|  |
| --- |
| http://www.cit.ie/contentfiles/images/Logos/CIT_large/CIT%20MAIN%202012%20(RGB)1.jpg |
| **PROJECT PLAN** |
| **Implementing Security Management** |
|  |
|  |
|  |

|  |
| --- |
|  |

**Student Name:** Emmanuela Ogbene

**Lecturer Name:** Noreen Gubbins

**Submittal Date:** May 30, 2015

**VERSION 1.0**

The purpose of this report is to outline how Security Management can be implemented in an organization such as Cork Institute of Technology (**CIT**).

Table of Contents

1. **Introduction …………………………………………………........1 – 1**

1.1. Purpose of Plan …………………………………….......................1 – 1

1.2. Project Background………………………………………………………….1 – 1

1. **Project Benefits……………………………………………….......1 – 1**
2. **Project Deliverables………………………………………......2 – 21**
   1. Elements of Information Security Management Process......2 – 6
   2. Implementation of ISO/IEC 27002.......................................7 – 21
      1. Security Governance and Organisation..................7 – 7

*3.2.1.1.* *Internal Organisation*………………….*7 – 7*

*3.2.1.2.* *Mobile Devices and Teleworking*….*7 – 7*

* + 1. Security Policies……………………………………………....8 – 8
    2. Risk Management…………………………………………….9 – 9
    3. Asset Classification/Management……………..…..10 – 10
    4. Physical and Environmental Security……………..11 – 12

*3.2.5.1. Secure Areas……………………………11 – 11*

*3.2.5.2. Equipment Security…………………11 – 11*

* + 1. Human Resources Security…………………….........13 – 13

*3.2.6.1. Prior to Employment…………….…13 – 13*

*3.2.6.2. During Employment…………….…13 – 13*

*3.2.6.3. Termination and Change of Employment...13 – 13*

* + 1. Network Servers Operational Security……………………….14 – 14

*3.2.7.1. Network Security Management*………..*14 – 14*

*3.2.7.2. Information Transfer*………………………14 – 14

* + 1. Access Control………………………………………………………..15 – 16

*3.2.8.1. Business Requirements of Access Control*…15 – 15

*3.2.8.2. User Access Management*......................15 – 15

*3.2.8.3. User Responsibilities*…………………………15 – 15

*3.2.8.4. System and Application Access Control*…15 – 15

* + 1. Business Continuity Management……………………………..17 – 18

*3.2.9.1. Information Security Continuity*…………..17 – 17

*3.2.9.2. Redundancies*……………………………………..17 – 17

* + 1. Compliance………………………………………………………………19 – 19

*3.2.10.1. Compliance with legal requirements…….*19 – 19

*3.2.10.2. Information Security Reviews*……………..19 – 19

* + 1. Supplier Management……………………………………………..20 – 20

*3.2.11.1. Information Security in Supplier Relationships*.20 – 20

*3.2.11.2. Supplier Service Delivery Management*…..20 – 20

* + 1. Cryptography…………………………………………………………..21 – 21

*3.2.12.1. Cryptographic Controls*………………………21 – 21

1. **Project Scope……………………………………………………22 – 22**
2. **Appendix…………………………………………………………23 – 24**
3. **Work Break Down Structure……………………………25 – 26**
4. **Conclusion……………………………………………………….27 – 27**
5. **References……………………………………………………….28 – 28**
6. **Introduction**

# Purpose of Plan

The purpose of this project is to outline how Security Management can be implemented in an organisation. Security Management is the management process within the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved. It is implemented to ensure that IT security meets the overall organisation security requirements through availability, integrity, and confidentiality. Information Security Management maintains and enforces an overall policy, together with a set of supporting controls within an integrated security management information system, aligned with business security policies and strategies.

# 1.2. Project Background

The organisation that I have chosen for this project is **Cork Institute of Technology** (CIT). Cork Institute of Technology, formerly the Regional Technical College, Cork, is an Institute of Technology in Ireland, located in Cork, Ireland opened in 1973.

The Institute has 17,000 students both part-time and full-time in [art](http://en.wikipedia.org/wiki/Art), [business](http://en.wikipedia.org/wiki/Business), [engineering](http://en.wikipedia.org/wiki/Engineering), [music](http://en.wikipedia.org/wiki/Music), [drama](http://en.wikipedia.org/wiki/Drama) and [science](http://en.wikipedia.org/wiki/Science) disciplines. Cork Institute of Technology comprises two constituent Faculties and three constituent Colleges.

The constituent Faculties are Engineering and Science, and Business and Humanities. The constituent colleges are the CIT Crawford College of Art and Design, the CIT Cork School of Music and the National Maritime College of Ireland.

1. **Project Benefits**

Implementing Security Management in CIT will allow information to be available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures availability. In addition, information will be observed by, or disclosed to only those who have the right to know (i.e. Confidentiality of Information). Information will be completed, accurate and protected against unauthorized modification. And, business transactions as well as information exchanges between partners, can be trusted – authenticity and non-repudiation.

1. **Project Deliverables**

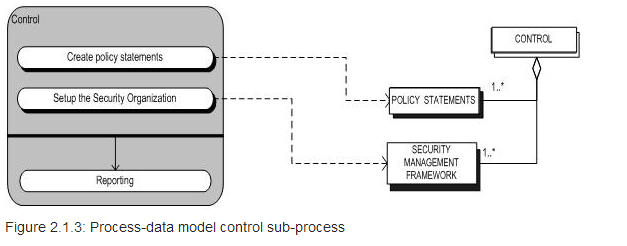
# Elements of Information Security Management Process

There are five elements of Information Security Management Process that can be considered when implementing Security Management in CIT. They are as follows:

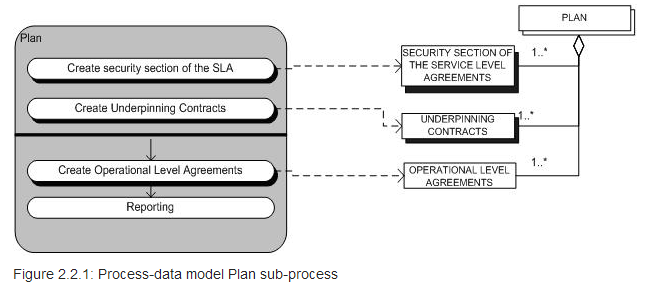
**Control:** This is the first activity in the security management process. The Control sub-process organizes and manages the security management process itself. It defines the processes, the allocation of responsibility for the policy statements and the management framework.

