CE/CZ 4064 - Security Management

Project 4 - Information Security Management Assessment

Authors:
Au Jit Seah (K1720050K)
Huang Peng (PHUANG008)
Wong Jing Yao (JWONG042)

Table of Contents

Purpose of the Assessment report

This Information Security Management System (ISMS) Assessment report serves individuals associated with the design, development, implementation, operation, maintenance, and disposition of Information Security Management Systems[1]. It is to provide a framework and guidelines to design, implement, access and monitor the Information Security Management System in the subsidiary companies. The scoring mechanisms derived from the appropriate measurements in the security controls enable the organization to either set the goals/targets or know the current/previous status of the information security assessments. Moreover, it can be used as part of justification process to obtain budget to build/acquire, manage and maintain secure information systems. We proposed to use the ISMS Assessment Matrix[2] for one of the selected subsidiary companies and upon having acceptances from all the stakeholders, we can use these guidelines to build the ISMS for the other subsidiaries in the organization.

Information Security Management System Assessments

Generally, the ISMS Assessment Matrix will be used to determine the current and previous information security management posture of the organization and its subsidiary companies. The score ratings in each security control objectives provide the identified security levels to achieve for the subsidiary company and can be shown to management on improvements over time with the implementation of the relevant controls.

We have used the ISMS Assessment Matrix to assess the current status of one of the identified subsidiary companies (located in Singapore) using the measures and set future goals for the respective security controls. The following summarize the desired security goals or actions for the Information Security Management System in the subsidiary company:

A.5 Information Security Policies (Targeted Score = 4)

This segment highlights the need to provide management with directions and support for drafting up information security policies in accordance with business requirements and relevant law and regulations. The set of information security policies are to be defined, approved by management, published and communicated to relevant subsidiary companies. At a high level, policies should address requirements created by business strategy, regulations, legislations and contracts. At a low level, policies should address topic-specific policies such as access control (Clause 9), information classification (clause 8.2), end user oriented topics such as acceptable use of assets (clause 8.1.3), information transfer (clause 13.2.1), restrictions on software installations and use (clause 12.6.2), cryptographic controls (clause 10), communications security (clause 13).

A.6 Organization of Information Security (Targeted Score = 4)

This segment deals with internal organization of information security which aims to establish a management framework to initiate and control the implementation and operation of information security within the organization, as well as ensuring the security of teleworking and use of mobile devices. All information security roles and responsibilities should be defined and allocated within the company, followed by the segregation of duties to respective employees. Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. Appropriate contacts with relevant authorities should be maintained,

if assistance from external authorities is required. Information security should be addressed in project management, regardless of the type of the project. That includes projects launched in subsidiary companies. A liaison between the parent company and its subsidiary companies should ensure that the projects are in line with security protocols of the parent company.

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices in both the parent company and its subsidiary companies. Employees are not allowed to use these devices interchangeably between the parent company and its subsidiaries. All company mobile devices is to be issued from the parent company.

A.7 Human Resource Security (Targeted Score = 4)

The objective of this clause is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered prior to employment, that they are aware of and fulfil their information security responsibilities during employment, and to protect the organization's interests as part of the process of changing or terminating employment.

Prior to employment, a thorough screening of employees is to be carried out in both parent company and its subsidiaries, whereby personnel from HR department and IT department is to be part of the interviewing and screening process. Verification of employees' background includes academic qualifications, independent identity verification, credit review, criminal records, personality and trustworthiness and whether he has the necessary skills for the required position.

During employment, management from both parent and subsidiary companies is to ensure a high morale in the working environment, and to provide training for employees to keep up to date with technological advancements. A formal disciplinary process must be in place to take actions against employees who have committed an information security breach.

After termination, information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

A.8 Asset Management (Targeted Score = 4)

The main aim of this clause is to identify organizational assets and define appropriate protection responsibilities, to ensure that information receives an appropriate level of protection in accordance with its importance to the organization and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

The inventory of assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. These assets must be owned by at least 1 employee. All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement. Assets delegated to subsidiaries must go through stringent checks to ensure no confidential information is leaked from the parent company to its subsidiary. The handling of assets, labelling and classification of information must be standardized between parent and subsidiaries to ensure a smooth flow of information. All

removable media that is scheduled for removable by subsidiary company is to be surrendered to parent company first.

A.9 Access Control (Targeted Score = 4)

The main objective of this clause is to limit access to information and information processing facilities, to ensure authorized user access and to prevent unauthorized access to systems and services, to make users accountable for safeguarding their authentication information, and to prevent unauthorized access to systems and applications. An access control policy should be established, documented and reviewed based on business and information security requirement and users should only be provided with access to the network and network services that they have been specifically authorized to use. User access for subsidiary companies should only be granted by the parent company. Subsidiaries are not allowed to grant access controls to one another. All back-end processes is to be done in the parent company, and subsidiaries are not allowed to store any confidential information pertaining to the whole organization in their internal server. All data is to be stored in the parent company.

A.10 Cryptography (Targeted Score = 4)

Cryptography is an important component of information systems and has to be dealt carefully with in order to ensure proper and effective use of this technology to protect the confidentiality, authenticity and integrity of information. The efficient adoption of cryptography involves mainly 2 stages: the development of the policies and the following management to take care of the policies and ensure proper actions are taken according to the requirements listed in the policies.

The policies development should clearly identify the management approach, principles, roles and responsibilities and target at achieving confidentiality, integrity, non-repudiation and authentication. The protection should be decided wisely based on the matric such as type, strength and quality of the encryption algorithm used. Apart from the cryptography itself, more actions need to be taken to make sure that the cryptographic keys are kept in safe places. Rules should also be made regarding the lifetime, protection level of the cryptography keys as well as the related equipment and systems.

A.11 Physical and Environmental Security (Targeted score = 4)

Physical and environmental security are extremely important, and they are also quite vulnerable without proper planning and efficient policies and measures being taken out. Two major areas fall under this security: secure areas and equipment. While the first one aims to prevent unauthorized physical access, damage and interferences to the information facilities, the second aims to prevent loss, damage, theft or compromise of assets and interruption to the operations.

To protect secure area, policies should be clearly drafted to identify the security perimeters, after which entry controls, security personnel should be deployed in the places of requirements to make guard these areas. At the same time, the events happening in these areas, such as working, loading and unloading of goods, and even unexpected events such as theft and natural disasters should have their corresponding handling methods to make sure that these events are appropriately monitored and remedy actions are standing by in case of happenings of the negative events.

To protect the equipment, attention should be paid to the location and physical barriers. Power cables, communication cables should also be taken care of. Policies regarding

maintenance and services of the equipment, recording of the equipment when they are off-premise, and re-use and disposal of the equipment should be drafted and adhered to closely.

A.12 Operations Security (Targeted Score = 4)

Operations security is one of the most important and complex aspect of the entire securities process due to its sheer size of complexity. The main areas under this security is operational procedures to ensure correct and escape operations of information processing facilities, protection from malware, backup to protect against loss of data, logging and monitoring to record events and generate evidence, and technical and information system vulnerability.

Policies should be drafted to clarify standard operating procedures and capacity managements. At the same time, controls should be adopted against malware. Proper monitoring and logging should also be set up to make sure that problems are discovered in the early stage and taken care of with proper measures. Backups should also be properly set up to protect the loss of data.

A.13 Communications Security (Targeted Score = 4)

Communication is important in the security process because a lot of data pass through the communication channels and losing or malicious modification of these data can result in huge negative impacts. To achieve communications security, two particular areas need to be considered network security to ensure the protection of information in networks and information transfer to maintain the security of information transferred within an organization and with any external entity.

To achieve the first area, proper network controls should eb established. Segregation of network domains should be properly designed. Apart from network, information transfer should be established on the basis on the safety and confidentiality of the information within the organization and between the organization and the external parties.

A.14 System Acquisition, Development and Maintenance (Targeted Score = 4)

Information security is an essential component of information systems and has to be involved early in the design phase of lifecycle for both new and enhancements to existing information systems. Additional security requirements are to be defined for services over public networks. Secure development policies for in-house/outsourced development, development environments and system engineering principles, change control procedures, technical reviews, restrictions on changes on software packages, system security and acceptance testing are required to ensure information security is part of secure development process.

Whenever operational data is used for testing, formal data protection and privacy policies shall be followed for the protection and usage of data in accordance to the relevant regulations and jurisdictions. Obfuscation of the Personally Identifiable Information (PII), removal of sensitive contents for data processing/transfer and destruction of the data after used in the test environments. All performed testing activities are logged for traceability and future audit purposes.

