficient for other testing, we need high availability, which mean data mirroring/redundancy/full backup is required.

Question 11

What are the the MTD, RPO, RTO values of the following scenario: Susan is the new BCM coordinator and needs to identify various preventive and recovery solutions her company should implement for BCP/DRP efforts. She and her team have carried out an impact analysis and found out that the companys order processing functionality cannot be out of operation for more than 15 hours. She has calculated that the order processing systems and applications must be brought back online within eight hours after a disruption. The analysis efforts have also indicated that the data that are restored cannot be older than five minutes of current real-time data.

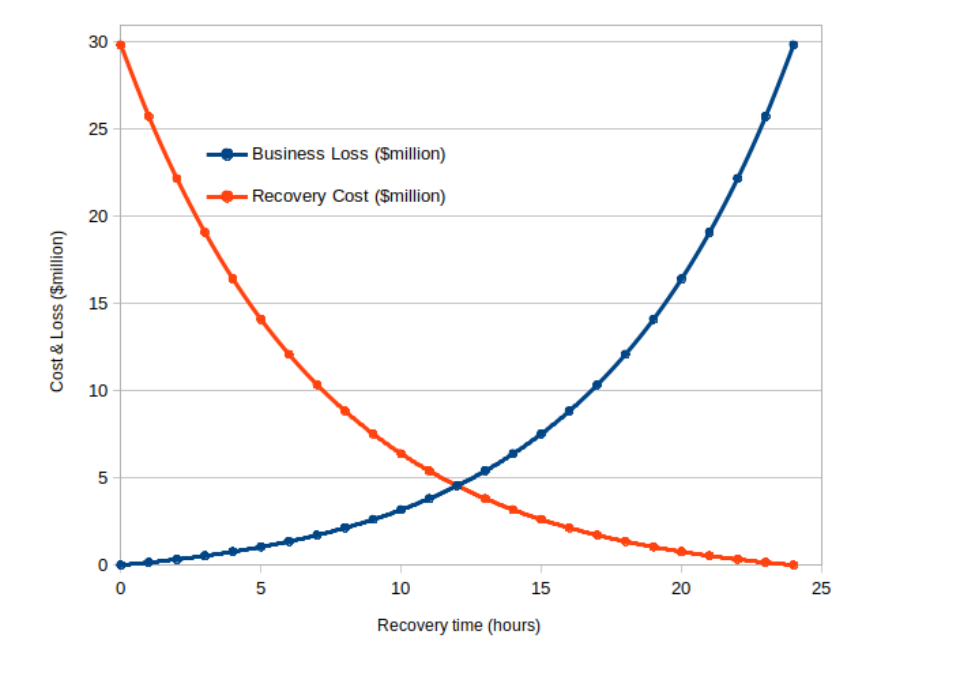
MTD of the order processing functionality is 15 hours. RTO value is 8 hours. WRT value is 7 hours.

RPO value is 5 minutes.

The order processing functionality as a whole has to be up and running within 15 hours. which is the maximum tolerable downtime (MTD). The systems and applications have to be up and running in eight hours, which is the Recovery Time Objective (RTO. RTO deals with technology, but we still need processes and people in place to run the technology. Work Recovery Time (WRT) is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything live for production purposes. The data that are restored for this function can only be five minutes old; thus, the Recovery Point Objective (RPO) has the value of five minutes.

Question 12

The BIA team of an organisation is determining the recovery time of their core system due to a disaster. The team has been able to plot the relationships between the business loss (due to ceasing of critical business activities) and the recovery cost (due to offsite facility and other related expenses) against recovery time below. The core system definitely needs to be recovered within 24 hours and the BIA team believes that a much quicker recovery can be achieved. Suppose that this is the only information available, suggest the optimal recovery time that the BIA team should aim for and explain your suggestion. Your argument must be based on the plot given below.



\*Find optimum point which is intersection betw 2 curves = 12hrs

Students are expected to find the optimal point being the intersection between two curves, which is exactly 12 hours (the two curves have been specially created). They are also expected to explain that if recovery time is less than 12 hours the recovery cost is much more than the loss and it is not worth spending that much, whilst longer recovery time can significantly increase business loss.

Furthermore, if the total cost is taken into account, the sum of the two curves also gives the minimum at that intersection (which gives a total cost of $9.1 millions, still much less than $30 millions perceived as maximum absorbed cost). In the absence of other information, the intersection is the best choice as far as the cost and loss are concerned

Question 13 What are the three main phases in a contingency plan as per the NIST SP800 standard? Briefly describe the activity in each phase.

Students are expected to look up the NIST SP800 standard before answering this question.

* Phase 1 - Activation and notification: The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, information system contingency plan (ISCP) staff will be prepared to perform recovery measures to restore system functions.
* Phase 2 - Recovery: Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BlA will be recovered at this stage.
* Phase 3 - Reconstitution: The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.