The **objectives** include:

* Establishing an organisation structure to prepare, approve and implement the information security policy in **CIT**.
* Establishing a management framework that will initiate and manage information security in **CIT**.
* Allocating responsibilities, establishing and controlling documentation in **CIT**.



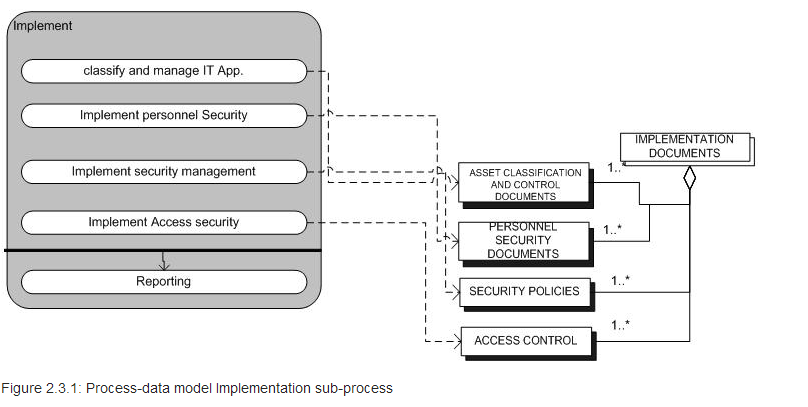
|  |
| --- |
|  |
| **Plan:** This is the second activity in the security management process. It contains activities that in cooperation with the Service Level Management lead to the Information Security section in the SLA. Furthermore, it contains activities that are related to the underpinning contracts which are specific for information security.  The **objectives** for CIT includes:   * Devising and recommending the appropriate security measures, based on an understanding of the requirements of the organisation. * The requirements will be gathered from such sources as business and service risk, plans and strategies, SLAs and OLAs and the legal, moral and ethical responsibilities for information security. |
|  |



**Implement:** The implementation sub-process makes sure that all measures, as specified in the plans, are properly implemented. During this process, no new or measures are defined nor changed. The change of measures will only take place in the Plan sub-process in cooperation with the Change Management Process.

The **objectives** include:

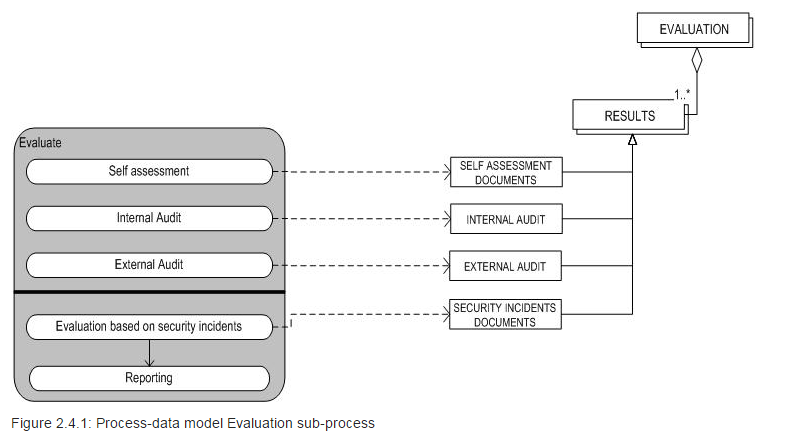
* Ensuring that appropriate procedures, tools and controls are in place to underpin the Information Security Policy in **CIT**.



**Evaluation:** The evaluation sub-process is necessary to measure the success of the implementation and the Security plans. The results of the Evaluation sub-process are used to maintain the agreed measures and the implementation itself. It can lead to new requirements and so lead to a Request for Change. Furthermore, there are three sorts of evaluation: the Self-assessment, internal audit, and external audit. The most important activities of this process is verifying if the security legislation and the implementation of the security plans are complied, traced and reacted to undesirable use of the IT-supplies.

The **objectives** of Evaluation element in **CIT** are:

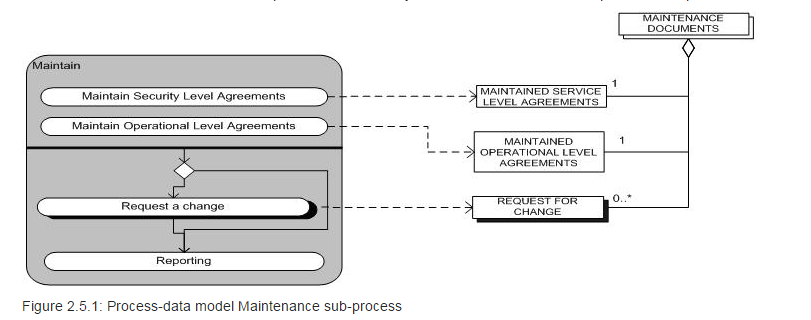
* Supervising and checking compliance with the security policy and security requirements in Service Level Agreements and OLAs.
* Carrying out regular audits of the technical security of IT systems in **CIT**.
* Providing information to external auditors and regulators, if necessary.