A.15 Supplier Relationships (Targeted Score = 4)

The subsidiary company shall provide information security policies, processes and procedures that require the suppliers to implement accurate and complete controls to meet the information security goals (i.e. confidentiality, integrity and availability). Train the

personnel involved in handling acquisitions, incidents and contingencies associated with supplier access. Explicit definitions of the information security requirements (e.g. information classification, access controls, reviews, audits) for the information access (i.e. processing, in transit, storage and disposal) in the supplier agreements.

The supplier management process shall identify the critical supplied technology or service components and assure that these critical components are traceable throughout the supply chain. The responsibility for managing supplier relationships should be assigned to a service management individual or team to review compliance with the supplier service agreement. This individual or team shall evaluate and validate that the new technologies provided by the supplier that mitigate the identified security risks.

A.16 Information Security Incident Management (Targeted Score = 4)

The information security team is responsible to establish an effective and orderly response to information security incidents. Whenever a security event is discovered, it is promptly reported via the established reporting channel. An information security lead shall be assigned to contain and mitigate the associated security risks and perform corrective actions till closure of the reported security event. After the information security event assessment, the security weakness is documented and whether the events will cause a security incident are determined. Impact Analysis and remediation actions are performed on the identified vulnerabilities and documented in the monthly security report.

During évidence collection, certified investigating personnel shall use only professional tools. Legal is involved early in the evidence collection process in order to maximize the chances for admission of the collected evidence. After post-incident analysis is performed, the Information Security management shall communicate the need-to-know details to both the internal/external people or organizations. Information security incident response training shall be part of New Employee Orientation program for Information Security new hires. Regular sharing of up-to-date information on security incidents and remediations via intranet bulletins/portals are important to the information security team.

A.17 Information Security Aspects of Business Continuity Management (Targeted Score = 4)

The subsidiary company shall identify the information security requirements and have them implemented in the Business Continuity Management Systems. The Business Impact Analysis (BIA) is used to access the impacts over time of not offering the required services (e.g. due to damage to physical assets, loss of life, denial of service). Prioritized timeframes are set for resuming the affected services/activities based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

The identified information security controls shall be maintained and aligned with the predetermined level of business objectives during adverse situations. These controls within the business continuity or disaster recovery processes, procedures and supporting systems need to be revised and reviewed on a half-yearly basis. Whenever there are changes in the Business Continuity or Disaster Recovery procedures, these information security continuity controls shall be reviewed for continual validities and effectiveness to maintain the desired Service Level Agreements during adverse situations. The redundant information systems shall be tested on a regular basis (e.g. quarterly) to ensure failover from one system to another system works as required in order to satisfy the business availability requirements.

Ensure sufficient redundancies for information processing facilities to provide “Business As Usual” during adverse situations.

A.18 Compliance (Targeted Score = 4)

The Information Security team shall work with the legal to identify and review all relevant legislative and contractual business requirements for each information system to avoid any form of legal breaches. Regular compliance awareness programs on intellectual property rights, storage and handling of records are conducted for all employees with reminders that violators shall have disciplinary actions taken against them.

A privacy officer or team is appointed to provide guidance on abiding to the data privacy and protection policies (include the import and export of hardware or software components that perform cryptographic functions). An independent review committee shall review/validate the relevancy of the controls, policies, processes and procedures. Identified corrective measures for non-compliant areas shall be assigned to the individual/team responsible in the respective implementation areas whom shall report the closure and sign-off the identified changes to the review committee.

Technical compliance reviews shall be conducted on half-yearly basis by technical specialists using automated tools whenever possible to general reports for subsequent interpretations. Penetration Testing and vulnerability assessments shall be conducted on half-yearly basis or whenever major security incidents have been reported inside or outside organization.

Representations

After all the scores are calculated put into a general report, analysis will be taken through a radar chart (Appendix 4). In the radar chart, the subsidiary and the parent companies will clearly show the targeted score for each of the objective and the current score that the subsidiary company gets. They will have a clear understanding of the areas of improvements by seeing the gap between the inner polygon and the outer polygon so that the areas of improvements can be clearly identified.

After objectives are identified, the companies should always go back to the ISMS Assessment Matrix, find the related objective and the controls inside it to figure out the guidelines and suggestions for improvements. They can find the measures as well as scenarios and decisions in the matrix for them to reflect upon what they have done insufficiently. In tis way, actions can be identified for the subsidiary company to undertake so as to have systematic progression from the current scores to the identified scores with the goal settings.

Conclusions

The ISMS Assessment Matrix we come up with will act as a solid guideline by providing the parent and subsidiary companies to match their actions to the requirements and come up with reliable performance score. At the same time, general guidelines and actions are also included in the matrix to guide the companies in improving themselves along the way. Appropriate graph representations are also available to provide a more visual and clearer representation of the current status and the target and serves as a motivation for the companies to improve. We are confident that this ISMS Assessment Matrix will serve its purpose well in assessing companies according to the ISO 27001 standards.

Appendices

[A] Audiences

- Individuals with mission/business ownership responsibilities or fiduciary responsibilities (e.g. chief executive officers, chief financial officers, chief information officers, chief information security officers)

- Individuals with information system development and integration responsibilities (e.g., program managers, information technology product developers, information system developers, information systems integrators, enterprise architects, information security architects)

- Individuals with information system and/or security management/oversight responsibilities (e.g., senior leaders, risk executives, authorizing officials, chief information officers, senior information security officers)

- Individuals with information system and security control assessment and monitoring responsibilities (e.g., system evaluators, assessors/assessment teams, independent verification and validation assessors, auditors, or information system owners)

- Individuals with information security implementation and operational responsibilities (e.g., information system owners, common control providers, information owners/stewards, mission/business owners, information security architects, information system security engineers/officers).

[B] ISMS Assessment Matrix

For clearer full matrix please refer to the attachment:

ISO 27001-2013	Objectives	Controls	Measures	Scenarios	Decision/actions	Champion	Score Ratings (1 - 5)	Goal Raw Score	Current Raw Score	Goal Total Weighted Scores	Current Total Weighted Scores	Weights
A.5	**Information security Policies**									**4**	**2**	**0.5**
A.5.1	Management direction for information security Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.											
A.5.1.1	Policies for information security	Set of information security policies are to be defined, approved by management, published and communicated to relevant external parties	At a high level, policies should address requirements created by business strategy, regulations, legislations and contracts. At a low level, policies should address topic-specific policies such as access control (Clause 9), information classification (clause 8.2), end user oriented topics such as acceptable use of assets (clause 8.1.3), information transfer (clause 13.2.1), restrictions on software installations and use (clause 12.6.2), cryptographic controls (clause 10), communications security (clause 13).	To ensure that policies for information security adheres to the security standards, and are inlined with management's and company's goal and vision, the technical expertise of IT security professionals and consultants could be tapped on by the management, A transparent, fast and efficient means of communication of updated policies between employeers, management, external parties and subsidiary companies, in a form that is relevant, accessible and understandable.	IT security department head to serve as IT security consultant and liase with management/senior management to provide solutions, advices for information security policies. He or she is to be kept updated on new management decisions with respect to any new policies to be implemented, as well as to communicate them with his or her department. Trusted IT security committee is to conduct period audits on external vendors, subsidiary companies to ensure that they are inline with company's security standards. A top down approach of communication channels is shown in the diagram:  	Jing Yao	5 : Company's information security policies strictly adhere to ISO/IEC TR 27005 security standards, fulfilling all high level and low level requirements. All employees, external vendors, subsidiary companies and involved departments are aware of the information security policies inplace and strictly adhere to them. 4 : Company's information security policies adhere to most of ISO/IEC TR 27005 security standards, fulfilling at least 80% of high level and low level requirements. More than 75% of external vendors, subsidary companies and involved departments are aware of the information security policies inplace and adhere to 80% of them. 3 : Company's information security policies adhere to some of ISO/IEC TR 27005 security standards, fulfilling at least 60% of high level and low level requirements. More than 50% of external vendors, subsidary companies and involved departments are aware of the information security policies inplace and adhere to 60% of them. 2 : Company's information security policies adhere to a few of ISO/IEC TR 27005 security standards, fulfilling at least 30% of high level and low level requirements. More than 25% of external vendors, subsidary companies and involved departments are aware of the information security policies inplace and adhere to 30% of them. 1 : Company's information security policies adhere to very little of ISO/IEC TR 27005 security standards, fulfilling less than 25% of high level and low level requirements. Less than 25% of external vendors, subsidary companies and involved departmnts are aware of the information security policies inplace and adhere toless than 30% of them.	4	3			
A.5.1.2	Review of the policies for information security	The company's information security policies should be reviewed at periodic intervals or if significant changes occur to ensure suitabality, adequacy and effectiveness	Each member of the IT security department is spearheading the development of information security policies. Reviews should include revising current policies to ensure no loopholes, assessing opportunities for improvement of the policies in response to changes in organizational environment, business circumstances, legal conditions and technical environment.	Semiannual reviews should be conducted to ensure that exisiting policies are up to date with current circumstances. Roster of responsibilities is up to date with current manpower. It includes ownership of each informatoin security policy, timeline and milestones for pre-review and after review.	Both internal IT auditing committee and IT security employees are to be involved in the semiannual information seurity policies review, with IT security head leading the session. Every employee is to conduct a presentation on current security policies he or she is in charge of, and any future improvements that can be made. IT security head is to notify everyone of current management directions. Roster of responsibilities is to be updated by assistant HOD if there is any changes in roster due to manpower changes.	Jing Yao	5 : Semiannual review is conducted right on schedule with everyone present. All IT team members in charge of their respective information security policies gave outstanding presentations. Thorough review of current policies are made and reasonable improvements are suggested. IT Head is aware of current management directions and able to communicate it with the department. Roster of responsibilities is up to date. 4 : Semiannual review is conducted right on schedule, with everyone present. All IT team members gave presentations, although a few fell short of their requirements. Some reasonable improvements are suggested. IT Head is aware of current management directions and able to communicate it with the department. Roster of responsibilities is up to date. 3 : Semiannual review is conducted right on schedule, with almost full attendance. All IT team members gave presentations, although 25% of them fell short of their requirements. Some improvements are suggested, albeit unrealistic and unreasonable. IT Head is aware of current management directions and somewhat able to communicate it with the department. Roster of responsibilities is up to date. 2 : Semiannual review is conducted right on schedule, with at least 75% attendance. Most IT team members gave presentations, although more than 50% of them fell short of their requirements. Little improvements are suggested. IT Head is aware of current management directions and somewhat able to communicate it with the department. Roster of responsibilities is up to date. 1 : No review is conducted	4	2			