**Maintenance:** The maintenance sub-process starts with the maintenance of the service level agreements and the maintenance of the operational level agreements. The maintenance of service level agreements is used to keep the service level agreements in proper condition. This process ends with MAINTAINED SERVICE LEVEL AGREEMENTS. The maintenance of operational level agreements is used to keep the operational level agreements in proper condition. Also, the process ends with MAINTAINED OPERATIONAL LEVEL AGREEMENTS.

The **objectives** of Maintain element in CIT include:

* Improving on security agreements as specified in SLAs and OLAs.
* Improving the implementation of security measures and controls in **CIT**.



# Implementation of ISO/IEC 27002

* + 1. **Security Governance and Organisation**

Information Security Governance consists of the leadership, organisational structures, processes/procedures, compliance enforcement/monitoring mechanisms and technologies that ensure that the confidentiality, integrity and availability of the organisation’s electronic assets (data, information, software, etc.) are maintained at all times, i.e. that all risks against CIT’s electronic assets are mediated and countered.

Information Security Governance will increase share value for CIT. It will provide accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response. It will also protect CIT’s reputation. Decrease likelihood of violations of privacy in CIT. It will provide greater confidence when interacting with their partners. Also, reduce operational costs by providing predictable outcomes – mitigating risk factors that may interrupt the process.

**3.2.1.1. Internal Organization**

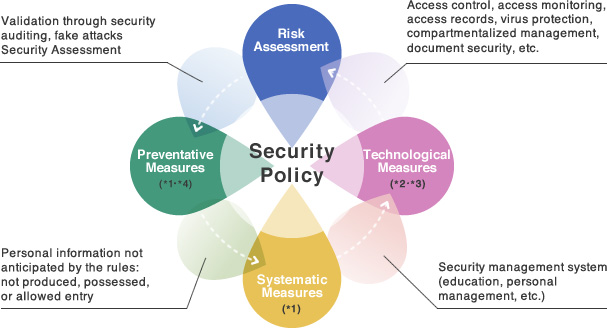
CIT will be able to lay out the roles and responsibilities for information security, and allocate them to individuals.  Where relevant, duties will be segregated across roles and individuals to avoid conflicts of interest and prevent inappropriate activities. Contacts with relevant external authorities (such as CERTs and special interest groups) on information security matters will be considered.  Information security will be an integral part of the management of all types of project.

**3.2.1.2. Mobile Devices and Teleworking**

Security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, and USB gadgets) and teleworking (such as telecommuting, working-from home, road-warriors, and remote/virtual workplaces) will be provided in CIT.

**3.2.2. Security Policies**

The goal of the Security Policies is to set the levels of security that need to be included as a part of the Service Level Agreements, Operational Level Agreements and Underpinning Contracts. This plan is drawn up on cooperation with Service Level Management, which is ultimately responsible for both the quality of the service delivered to CIT Students and Staff and the service received by the IT organisation and their external service providers. The security plan is defined in such a way that it offers a better and more secure service to CIT and never as an obstacle to developing their business activities. Moreover, key metrics and indicators are defined to allow the agreed levels of security to be evaluated.

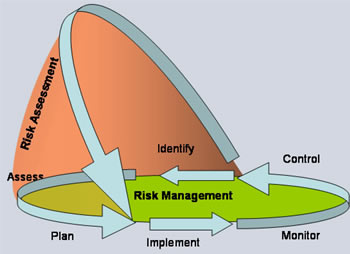


**3.2.3. Risk Management**

Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measurements and the enforced security policy. It is the process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. It is also an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

The purpose of a risk assessment is to determine if countermeasures in CIT are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

This management tool will be able to provide a systematic approach for determining the relative value and sensitivity of computer installation assets, assessing vulnerabilities, assessing loss expectancy or perceived risk exposure levels, assessing existing protection features and additional protection alternatives or acceptance of risks and documenting management decisions in CIT.



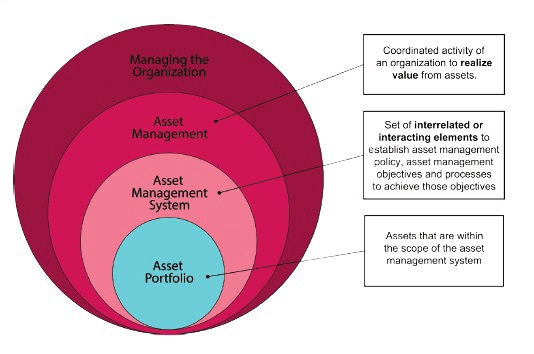
**3.2.4. Asset Classification/Management**

Asset Management is the set of business practices that join financial, contractual and inventory functions to support lifecycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in CIT environment. It is also an important part of CIT’s strategy that usually involves gathering detailed hardware and software inventory information which is then used to make decisions about hardware and software purchases and redistribution.

With IT asset management also known as IT inventory management, CIT will be able to manage their systems more effectively and save time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources. It will further minimize the incremental risks and related costs of advancing IT portfolio infrastructure projects based on old, incomplete and/or less accurate information.

The hardware asset management involves the management of the physical components of computers and computer networks, from acquisition through disposal. Common practices that can be seen in CIT include request and approval process, procurement management, lifecycle management, redeployment and disposal management. Capturing the financial information about the hardware lifecycle will help CIT in making business decisions based on meaningful and measurable financial objectives. The software asset management is also a similar process, where software assets, including licenses, versions and installed endpoints are focused on.

Asset Management is responsible for the development and maintenance of policies, standards, processes, systems and measurements that will enable CIT to manage the IT Asset Portfolio with respect to risk, cost, control, IT Governance, compliance and organisation performance objectives as established by the organisation. It will use integrated software solutions that work with all departments that are involved in the procurement, deployment, management, and expense reporting of IT assets.



**3.2.5. Physical and Environmental Security**

Physical and environmental security are security measures designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm such as theft, espionage, or terrorist attacks.

It involves the use of multiple layers of interdependent systems which include CCTV surveillance, protective barriers, security guards, locks, access control protocols, and many other techniques. These physical security systems are generally intended to deter potential intruders (these include warning signs and perimeter markings) in the organisation’s environment like **CIT**.

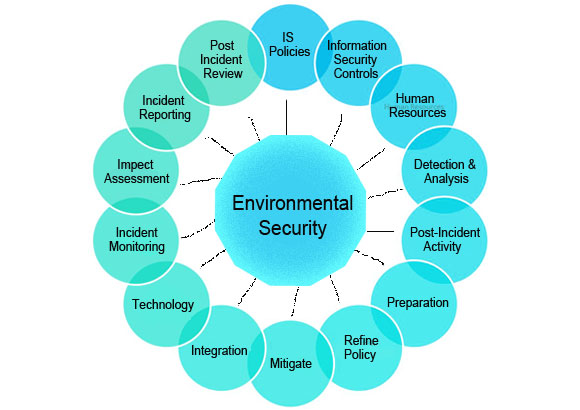
They also detect intrusions and monitor/record intruders (for instance, intruder alarms and CCTV systems) and trigger appropriate incident responses (e.g. by security guards and the police). In **CIT**, security controls are balanced against risks, taking into consideration the costs of specifying, developing, testing, implementing, using, managing, monitoring and maintaining the controls, along with broader issues such as human rights, health and safety, aesthetics, and societal norms or conventions.

**3.2.5.1.** **Secure Areas**

Defined physical perimeters and barriers, with physical entry controls and working procedures, are used in CIT to protect the premises, offices, rooms, delivery/loading areas against unauthorized access. Expert advice is sought regarding protection against fires, floods, earthquakes, bombs etc. in CIT.

**3.2.5.2.** **Equipment Security**

Equipment such as ICT equipment plus supporting utilities (such as power and air conditioning) and cabling will be secured and maintained in **CIT**. Equipment and information will not be taken off-site unless authorized, and must be adequately protected both on and off-site. Implementing equipment security for Information Security Management System in CIT will enable information to be destroyed prior to storage media being disposed of or re-used. Unattended equipment will be secured and a clear desk and clear screen policy will be in place.



**Implementing Physical and Environmental Security**

**3.2.6. Human Resources Security**

Human Resources Security is security aspects for employees joining, moving and leaving the organisation. With this security implemented in **CIT**, all employees will be screened prior to employment, including identity verification using a passport or similar photo ID and at least two satisfactory professional references. Additional checks will be required for employees taking up trusted positions. Also, all staff in **CIT** will formally accept a binding confidentiality or non-disclosure agreement concerning personal and proprietary information provided to or generated by them in the course of employment. Human Resources department would be able to inform Administration, Finance and Operations when staffs (employees) is taken on, transferred, resigns, is suspended or released on long-term leave, or their employment is terminated.

**3.2.6.1.** **Prior to Employment**

These are security responsibilities that are taken into account when recruiting permanent employees, contractors and temporary staff (for instance through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements on security roles and responsibilities).

**3.2.6.2. During Employment**

This is ensuring that employees and contractors in **CIT** are made aware of and motivated to comply with their information security obligations. Moreover, a formal disciplinary process is necessary to handle information security breaches.

**3.2.6.3. Termination and Change of Employment**

This is managing security aspects of a person’s exit from **CIT** or significant changes of roles such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy laws, contractual terms etc.

**3.2.7. Network Servers Operational Security**

This is the management of technical security controls in systems and networks. This describes where written operating procedures is developed to ensure the correct, consistent, and secure functioning of systems, particularly for systems that are critical to the well-being of the institution (i.e. CIT). Supplemental standards and procedures will also be established in CIT that will guide the selection of system safeguards and assign responsibility for the system and its components.

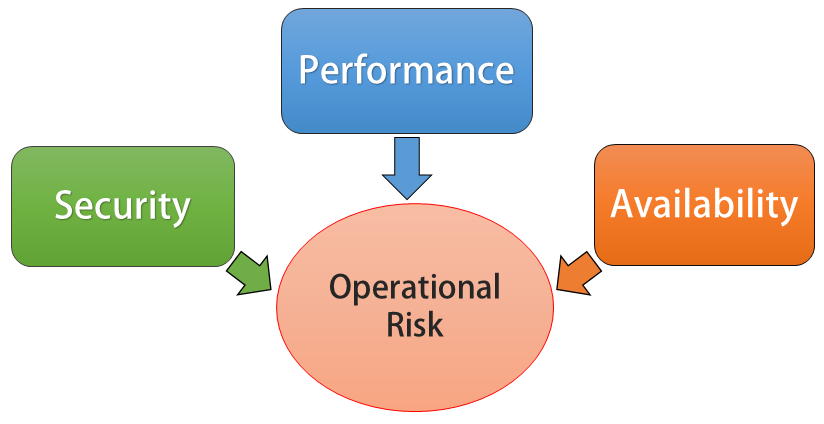
Information transmitted across CIT network and the Internet will be adequately protected to avoid data corruption, manipulation, or interception. In addition to processing [institutional data](https://protect.iu.edu/glossary/10#term688) in the traditional sense, data networks are increasingly being used for voice and video conversations. Furthermore, institution's data network is being used for critical services. Therefore, CIT’s network, including its related networking systems and services, will be appropriately managed and controlled.

**3.2.7.1. Network Security Management**

Networks and network services will be secured for example by segregation.

**3.2.7.2. Information Transfer**

Policies, procedures and agreements e.g. non-disclosure agreements will be in place concerning information transfer to/from third parties, including electronic messaging.



**3.2.8. Access Control**

This means that access to protected information is restricted to people who are authorized to access the information. For instance, computer programs, and in many cases the computers that process the information are also authorized. With access control implemented in CIT, there will be mechanisms in place in order to control the access to protected information. The sophistication of the access control mechanisms will be in parity with the value of the information being protected i.e. the more sensitive or valuable the information the stronger the control mechanisms need to be. Access control is generally considered in three steps such as Identification, Authentication and Authorization.