A.6	Organization of information security								
A.6.1	Internal organization Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.								
A.6.1.1	Information security roles and responsibilities.	All information security roles and responsibilities should be defined and allocated	Roles and responsibilities for each information security policy are to be clearly defined and communicated to all IT security employees. Team leaders are in charge of multiple security policies. Intrinsic security processes, risk management for acceptance of residual risks should be identified, and responsibilities to be delegated to team members. Information security manager is to take overall responsibility for the development and implementation of information security. 1. Assets and information security processes should be identified and defined. 2. Entity responsible for each asset or information security process should be assigned and details of his responsibilty should be documented. 3. Authorization levels should be defined and documented 4. Appointed individuals should be competent and be given frequent training to be up to date with current technological developments.	Form an information security department to oversee all processes and information security standards. An information security manager will lead this department and liase with other department heads. Assets require day-to-day protection from respective responsibility holders.	Senior management is to appoint an information security manager. He or she will then source for manpower for the information security department. Each asset identified must be assigned an owner who will be incharge of it's day to day protection. Responsibilities must be clearly indicated for the whole department, so that everyone is accountable for every asset. Different levels of authorization is to be set up. Low level of authorization pertaining to assets and information security processes that does not hold critical information can be given to all information security employees. Mid level authorization comprises of assets and processes that could compromise the integrity of information security if mishandled. Only trustable employees with a good track record and years of experience is given this level of authorization. High level authorization is given to processes and assets which are highly confidential and if compromised, could result in huge losses. Only the top management executives are given this level of authorization.	Jing Yao	5: All assets and information security processes are identified and defined. Sufficient manpower is allocated for each asset and information security process, with the details of their responsibilities well documented. Authorization levels are well defined and documented. 4: All assets and information security processes are identified and defined. Sufficient manpower is allocated for each asset and information security process, with the details of their responsibilities well documented. Authorization levels are well defined and documented. A few minor lapses in present. 3: All assets and information security processes are identified and defined. However, insufficient manpower is allocated for each asset and information security process, with the details of their responsibilities well documented. Authorization levels are well defined and documented. some lapses, but generally not high risk. 2: Some assets and information security processes are identified and defined. lack of manpower for each asset and information security process, with the details of their responsibilities well documented. Authorization levels are defined and documented. huge lapses which may pose a potential risk to the company. 1: Very little is done to identify and define roles and responsibilities for information security	4	3
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	No individual is to be in charge of large amount of assets or entire processes. Each asset and different parts of the information security process is to be managed by different individuals.	In a large organization, there are many levels of authentication, information security processes and large amount of assets. These are delegated to information security specialists to maintain. However, there is a tradeoff between manpower allocation and information security. Maximizing manpower efficiency by allocating large amounts of assets and processes could lead to a violation of ISO 27006.1.2 security standard, whereas allocating large amounts of manpower would result in low efficiency.	In a large organization, sufficient manpower must be allocated to information security such that no individual is in full control of any process or asset. This is to ensure that no single person can access, modify or use assets without authorization or detection. If there is not enough manpower and it is difficult to segregate the duties, other controls such as monitoring of activities, audit trails and management supervision should be considered.	Jing Yao	5: Every asset and process is managed by a number of employees at all times, where their responsibilities are mutually exclusive. 3: Some employees are holding on to multiple responsibilities for an asset or a single process. 1: Huge shortage of manpower leading to entire processes or assets being managed by a single person.	5	3
A. 6.1.3	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.	Organizations must have procedures that specify when and whom authorities should be contacted and how identified information security incidents should be reported in time.	A power outage would be detrimental if power is not restored in time. It could lead to a breach in security while the system is down. An external DDoS alert is flagged and the relevant authorities need to be contacted to repel this threat.	All employees are required to know the hotline phone numbers and contact person, as well as the procedures should there be a need. This include power outages, fire alarm, faulty machinery, physical intrusion, software intrusion, compliance, audit, consultation. Noticeboards must be placed in an accessible area and kept up to date with the respective hotline numbers. This includes an extension line to another department, or a line to external vendors.	Jing Yao	5: All contact numbers are kept up to date and every employee is aware of the procedures and numbers to call. Noticeboard is in an accessible location. 3: Some contact numbers are outdated and some employees are unaware of the procedures to contact the relevant authorities. 1: No physical noticeboard for employees to refer to if they wish to contact the relevant authorities.	5	3
A. 6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	Memberships in special interest groups or forums to: 1. improve knowledge and best practices to stay up to date with relevant security information 2. Receive early warnings of new alets, patches and advisories pertaining to attacks and vulnerabilities. 3. Access to specialist information security advice. 4. Exchange information about new technologies Information sharing agreements are set up to improve coorperation and coordination of security issues.	In a fast changing society, information security environment is constantly improving. What works now may not work in the future. To keep up with the times, not only do information security specialists have to constantly improve their skills, they need to have a wide network of connections to always be in the know.	Join open source forums and communities which discusses the latest information security trends and the latest technologies. Platforms like GitHub and Reddit offer many technicial intricasies to solutions that companies may face in the workplace. Employees in the information security department are required to be part of these communities to be kept up to date with the latest trends. There can be bi-annual sharing sessions where selected employees are required to present on the latest trends and information they found in these communities.	Jing Yao	5: All of the employees are part of at least 1 IT forum, and are actively participating in these communities. Many new concepts and solutions are brought up in the bi-annual sharing 3: Some of the employees are part of at least 1 IT forum and are quite active in them. Some new concepts and solutions are brought up in the bi-annual sharing session. 2: Some of the employees are part of at least 1 IT forum. There is no sharing session among the department. 1: Only a few of the employees are part of these special interest groups.	3	2
A 6.1.5	Information security in project management	Information security should be addressed in project management, regardless of the type of the project.	Information security objectives are should be included in project objectives. Information security risk is conducted at an early stage of the project to identify necessary controls Information security is observed throughtout the course of the project.	Regardless of the origin of the project, information security should be integrated into the organization's project management method to ensure that information security risks are identified and addressed as part of the project.	During the draft of any project, an employee of the information security department must be present to advise on the requirements for information security on the project. The employee must be accountable for all aspects of information security throughout the course of the project, from project planning phase to project completion. Frequent review and audits to ensure that information security requirements are always met.	Jing Yao	5: Prior to any submission of project proposal, an information security employee must first be consulted and be part of the management of this project. Frequent audits are present, and information security requirements are always being met, from project planning phase to project completion. 4: Frequent audits present, and information security requirements are met most of the time. 3: During project planning phase, information security objectives are not focused and lacking in depth analysis. 2: Very little information security objectives are identified during project planning, and are mostly not met during project execution. 1: No information security personnel is present during project planning. Information security objectives are missing.	4	3

A.6.2	Mobile devices and teleworking Objective: To ensure the security of teleworking and use of mobile devices.											
A 6.2.1	Mobile device policy	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	All mobile devices must be registered with the company. No personal laptops are allowed in the work premises. Only company issued workstations are allowed. Company workstations have strict restrictions on network access and employees are not allowed to connect to public networks. Company workstations are equiped with the latest malware protection . Should there be a a network breach originating from a localised address, immediate measures must be taken to block the device. A follow up investigation must be ordered to find out about the lapse.	Employees are constantly reminded the importance of information security in the organisation, and never to compromise the integrity of the system, by engaging in unsafe network practices. Employees are fully responsible for their own mobile devices. These mobile devices are susceptible to physical theft.	Frequent audits and checks to ensure that all employees abide by the rules and regulations. Should there be a breach of conduct, a fine should be issued to the offender. Should there be a physical loss of these devices, a report must be immediately lodged to the organisation, such that necessary measures can be taken to ensure sensitive information in these devices are not compromised.	Jing Yao	5: To ensure that all sensitive information are kept, the company is declared as a red zone, which prohibits all mobile devices from entering or exiting the work premises. All work related assets must be left at the workplace, and personal mobile devices must be surrended before entering the workplace. 4: Employees are allowed to bring in their personal mobile devices, but are not allowed to leave the premises with any company related assets. 3: Employees are allowed to bring in their personal mobile devices and leave the premises with company related assets. Stringent checks to ensure that all employees adhere to the code of conduct. 2: Employees are allowed to bring in their personal mobile devices and leave the premises with company related assets. insufficient checks to ensure that all employees adhere to the code of conduct. 1: Existing breach of information security due to mobile devices being compromised.	4	3			
A 6.2.2	Teleworking	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as telecommuting, flexible workplace, remote work and virtual work environments.	Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking.	Employees using teleworking are allowed to bring their workstations out of the work premises. These workstations are subjected to physical theft, security breach in a public network, as well as misuse.	Stringent and frequent checks on these employees to be carried out. Their workstations are subjected to frequent audits, and must be frequently changed. Use of home networks and wireless network services is tighly regulated. Provision of virtual desktop access by the company is present.	Jing Yao	5: Teleworking is not allowed in the company. 4: Teleworking is allowed, only for a handful of individuals. 3: Teleworking is generally allowed, frequent audits to ensure no lapses. 2: Less frequent audits 1: No audits at all.	4	3			
A.7	**Human resources security**									**4**	**2**	**0.16**
A.7.1	Prior to employment Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.											
A 7.1.1	Screening	Background checks on all candidates for employment to be carried out	Verification of employees background includes: Academic qualifications Independent identity verification Credit review, criminal records Personality and trustworthiness Has the necessary skills for the required position.	The hiring of IT personnels should be handled by management from the IT department, not just the HR department.	During the hiring process, a team of interviewers should comprise of members from the IT department and HR department. IT interviewer should access the techincal skillsets of the interviewee, while HR interviewer should access the personality of the interviewee.	Jing Yao	5: A thorough background check of all interviewee is carried out. This includes sourcing for information on personal media accounts, referrals, and face to face interviewing. Team of interviewers are equipped with the necessary interviewing skills to access candidates. 3: Sufficient background checks on interviewee, limited to resume and face to face interviewing. 1: Insufficient screening of candidate, whereby interviewing process only involved interviewer from HR department.	5	3			
A 7.1.2	Terms and conditions of employment	Employers are to explicitly state the responsibilities of employee for information security in a contractual agreement.	Black and white contracts are to be drafted as evidence of agreement between employer and employee. Contract is to include: Condifentiality agreement Personal Data Protection Act Legal responsibilities and rights Responsibilities and roles of employee Actions to be taken upon violation of agreement	All incoming employees are mandated to sign a contract of agreement with the company. Failure to do so will result in employee's application rejection.	Company is to have a template contract of agreement that is universal for all incoming employees in the IT security department.	Jing Yao	5: Contract of agreement template is well drafted. It includes all the listed requirements a contract should have, as well as the terms and conditions for employment. 3: Contract of agreement lacks some information, but is generally acceptable. 1: Contract of agreement is very simple and lacks important information.	5	3			
A.7.2	During employment Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.											
A 7.2.1	Management responsibilities	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Management responsibilities should include ensuring employees and contractors: Are properly briefed on their information security responsibilities and roles Are motivated to fulfil their roles and responsibilities Conform to the terms and conditions of employment Are constantly up to date with the skills necessary to perform their responsibilities	A motivated and well informed employee is less likely to cause information security incidents or cause considerable damage to the organization.	An orientation must be held for incoming employees to get them to familiarise themselves with the new environment, and understand more about their roles and responsibilities from the senior colleagues. Management's role should not just be a boss of their employees, but a leader, a mentor, and a friend. Motivating their employees can be in the form of occasional department events and lunches.	Jing Yao	5: Employees are motivated and are well informed of their roles and responsibilities. Management is doing a splendid job to ensure high morale in the organization. 3: Employees are going on with their tasks as per norm. 2: Low morale in the organization although management is doing something about it. 1: Low morale in the organization and management is not doing anything about it.	5	3			
A 7.2.2	Information security awareness, education and training	All employees of the organization is to undergo regular training and updates in relevant skillsets for their job function.	Information security awareness should be established in line with organization's information security policies and procedures. Awareness training can be in the form of class-room based learning, distance learning, self-paced, web based and others, focusing on the 'what', 'how' and 'why' with respected to the importance of information security. Information security trainng and education should cover the following: 1. stating management's commitment to information security throughout the organization. 2. the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements. 3. Personal accountability for one's actions and inactions. 4. Basic information security procedures.	Due to complacency, employees may start to downplay the importance of information security. This may cause lapses in security.	A periodic awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills. An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.	Jing Yao	5: Bi-annual awareness, education and training of employees is held. Reputable external vendors are invited to give talks and update employees on recent technological advancements, and the importance of information security. All employees manage to score excellent marks in the assessment at the end of the training. 4: Employees manage to score reasonable marks in the assessment. 3: Awareness, education and training of employees is held semi-annually instead of bi-annually. 2: Awareness, education and training of employees are very superficial. Not much is learnt. 1: No such training is present.	5	3			
A 7.2.3	Disciplinary process	There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Information security breach needs to be verified and confirmed. Disciplinary process should be fair for employees who are suspected of committing breaches of information security. Disciplinary process should be held internally for the first or second offenders. Escalation of disciplinary actions to be taken for repeated offenders, with the most serious offenders being refered to external regulatory authorities.	An employee is suspected of being in violation of information security breach. Not enough information is available prior.	An investigative committee is set up to investigate the violation. Employee needs to be given notice. If the employee is found to be in violation, disciplinary process is to be carried out after confirmation.	Jing Yao	5: An internal disciplinary committee is present to look into cases where employees are suspected of being in violation of security protocols. Disciplinary process is fair and impartial. 3: Disciplinary process has a few lapses but generally still able to serve as a deterrent for others. 2: Disciplinary process has huge lapses and offender is able to escape with minimal repercussions. 1: No disciplinary committee present.	5	3			