In addition, users of IT systems, networks, applications and information in CIT will be individually identified and authenticated. Students and Staff in CIT will either log off or password-lock their sessions before leaving IT systems, networks, applications and information unattended. CIT will be able to consider enabling password-protected screensavers with an inactivity timeout of no more than 10 minutes on all workstations/PCs.

**3.2.8.1. Business requirements of access control**

The CIT’s requirements to control access to information assets will be clearly documented in an access control policy and procedures. Network access and connections will also be restricted.

**3.2.8.2. User access management**

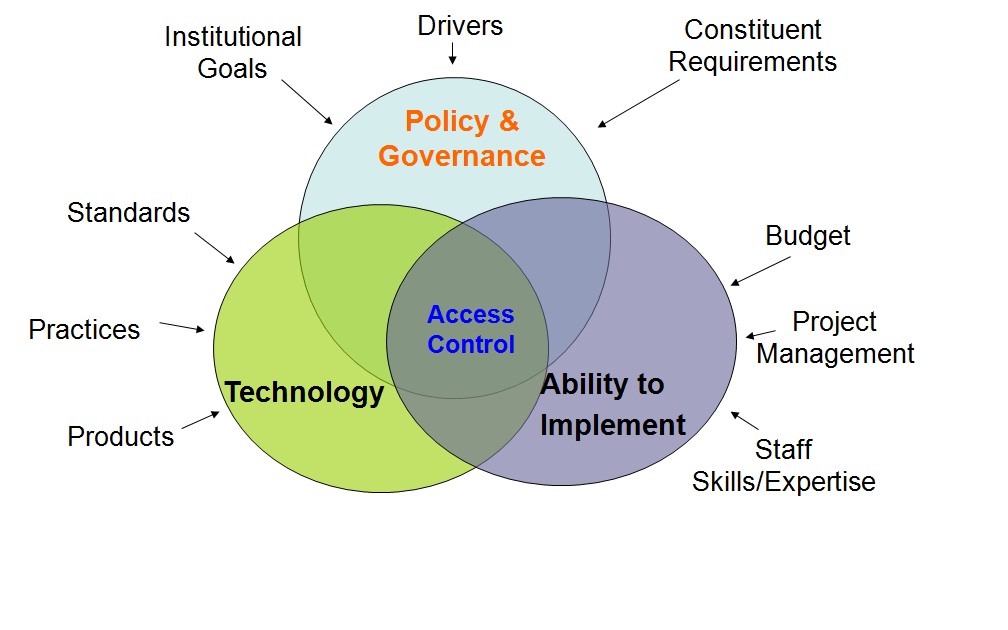
The allocation of access rights to users in CIT will be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (also called *secret authentication information*) plus regular reviews and updates of access rights.

**3.2.8.3. User responsibilities**

CIT users will be made aware of their responsibilities towards maintaining effective access controls such as choosing strong passwords and keeping them confidential.

**3.2.8.4. System and application access control**

Information access in CIT will be restricted in accordance with the access control policy for instance, through secure log-on, password management, control over privileged utilities and restricted access to program source code.



**Implementing Access Control**

**3.2.9. Business Continuity Management**

Business Continuity Management specifies a management system to manage an organisation’s business continuity arrangements. It is implemented in order to facilitate compliance auditing and certification. It is a set of plan, preparatory and related activities which are intended to ensure that CIT’s critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period.

It will provide a best practice framework for CIT to minimize disruption during unexpected events that could bring the organisation to a standstill. It will give CIT a practical plan to deal with most eventualities i.e. from extreme weather conditions to terrorism, IT system failure and staff sickness.

Implementing business continuity management includes three key elements such as:

* **Resilience**

This allows critical business functions and the supporting infrastructure in CIT to be designed and engineered in such a way that they are materially unaffected by most disruptions, for instance, through the use of redundancy and spare capacity.

* **Recovery**

Implementing this management will allow CIT to make arrangements to recover or restore critical and less critical business functions that fail for some reason.

* **Contingency**

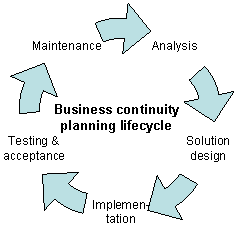
This is where CIT establishes a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen.

**3.2.9.1. Information Security Continuity**

This implementation allows the continuity of information security in CIT to be planned, implemented and reviewed as an integral part of the organisation’s business continuity management systems.

**3.2.9.2. Redundancies**

This is where CIT’s IT facilities have sufficient redundancy to satisfy availability requirements.



**Implementing Business Continuity Management**

**3.2.10. Compliance**

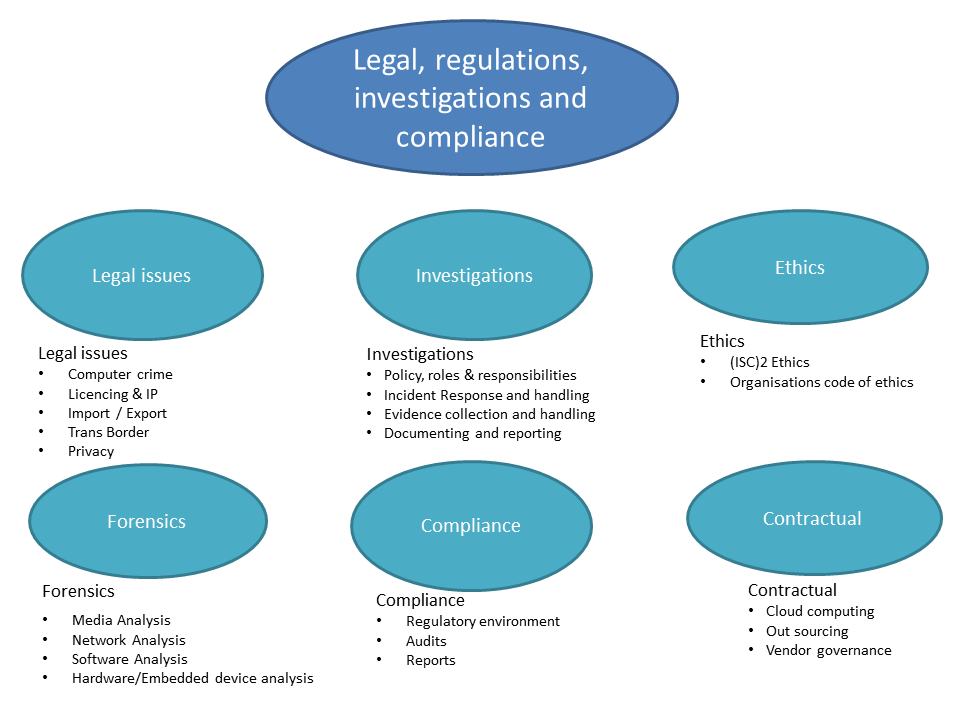
Implementing Compliance in CIT ensures conformance with information security policies, standards, laws and regulations. It means conforming to a rule, such as a specification, policy, standard or law. It also describes the goal that CIT aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations. This approach can be used by CIT to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

**3.2.10.1. Compliance with legal and contractual requirements**

Implementing compliance will allow CIT to identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, records, privacy/personally identifiable information and cryptography.

**3.2.10.2. Information Security Reviews**

This allows CIT’s information security arrangements to be independently reviewed/ audited and reported to management. CIT will also routinely review systems’ compliance with security policies, procedures, etc. and initiate corrective actions where necessary.



**3.2.11. Supplier Management**

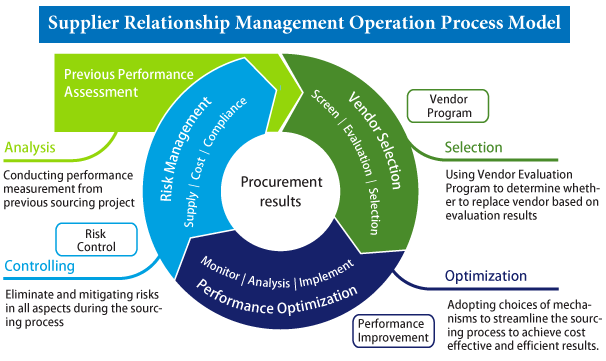
This is the process that is responsible for getting value for money from suppliers, ensuring all supplier contracts and agreements support business needs, and all suppliers meet contractual commitments. Implementing supplier management will enable CIT to obtain value for money from suppliers and contracts, maintain a supplier policy and a Supplier and Contract Database (SCD). It will also allow CIT to manage supplier relationships and performance, negotiate and agree underpinning contracts and manage through their lifecycle. Supplier Management will work with Service Level Management (SLM) to ensure underpinning contracts support and are aligned with CIT needs, Service Level Requirements (SLRs) and Service Level Agreements (SLAs).

**3.2.11.1. Information Security in Supplier Relationships**

Policies, procedures, awareness etc. would be available in CIT, in order to protect the organisation’s information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

**3.2.11.2. Supplier Service Delivery Management**

The service delivery by external suppliers will be monitored in CIT, and reviewed/audited against the contracts/agreements. Also, the service changes and services delivered by internal suppliers will be controlled.



**3.2.12. Cryptography**

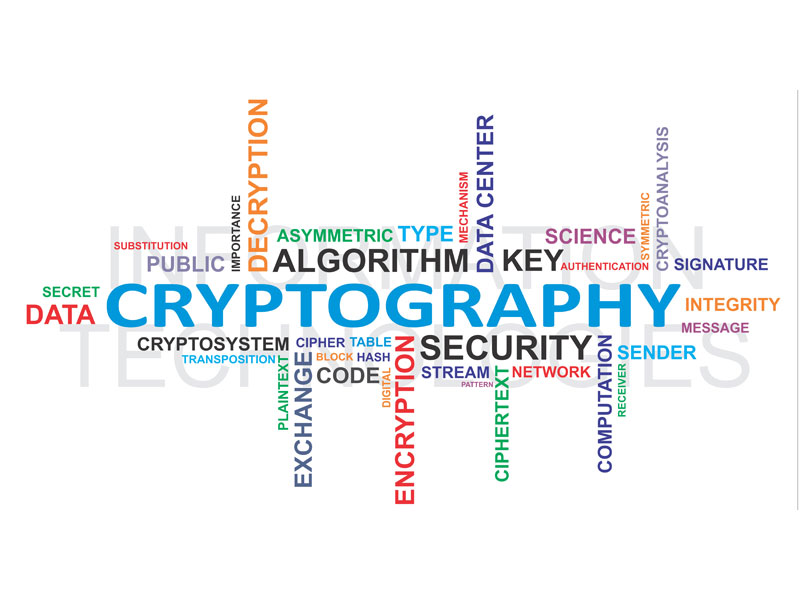
Cryptography is used to protect the confidentiality, authenticity or integrity of information by cryptographic means. Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user. This process is known as encryption.

Cryptography can be used in information security to protect CIT information from unauthorized or accidental disclosure while the information is in transit either electronically or physically and while information is in storage. It will provide CIT information security with other useful applications including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications.

This can be evidenced in CIT where wireless communications are encrypted using protocols such as WPA/WPA2. Moreover, wired communications such as ITU-T G.hn are secured using AES for encryption and X.1035 for authentication and key exchange.

**3.2.12.1. Cryptographic Controls**

There will be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management in CIT.