A.7.3	Termination and change of employment	Objective: To protect the organization's interests as part of the process of changing or terminating employment.										
A. 7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.	Prior notice is to be given to employee due for termination. Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment Hand-over process is to be initiated to ensure smooth transition of responsibilities between different employees	An employee is resigning in a month's time. Proper handover procedures is to be initiated to ensure that outgoing employee does not leave with any of the organization's confidential information, while incoming employee is able to smoothly transition into this role.	A short transition period is initiated, whereby at no point in time will there be a lapse in manpower. HR is to work closely with supervising manager to manage information security aspects of te relevant procedures. Changes in personnel is to be made known to relevant affected parties.	Jing Yao	5: transition period is well handled and there is a smooth transition between the outgoing and incoming employee. Outgoing employee remains accountable and contactable for processes that he/she had been in charge of. 4: .Responsibilities and duties that remain valid are communicated clearly to employee after termination. 3: A small delay in the transition but generally no risk involved 2: Responsibilities and duties that remain valid are not communicated to employee after termination, resulting in lack of accountability. 1: Outgoing employee shreds all responsibilities due to not being communicated of termination procedures, and is not liable for accountability should there be any faults in his procedures during his term of service.	4	3			
A.8	**Asset Management**									**4**	**3**	**0.1**
A.8.1	Responsibility for assets	Objective: To identify organizational assets and define appropriate protection responsibilities.										
A. 8.1.1	Inventory of assets	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.	An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate. The asset inventory should be accurate, up to date, consistent and aligned with other inventories.	An organization has a large database of assets to keep track of.	A dedicated team of asset management employees should be present to ensure that asset inventory are well organised and up to date. Monthly stock taking should be present.	Jing Yao	5: Asset management team is competent. Stock taking done with due diligence, accurate and on time. 4: A small delay in the updating of assets. But accurate nonetheless. 3: Some inaccuracy in asset inventory, but generally well organised. 2: Disorganised management of assets. 1: No asset management present.	4	3			
A 8.1.2	Ownership of assets	Assets maintained in the inventory should be owned.	An owner is given ownership to an asset as well as other entities after having approved management responsibility for them. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle. The owner should: 1. ensure that assets are inventoried; 2. ensure that assets are appropriately classified and protected; 3. define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies; 4. ensure proper handling when the asset is deleted or destroyed.	A new asset is created	An owner is to claim ownership of the asset. The owner of this asset is accountable for the delivery of the service, including the operation of the asset.	Jing Yao	5: All assets are owned. 4: More than 80% of the assets are owned. 3: More than 50% of the assets are owned. 2: Assets are mishandled 1: No ownership of assets	5	4			
A 8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.	Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.	An owner of an asset is fully responsible and accountable for the usage of the asset.	The owner is not allowed to use the asset for personal interests and personal gains. Assets should not be used for exploitation, blackmailing, monetary gains.	Jing Yao	5: Rules for the usage of assets is well identified, documented and implemented. 3: Implementation of the rules require improvements. 1: No rules for usage of assets.	5	3			
A 8.1.4	Return of assets	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.	An employee due for termination has to return all the assets under his possesion	The termination process is invoked, which require the organization to control unauthorized copying of sensitive information by terminated employee.	Jing Yao	5: Smooth return of assets. No mishandling or withholding of sensitive information by terminated employee. 4: Smooth return of assets. Accidental mishandling of information is detected by terminated employee is detected and handled. No sensitive information is leaked. 3: Smooth return of assets. Some of the assets are compromised but recovery with low risk is possible 2: Terminated employee continues to hold on to sensitive information. Some of the assets are not returned. 1: Assets are not returned.	5	4			
A.8.2	Information classification	Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.										
A 8.2.1	Classification of information	Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset. The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered.	Information can cease to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or on the contrary under-classification can endanger the achievement of business objectives.	An example of an information confidentiality classification scheme could be based on four levels as follows: 1. disclosure causes no harm; 2. disclosure causes minor embarrassment or minor operational inconvenience; 3. disclosure has a significant short term impact on operations or tactical objectives; 4. disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.	Jing Yao	5: Accurate classification of information. Results of classification indicate value of assets depending on their sensitivity and criticality to the organization respect to confidentiality, integrity and availability. The scheme is consistent across the whole organization. 4: Scheme is generally consistent throughout organization, with small inaccuracy in classification. 3: Scheme is not consistent throughout organization 2: Classifications are missing out on major aspects. 1: No classification present.	4	3			
A 8.2.2	Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in 8.2.1. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media.	Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and Metadata are a common form of labelling. Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.	A list of buzzwords is used for coming up with labels. Words with similar meaning will fall under the same category in the buzzword header. Buzzwords can be encrypted to prevent external attackers from extracting sensitive information	Jing Yao	5: Labels are simple and easy to understand. 3: Labels are complicated and are not a good representation of the assets and entities that it holds. 1: no labels are present	5	3			
A 8.2.3	Handling of assets	Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification. the following items should be considered: 1. access restrictions supporting the protection requirements for each level of classification; 2. maintenance of a formal record of the authorized recipients of assets; 3. protection of temporary or permanent copies of information to a level consistent with the protection of the original information; 4. storage of IT assets in accordance with manufacturers' specifications; 5. clear marking of all copies of media for the attention of the authorized recipient.	The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, even if the names for levels are similar; in addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical.	Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organizations.	Jing Yao	5: All of the procedures are relevant for handling, processing and communicating information consistent with its classification. Agreements with other organizations in place to ensure accurate identification of classification of the information. 3: No agreements with other agreements. Procedures are solely for internal processes. 2: Procedures are inaccurate for handling, processing and communicating information. 1: Procedures are not relevant for handling, processing and communicating information.	5	3			

A.8.2.3	Handling of assets	Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Procedures should be drawn up for handling, processing, storing and communicating information consistent with its classification. the following items should be considered: 1. access restrictions supporting the protection requirements for each level of classification; 2. maintenance of a formal record of the authorized recipients of assets; 3. protection of temporary or permanent copies of information to a level consistent with the protection of the original information; 4. storage of IT assets in accordance with manufacturers' specifications; 5. clear marking of all copies of media for the attention of the authorized recipient.	The classification scheme used within the organization may not be equivalent to the schemes used by other organizations, even if the names for levels are similar; in addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical.	Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organizations.	Jing Yao	5: All of the procedures are relevant for handling, processing and communicating information consistent with its classification. Agreements with other organizations in place to ensure accurate identification of classification of the information. 3: No agreements with other agreements. Procedures are solely for internal processes. 2: Procedures are inaccurate for handling, processing and communicating information. 1: Procedures are not relevant for handling, processing and communicating information.	5	3			
A.8.3	Media Handling	Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.										
A. 8.3.1	Management of removable media	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	1. if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable; 2. where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail; 3. all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications; 4. if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media; 5. to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable; 6. multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss; 7. registration of removable media should be considered to limit the opportunity for data loss; 8. removable media drives should only be enabled if there is a business reason for doing so; 9. where there is a need to use removable media the transfer of information to such media should be monitored.	A piece of removable media is due for termination	Contents of the removable media is to be removed from the media and be made unrecoverable. Record and documentation of all removals to be kept for auditing. If data is required to be kept, multiple copies of data should be stored in another seprate media to reduce rik of data damage or loss.	Jing Yao	5: All removable media data is cleared and made unrecoverable if due for termination. Accurate and organised documentation of all procedures is present for audit trail. 4: Removable media is disposed and made unrecoverable. Documentation present but may not be accurate. 3: Removable media is disposed and made unrecoverable, but lack of documentation. 2: Removable media is disposed of, however it is still recoverable. 1: Removable media is not disposed of properly, presenting potential risk of data leak and vulnerabilities.	5	4			
A. 8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures.	Formal procedures for the secure disposal of media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure disposal of media containing confidential information should be proportional to the sensitivity of that information.	A piece of media is due for disposable.	A procedure is in place to identify media items that require secure disposal. The procedure weighs on the sensitivity of information in the media. A suitable external party is selected to dispose of the media. Media should be disposed at multiple locations to prevent aggregation effect, whereby the congregation of non-sensitive media could lead to potential sensitive information being leaked.	Jing Yao	5: Multiple external parties are sourced to dispose of the media. Frequent audits on these external parties are required to ensure these media are completely disposed of and not recovered by these parties. 3: A single external party is responsible for disposing all of the media containing sensitive information. 1: Physical disposal of media only. Information is recoverable if fallen into the wrong hands.	5	3			
A 8.3.3	Physical media transfer	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.	1. reliable transport or couriers should be used; 2. a list of authorized couriers should be agreed with management; 3. procedures to verify the identification of couriers should be developed; 4. packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields; 5. logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.	Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. In this control, media include paper documents.	When confidential information on media is not encrypted, additional physical protection of the media should be considered.	Jing Yao	5: Confidential information on media is encrypted. Reliable transport courier is used, packaging is sufficient to protect the contents from any physical damage. Logs should be kept to identify the content of the media, the date, time and venue of the transfer. 3: Confidential information on media is not encrypted 1: A suspicious courier is utilised to transport the media.	5	3			
A.9	**Access control**										**4**	**3**	**0.07**
A. 9.1	Business requirements of access control	Objective: To limit access to information and information processing facilities.										
A. 9.1.1	Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks. The policy should take account of the following: 1. security requirements of business applications. 2. consistency between the access rights and information classification policies of different systems and networks 3. segregation of access control roles, e.g. access request, access authorization, access administration; 4. archiving of records of all significant events concerning the use and management of user identities and secret authentication information; Role based access control to link access rights with business roles. Two of the frequent principles directing the access control policy are: a) Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile); b) Need- to- use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.	There is always a tradeoff between convenience and security when handling access control. A tight security access control would be very inconvenient for the user due to the high levels of complications when trying to authenticate. Whereas a convenient access control will result in security being to lax. A good balance must be found.	To identify the need for convenience over security, the organization needs to identify which processes requires more security. Processes such as In-server authentication, system administrator authentication and back-end processes requires high security with convenience being the tradeoff. Processes such as end user authentication requires less security as users prefers convenience and are not able to remember long passwords.	Jing Yao	5: Asset ownersable to determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks. 3: Generally a fine balance between convenience and security for different specific user roles. 1: Mismatch of access control rules, access rights and restrictions for users towards their assets.	5	3			
A. 9.1.2	Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	This policy should cover: 1. the networks and network services which are allowed to be accessed 2. authorization procedures for determining who is allowed to access which networks and networked services 3. management controls and procedures to protect access to network connections and network services 4. monitoring of the use of network services.	Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations,	A network structure is drawn to make sure that not all workstations are connected directly to the public network. Back-end servers and workstations connect to the network using in-house networks, which are then routed through different layers of authentication and firewalls to the public server.	Jing Yao	5: Network structure shows clearly how each different layer of authentication is linked to one another, from the highly sensitive back-end internal servers to the network access terminals. Only a few ports are directly linked to the public domain, while the rest are connected through several layers of authentication and re-routing from different ports. 4: Less than 25% of the network structure is directly linked to the public domain. 3: about half of the workstations are directly linked to the public domain. 2: More than half of the workstations are directly linked to the public domain. 1: All of the workstations are connected to the public domain, with no evidence of any layers of authentication.	5	4			

A. 9.2	User access management	Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.										
A. 9.2.1	User registration and de-registration	A formal user registration and de-registration process should be implemented to enable assignment of access rights.	The process for managing user IDs should include: 1. using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented 2. immediately disabling or removing user IDs of users who have left the organization 3. periodically identifying and removing or disabling redundant user IDs 4. ensuring that redundant user IDs are not issued to other users.	Creating new user IDs and deleting user IDs are common in the workplace. A new employee has just joined the company and needs a new user ID	Firstly, a database of User IDs are kept in the SQL server. Unique User IDs are used to ensure no duplication of users. When a new user ID is created for the new employee, it first checks the database to see if there is any duplicates. If not, it is stored in the database. Redundant user IDs are frequently checked and filtered in the database.	Jing Yao	5: Database of User IDs is well organised, and is devoid of any redundant user IDs. No duplicate IDs detected in the database. 3: Less than 0.0001% duplicate IDs detected in the database, with a 0% failure to return. 1: Multiple duplicate IDs detected in the database.	5	3			
A 9.2.2	User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	The provisioning process for assigning or revoking access rights granted to user IDs should include: 1. obtaining authorization from the owner of the information system or service for the use of the information system or service. separate approval for access rights from management may also be appropriate 2. verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties 3. ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed; 4. maintaining a central record of access rights granted to a user ID to access information systems and services; 5. adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization; 6. periodically reviewing access rights with owners of the information systems or services	Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews are easier managed at the level of such roles than at the level of particular rights. Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or contractors	User access roles are grouped into different levels of authentication. For example in an organisation, users can be grouped based on their roles. Users are created for the finance department, IT department, logistics department etc. Rights for each of the roles are consistent to every entity in the group. Employees are reminded not to use multiple user IDs or share user IDs with another employee.	Jing Yao	5: Role based Access Control implemented for ease of revoking or assigning access rights. Delegatory access control is present to grant control to other users. Frequent reviews of user access to ensure access control is given/taken away from the correct users. 3: A short delay is present whenever user access needs to be given or taken from a user. 1: No access control protocols are implemented.	5	3			
A 9.2.3	Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	The allocation of privileged access rights should be controlled through a formal authorization process in accordance with the relevant access control policy . The following steps should be considered: 1. the privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be identified 2. privileged access rights should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (see 9.1.1), i.e. based on the minimum requirement for their functional roles 3. an authorization process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization process is complete; 4. requirements for expiry of privileged access rights should be defined 5. privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged 6. specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities	Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems	Administration privileges only given to the top most management executives and the most trustworthy employees. Parsing of information between each systems should be encrypted with one way functions to prevent abuse of administrative priviledges.	Jing Yao	5: Only a few selected individuals hold administrative priviledged access rights. Even so, they are unable to abuse this priviledge as all sensitive information are encrypted with one way functions, which makes it almost impossible to reverse. 4: Encryption is present but is reversible. 3: Some selected individuals hold priviledged access rights. No encryption is present. 2: Priviledged access control is held by too many people. 1: No priviledged access control is present.	5	4			
A. 9.2.4	Management of secret authentication information of users	The allocation of secret authentication information should be controlled through a formal management process.	The process should include the following requirements: 1. users should be required to sign a statement to keep personal secret authentication information confidential and to keep group information. information solely within the members of the group; this signed statement may be included in the terms and conditions of employment. 2. when users are required to maintain their own secret authentication information they should be provided initially with secure temporary secret authentication information, which they are forced to change on first use 3. procedures should be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information 4. temporary secret authentication information should be given to users in a secure manner; the use of external parties or unprotected electronic mail messages should be avoided 5. temporary secret authentication information should be unique to an individual and should not be guessable; 6. users should acknowledge receipt of secret authentication information	Passwords are a commonly used type of secret authentication information and are a common means of verifying a user's identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens that produce authentication codes.	2 factor authentication should be implemented to ensure that both sides authenticate and validate each other. One way functions and salting of passwords must be implemented to ensure that system administrators are not able to reverse the hash functions.	Jing Yao	5: 2 factor authentication present. One way function and salting of passwords present. Hardware token given to user. 4: No one way function used. 3: No salting of passwords. 2: No hardware token. 1: Simple authentication process.	5	3			
A. 9.2.5	Review of user access rights	Asset owners should review users' access rights at regular intervals.	1. users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment 2. user access rights should be reviewed and re-allocated when moving from one role to another within the same organization; 3. authorizations for privileged access rights should be reviewed at more frequent intervals; 4. privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained; 5. changes to privileged accounts should be logged for periodic review.	With the addition and deletion of many user access rights frequently, database can be quite cluttered and laden with redundant user IDs.	Frequent audits and reviews to ensure the database is clean and up to date. Incentives given for good performances.	Jing Yao	5: Frequent audits present. Database is clean and user access rights is checked to ensure that the correct users have the right user access rights. 4: Frequent audits, database is generally clean with few redundant user IDs, and mostly correct user access rights 3: Frequent audits, database is filled with many redundant clutters of user IDs. Many wrong user access rights given to users 2: Infrequent audits. 1: No review present.	5	4			
A. 9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended. This will determine whether it is necessary to remove access rights. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.	In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs.	In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing.	Jing Yao	5: Removal or adjustment of access rights are done immediately upon request or employee's termination 4: Removal or adjustment of access rights are done within 24 hours upon request or employee's termination 3: Removal or adjustment of access rights are done within 48 hours upon request or employee's termination 2: Removal or adjustment of access rights are done within 72 hours upon request or employee's termination. 1: No removal or adjustment of access rights	5	3			
A.9.3	User responsibilities	Objective: To make users accountable for safeguarding their authentication information.										
A 9.3.1	Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	All users should be advised to: 1. keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority; 2. avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely and the method of storing has been approved (e.g. password vault); 3. change secret authentication information whenever there is any indication of its possible compromise; 4. when passwords are used as secret authentication information, select quality passwords with sufficient minimum length	Users are accountable for the confidentiality and secrecy of their own secret authentication information	When users are signing up for a new password, sufficient prompts are given to ensure the password is a strong one. System will only accept passwords that are strong, with a minimum of 8 characters, at least 1 uppercase, 1 lower case and 1 symbol. Under the terms and conditions, users are again reminded to practice responsible handling of their passwords	Jing Yao	5: Password strength of users are enforced through the rejection of weak passwords and prompting users on the types of acceptable passwords. Terms and conditions clearly state the types of good practices when handling their passwords. 3: terms and conditions did not advise users on responsible handling of their passwords 1: Weak passwords are accepted. No prompts given.	5	3			