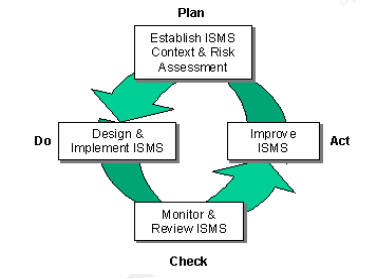


1. **Project Scope**

This project plan will identify information security needs, establish security policies and methods, implement security policies and methods, and monitor system access and needs.

In other words, it will detail the process of planning and managing a defined level of security for information and IT services, including all aspects associated with reaction to security incidents. Additionally, it will include the assessment and management of risks and vulnerabilities, and the implementation of cost justifiable countermeasures.

The diagram below illustrates all of the stages required in the planning, improvement, execution and continuation of an Information Security Management Systems.



The **“Plan-Do-Check-Act”** (**PDCA)** model shown above, applies at different levels throughout the ISMS (i.e. cycles within cycles). The approach is also used for quality management in ISO9000. The model illustrates how an ISMS takes as input the information security requirements and expectations and through the PDCA cycle produces managed information security outcomes that satisfy those requirements and expectations.

**PDCA MODEL**

**Plan (Establish the ISMS)**

* Establishing ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the organisation’s overall policies and objectives.

**Do (Implement and operate the ISMS)**

* Implementing and operating the ISMS policy, controls, processes and procedures.

**Check (Monitor and review the ISMS)**

* Assessing and, where applicable, measuring process performance against ISMS policy, objectives and practical experience and reporting the results to management for review.

**Act (Maintain and improve the ISMS)**

* Taking corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

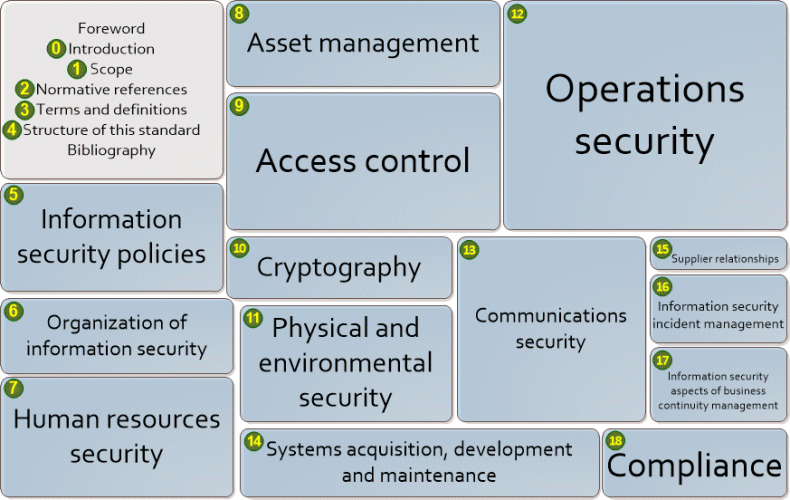
1. **Appendix**

Appendix A: Summary of the Information Security Management Systems (ISMS). ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).

Information security is defined within the standard in the context of the C-I-A triad:

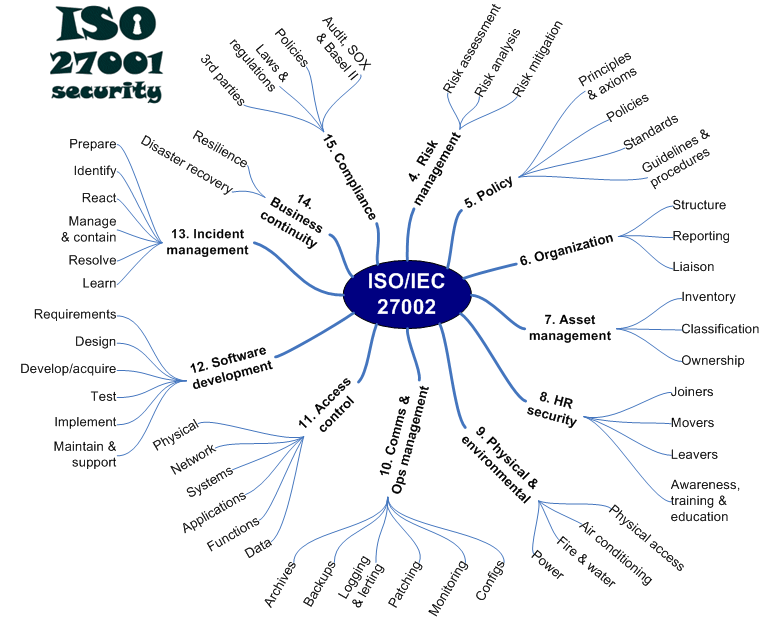
*The preservation of* ***confidentiality*** *(ensuring that information is accessible only to those authorized to have access),* ***integrity*** *(safeguarding the accuracy and completeness of information and processing methods) and* ***availability*** *(ensuring that authorized users have access to information and associated assets when required).* (Wikipedia, 2015)