A.9.4	System and application access control	Objective: To prevent unauthorized access to systems and applications.							
A. 9.4.1	Information access restriction	Access to information and application system functions should be restricted in accordance with the access control policy.	The following should be considered in order to support access restriction requirements: 1. providing menus to control access to application system functions; 2. controlling which data can be accessed by a particular user; 3. controlling the access rights of users, e.g. read, write, delete and execute 4. controlling the access rights of other applications; 5. limiting the information contained in outputs; 6. providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.	In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs.	In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing.	Jing yao	5: Removal or adjustment of access rights are done immediately upon request or employee's termination 4: Removal or adjustment of access rights are done within 24 hours upon request or employee's termination 3: Removal or adjustment of access rights are done within 48 hours upon request or employee's termination 2: Removal or adjustment of access rights are done within 72 hours upon request or employee's termination. 1: No removal or adjustment of access rights	5	3
A. 9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	A suitable authentication technique should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used. The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application	If passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network " sniffer" program.	Passwords are a common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user authentication should be appropriate for the classification of the information to be accessed.		5: Only a few selected individuals hold administrative priviledged access rights. Even so, they are unable to abuse this priviledge as all sensitive information are encrypted with one way functions, which makes it almost impossible to reverse. 4: Encryption is present but is reversible. 3: Some selected individuals hold priviledged access rights. No encryption is present. 2: Priviledged access control is held by too many people. 1: No priviledged access control is present.	5	3
A. 9.4.3	Password management system	Password management systems should be interactive and should ensure quality passwords.	A password management system should: 1. enforce the use of individual user IDs and passwords to maintain accountability; 2. allow users to select and change their own passwords and include a confirmation procedure to allow for input errors; 3. enforce a choice of quality passwords; 4. force users to change their passwords at the first log-on; 5. enforce regular password changes and as needed; 6.maintain a record of previously used passwords and prevent re-use; 7. not display passwords on the screen when being entered; 8. store password files separately from application system data; 9.store and transmit passwords in protected form.	Employees are accountable for the confidentiality and secrecy of their own secret authentication information	When employees are signing up for a new password, sufficient prompts are given to ensure the password is a strong one. System will only accept passwords that are strong, with a minimum of 8 characters, at least 1 uppercase, 1 lower case and 1 symbol. Under the terms and conditions, users are again reminded to practice responsible handling of their passwords		5: Password strength of users are enforced through the rejection of weak passwords and prompting users on the types of acceptable passwords. Terms and conditions clearly state the types of good practices when handling their passwords. 3: terms and conditions did not advise users on responsible handling of their passwords 1: Weak passwords are accepted. No prompts given.	5	3
A. 9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered: 1. use of identification, authentication and authorization procedures for utility programs; 2. segregation of utility programs from applications software; 3. limitation of the use of utility programs to the minimum practical number of trusted, authorized users 4. authorization for ad hoc use of utility programs; 5. limitation of the availability of utility programs, e.g. for the duration of an authorized change; 6.logging of all use of utility programs;	Most computer installations have one or more utility programs that might be capable of overriding system and application controls.	Similar to how OS has kernel mode and handler mode, priviledged and user access. Utility programs that are capable of overriding system and application controls must be identified and given only user access and handler modes. To prevent editting of major critical components.	Jing Yao	5: Utility programs that are able to override system and application controls are identified and are given user access and handler modes. 4: Some degree of control on these utility programs 3: Some utility programs are identified, but little is done to control them. 1: No inteference involved.	5	4
A. 9.4.5	Access control to program source code	Access to program source code should be restricted.	Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of	Source codes library are read and write only where anyone is able to read and edit it.	under the role based user access, only support personnel should have read and write access to source codes library.	Jingyao	5+B104:J117: Only a few support personnel hold administrative priviledged access rights to source codes library.	5	3
A.10	**Cryptography: to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integity of information**								
A.10.1	Cryptographic Controls								
A10.1.1	Policies development	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	1. No. of purposes covered 2. Clarity of the approach and principles 3. Whether risk assessment is used in level of protection determination 4. Key managements, rols and responsibilities identified.	1. The management approach and principles should be clearly defined and procted. 2. The report should help cryptographic controls to achieve confidentiality, integrity, non-repudiation and authentication. 3. Level of protection should be identified based on a risk assessment such as type, strength and quality of The encryption algorithm used. 4. Cleared defined approach to key managements, roles and responsibilities.	The policy regarding the use of cryptographic controls should be developed after thorough discussions with the professions and the expects and implementation should be frequently checked to make sure they align with the standards	Huang Peng	1. /4 2. /5 3. /1 4. /3	5	3
A10.1.2	Key Management	a policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	1. No. of lifecycle stages covered 2. Algorithms, key lengths identified according to best practice 3. Whether secret and private keys protected. 4. Whether equipment protected physically. 5. No. of processes covered in the standards	1. Policy should include requirements for managing keys through their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys. 2. Cryptographic algotirhms, key lengths and usage practices should be selected according to best practice. 3. Secret and private keys need protection. 4. Equipment used to generate and store keys should be physically protected. 5. Key management system should be developed according to the set of standards, procedures and secure methods for	The policy regarding the use, protection and lifetime of cryptographic keys should be developed within the management sectors and the respective professions.	Huang Peng	1. /7 2. /5: difficulty level used 3. /1 4. /1 5. /11	5	3