**Appendix A:**

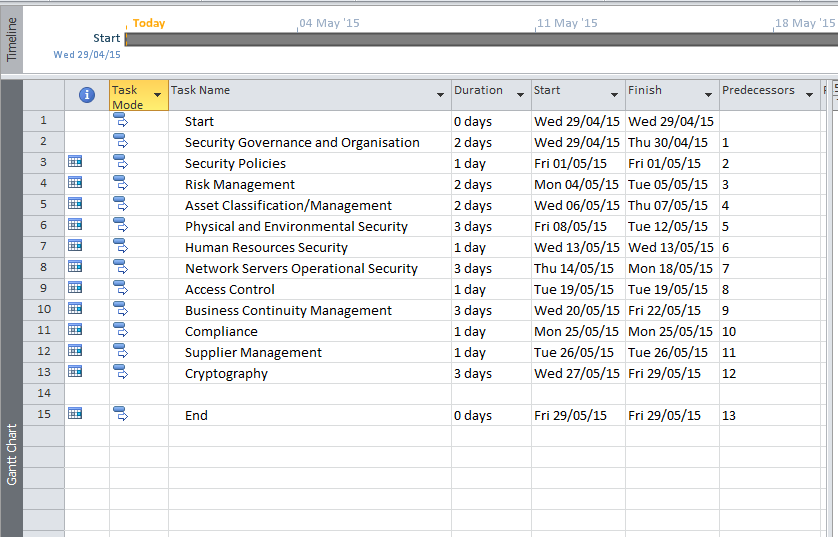


**Appendix B:**

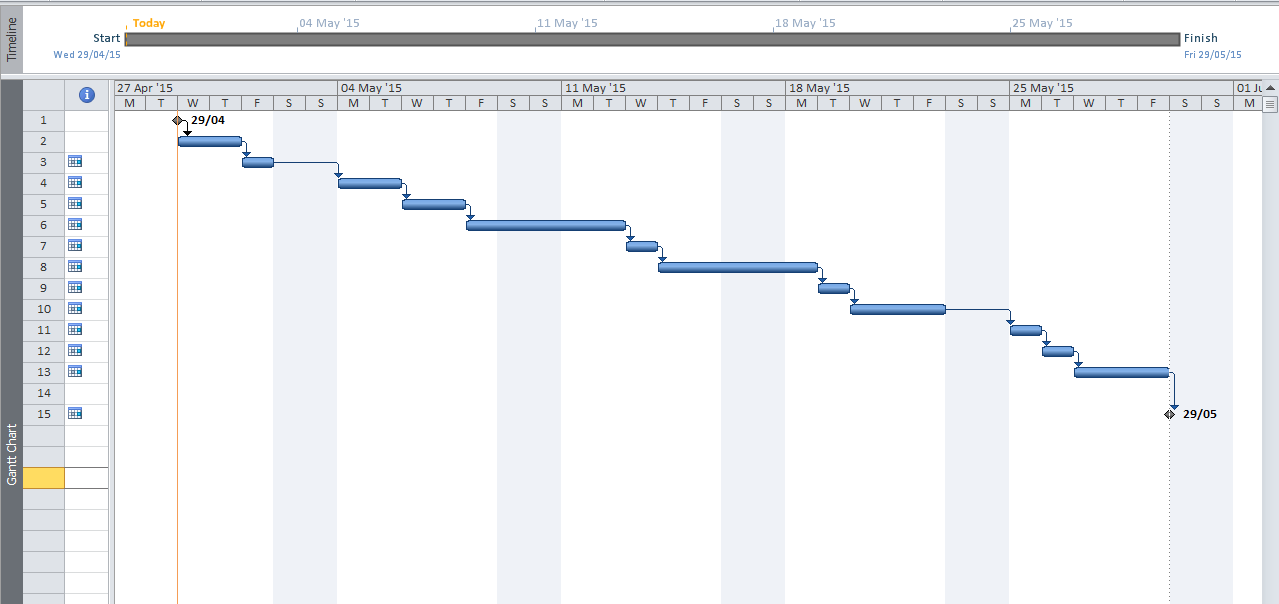
Appendix B: Summary of Information Security Management Systems (ISMS) in more detail.



1. **Work Break Down Structure**



**Plan – Gantt chart**



1. **Conclusion**

In conclusion, implementing Information Security Management System (ISMS) in CIT will be a systematic approach to managing sensitive information so that it remains secure. This includes the organisations processes and IT systems when a risk management process is applied. In other words, it will preserve the confidentiality, integrity and availability of information when risk management process is applied.

This project plan specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation (i.e. CIT). The project plan also includes requirements for the assessment and treatment of information security risks tailored to the needs of CIT. The requirements set out are generic and are intended to be applicable to CIT and all other organisations, regardless of type, size or nature.

Moreover, I learnt that Information Security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions. And, the controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of CIT are met.

I also learnt that identifying which controls that should be in place requires careful planning and attention to detail. Therefore, a successful ISMS requires support by all staff in the organisation. Also, it can require participation from suppliers or other external parties. Specialist advice from external parties can also be needed. Effective information security assures CIT that the organisation’s assets are reasonably safe and protected against harm, thereby acting as a business enabler.

1. **References**

Giac.org, (2015). [online] Available at: <http://www.giac.org/paper/g2700/39/implementing-information-security-management-system-isms-training-process/107335> [Accessed 25 Apr. 2015].

Innovation, (2013). How To Implement IT Security Management In Your Organization. [online] Available at: <http://blogs.sap.com/innovation/industries/how-to-implement-it-security-management-027310> [Accessed 25 Apr. 2015].

Iso.org, (2015). [online] Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en> [Accessed 26 Apr. 2015].

Iso27001security.com, (2015). ISO/IEC 27002 code of practice. [online] Available at: <http://www.iso27001security.com/html/27002.html> [Accessed 25 Apr. 2015].

Itil.osiatis.es, (2015). [online] Available at: <http://itil.osiatis.es/ITIL_course/it_service_management/security_management/overview_security_management/overview_security_management.php> [Accessed 25 Apr. 2015].

Itil.osiatis.es, (2015). [online] Available at: <http://itil.osiatis.es/ITIL_course/it_service_management/security_management/process_security_management/process_security_management.php> [Accessed 25 Apr. 2015].

Tutorialsweb.com, (2015). ITIL Foundation Certification Notes. [online] Available at: <http://www.tutorialsweb.com/CertNotes/ITIL-cert/itil-foundation-6.htm#4.8.4> [Accessed 25 Apr. 2015].

Wikipedia, (2015). ISO/IEC 27002. [online] Available at: <http://en.wikipedia.org/wiki/ISO/IEC_27002> [Accessed 25 Apr. 2015].

Wikipedia, (2015). IT risk management. [online] Available at: <http://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment> [Accessed 25 Apr. 2015].