A.11	**Physical and Environmental Security**									**4**	**3**	**0.08**
A11.1	Secure Areas: to prevent unauthorized physical access, damage and interferences to the organization's information and information processing facilities.											
A11.1.1	Physical Security Perimeter	security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	1. Clarity of definition. 2. Assessment results into consideration 3. Physical strength of facilities 4. Presence of reception 5. Coverage of physical barriers 6. % of firedoors being alarmed, monitored and tested 7. Coverage of intrudence system 8. % of information processing facilities seperated	1. Clear definition of security parameters 2. Siting and strength of the parameter based on security requirementes of the asset and risk assessment results. 3. Information processing facilities should be physically sound. 4. Manned reception in place and access to buildings should be restricted. 5. Physical barriers should be built where applicable. 6. All firedoors should be alarmed, monitored and tested. 7. Suitable implementation of intruder detction systems to standards and regularly tested. 8. Seperation of information processing facilites managed by internal or external organizations.	The security parameters should be clearly defined based of different security requirements of asset and risk management results, after which proper inception, barriers, moniroting and alarming systems should be in place to fulfill the protection of the security parameters.	Huang Peng	1. /5 2. /1 3. /5 4. /1 5. /5 (100%, 80%, 60%, 40%, 20%) 6. /5 (100%, 80%, 60%, 40%, 20%) 7. /5 (100%, 80%, 60%, 40%, 20%) 8. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A11.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	1. Completeness of record 2. % of time authentication is done 3. % of time visitors under supervision 4. Clarity of purposes 5. % of time briefing is given according to standards 6. Coverage of access controls 7. % of time log book maintained 8. % of people wearing identifications 9. Frequency of review and update	1. Clear record of date and time of entry and departure of visitors. 2. Authenticated identification of visitors. 3. Continuous supervision of visitors. 4. Clear set of purposes allowed for visiting. 5. Clear briefing about security requirements and emergency procedures given to the visitors. 6. Areas of confidential information should implement appropriate access controls. 7. Security log book or electronic audit trail maintained all times. 8. Visible identification worn all time by emplotees, contractors and external parties. 9. Access rights to secure areas should be regularly reviewed and updated	Secure areas should have appropriate and up to date control measures. The process should start from the very beginning of the visitors entering into the facilties until the visitors completely leave the facilities. Appropriate access records and logs should also be maintained.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 5. /5 (100%, 80%, 60%, 40%, 20%) 6. /5 (100%, 80%, 60%, 40%, 20%) 7. /5 (100%, 80%, 60%, 40%, 20%) 8. /5 (100%, 80%, 60%, 40%, 20%) 9. /5 (Once half a month, once a month, once every three months, once every half-year, once every year)	5	4			
A11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be desiged and applied.	1. % of key facilities blocked access 2. % of buildings with signs 3. Amount of information available from outside 4. % of directories and phone books with restricted accessibility	1. Key facilities are sited to avoid access by the public. 2. Buildings should be unobtrusive and give minimum indication of their purpose. 3. Facilities configured to prevent information or activities from being visible and audible from outside. 4. Directories and internal telephone books should be restricted accessible.	Proper desige and selection of the locations of the offices, rooms and facilties should be carried out including all the peripheral facilities in these areas.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (0%, 20%, 40%, 60%, 80%) 3. /5 (0%, 20%, 40%, 60%, 80%) 4. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A11.1.4	Protecting against external and environmental threats	physical protection against natural disasters, malicious aattack or accidents should be designed and applied	1. No. of areas covered	1. Specialist advice should be obtained regularly covering multiple areas such as fire, flood, earthquake, explosion, civil unrest and other forms of disasters.	physical protection against natural disasters, malicious aattack or accidents should be designed and applied	Huang Peng	1. /5 (8, 6, 4, 2, 1)	5	4			
A11.1.5	Working in Secure Areas	Procedures for working in secure areas should be designed and applied.	1. % of time unsuperveised working is conducted 2. % of areas get locked 3. Confidentiality of the activities 4. No. Of times recording equipment is discovered in a month	1. Unsupervised working in secure ares should be avoided. 2. Vacant secure areas should be locked. 3. Activities in secure ares should only be known to person on a need-to-know basis. 4. Recording equipment should noe be allowed.	Procedures should be designed pertaining to the requirements, attentions to pay to, and monitoring of activities in the secure areas.	Huang Peng	1. /5 (0%, 20%, 40%, 60%, 80%) 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 4. /5 (0, 1, 2, 3, 4)	5	2			
A11.1.6	Delivery and loading areas	access points where unauthorized persons should enter should be controlled and if possible, isolated from information processing facilities to avoid unauthorized access.	1. % of times personnel are identified and authorized 2. Whether loading areas allowed delivery personnel gaining access 3. Whether design mechanism fulfills this requirement 4. % of times incoming materials are inspected 5. % of times shipments are physically segregated	1. Access to a delivery and loading area from outside should be restricted to identifies and authorized personnel 2. Area should be designed so that suppliers can be loaded without delivery personnel gaining access to other parts of the building 3. External doors should be closed when internal doors are opened 4. Incoming materials should be inspected and examined. 5. Incoming and outgoing shipments should be physically segregated.	Access policies should be established and successfully carried out regarding the incoming and outgoing materials transactions.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /2 3. /2 4. /5 (100%, 80%, 60%, 40%, 20%) 5. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A11.2	Equipment: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations											
A11.2.1	Equipment siting and protection	equipment should be sited and protected to reduce the risks from environment threats and hazards, and opportunities for unauthorized access.	1. % of facilities that are positioned this way 2. Whether storage securities are secured or not 3. % of time that environmental conditions are monitored 4. % of special protection adopted when required 5. % of equipment processing confidential information that are protected from electromagnetic emanation	1. Information processing facilites should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use. 2. Storage securities should be secured to avoidd unauthorized access 3. Environmental conditions should be monitored continuously 4. Use of special protection methods should be considered if necessary 5. Equipment processing confidential information should be protected from electromagnetic emanation	Proper equipment usage, storage policies should be established based on the environmental conditions and their importance.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /2 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 (100%, 80%, 60%, 40%, 20%) 5. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
A11.2.2	Supporting Utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities	1.% of specifications and requirements that are conformed 2. Frequency of appraisal 3. Frequency of inspection and testing	1. Conform to equipment manufacturer's specification and local legal requirements 2. appraised regularly for capacities to meet business growth 3. Inspected and tested regularly to ensure proper functioning	Equipement protection from electricity issues should be identified and carried out.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (half a month, one month, 2 months, 3 months, half a year) 3. /5 (half a month, one month, 2 months, 3 months, half a year)	5	3			
A11.2.3	Cabin Security	power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage	1. % of lines that are underground 2. % of area that power cables are segregated from communication cables 3. % of additional protective controls adopted in critical systems	1. Power and telecommunication lines should be underground. 2. Power cables should be segregated from communication cables. 3. For sensitive or critical systems additional protective controls should be adopted.	Protection from interception, interference or damage should be implemented on the power and telecommunication cables.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A11.2.4	Equipment maintenance	equipment should be correctly maintained to ensure its continued availability and integrity.	1. % of maintenances that are in line with recommended intervals and specifications 2. Correctness of the records 3. % of maintenance requirements that are complied with 4. % of times that inspection are done	1. Equipment maintenance should be in accordance with recommended service intervals and specifications 2. Records should be kept of all suspected or actual faults 3. Maintenance requirements imposed by insurance policies should be complied with 4. Inspection should be done before putting equipment back into operation after maintenance	Make sure there is a maintenance schedule according to the requirements and the specifications.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
A11.2.5	Removal of assets	equipment, information or software should not be taken-off-site without prior authorization	1. % of completeness of the records 2. % of cases that time limits are set and verified 3. % of completeness of the removal histories	1. Employees and users permitting off-site removal of assets should be recorded and identified 2. Time limites for asset removal should be set and returns verified for compiance 3. Removal histories should be complete, together with the	Make sure that off-site equipments are properly recorded and policies should take care of such activities.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
A11.2.6	Security of Equipment and assets off-premises	security should be applied to off-site assets taking into account the different risks fo working outside the organization's premises	1. % of premises that are attended to 2. % of completeness of the log	1. equipment and media taken off premises should always be attended to according to the instructions 2. Log should be maintained for the assets off-premises	Off-sites assets should always be attained to.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media should be verifield to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	1. % of times that verification is done 2. % of times that storage media is physically destroyed as required	1. Verify equipment to ensure storage media is not contained 2. Physically destroy storage media containing confidential or copyrighted information	Equipments with storage information should be dealt with according to the policies requirements.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A11.2.8	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection	1. % of times that active sessions are left as they are 2. % of times that log off is performed 3. % of computers that have a key lock	1. Terminate active sessions when finished (unless secured by locking mechanism). 2. Log-off from applications or betwork services when no longer needed. 3. Secure computers by a key lock.	Unattended equipment should always have protection.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
A11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	1. % o sensitive information that is locked away 2. % of time that computers and terminals are logged off 3. % of time photocopiers are authorized use 4. No. Of times media is discovered left on the printers in the week	1. Sensitive information should be locked away. 2. Computers and terminals should be logged off or protected when not in use. 3. Photocopiers and reproduction technologies by authorised use only. 4. Media should be removed from printers immediately	Papers and removable storage should be properly taken care of.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 1. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 (0, 1, 2, 3, 4)	5	3			

A12	**Operations security**									**4**	**2**	**0.06**
A12.1	Operational procedures and responsibilities: to ensure correct and secure operations of information processing facilities											
A12.1.1	Documented operating procedures	operating procedures should be documented and made available to all users who need them	1. Clarity and scope of the documented procedures	1. Clear and comprehensive docuented procedures for operational activities.	operating procedures should be documented and made available to all users who need them	Huang Peng	1. /5	5	2			
A12.1.2	Change management	changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled	1. Completeness of the recordings 2. No. Of fields identified	1. comprehensive recordings of significant changes 2. identify planning, testing, assessment, fall-back options, emergence processes, involved parties and approval for proposed changes	Comprehensive recordings should be made available to the operational procedures and responsibilities changes.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /7	5	3			
A12.1.3	Capacity Mangement	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required sstem performance	1. Frequency of changes for capacities requirements and clarity of the definition 2. % of times that detective controls work to indicate problems 3. % of times that procedures get monitored 4. Activeness of the capacity management (frequency of monitoring)	1. Capacities requirements should be clearly identifies and changed at a regular interval taking into considerations of new businesses and system requirements. 2. Detective controls in place to indicate problems in due time. 3. Procedures with long procurement lead times should be monitored and actions should be taken to avoid potential bottlenecks. 4. Active sufficient capacity management.	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required sstem performance	Huang Peng	1. /5 (half a month, one month, 2 months, 3 months, half a year) 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 (Once a week, half a month, one month, 3 months, half a year)	5	2			
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment	1. Clarity of the rules 2. No. Of systems and user profiles tested 3. No. Of times the development gets tested	1. Rules should be clearly identified. 2. Development should be tested on different systems and different user profiles multiple times before delopyment	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment	Huang Peng	1. /5 2. /5 (5, 4, 3, 2, 1) 3. /5 (5, 4, 3, 2, 1)	5	2			
A12.2	Protection from malware: to ensure that information and information processing facilities are protected against malware											
A12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	1. Clarity of the prolicies 2. % of users the controls covered 3. Whether there are formal policies 4. How detailed are the plans (no. of ways considered) 5. Frequency of updates 6. % of environments that get isolated	1. Clear policies in prohibiting the use of unauthorized software. 2. Controls prevent and detect use of unauthorized software, suspected malicious websites. 3. Formal policies against risks and vulnerabilitis from malware 4. Detailed plans for recovery from malware attackes 5. Installation and regular updates of malware detection and repair software	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Huang Peng	1. /5 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /2 4. /5 (5, 4, 3, 2, 1) 5. /5 (a week, 2 weeks, one month, 2 months, 3 months) 6. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
A12.3	Backup: to protect against loss of data											
A12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	1. Clarity of the policies 2. % of information that can be recovered from backup facilities 3. Completeness of the records 4. Distance of backups from main facilities 5. % of physical and software protection that align with the needs	1. Clear policy should be defined. 2. Adequate backup facilities should be provided to ensure all essential information can be recovered. 3. Accurate and complete records should be recorded. 4. Backups should be at a distant location to escape from damages. 5. Appropriate level of physical and software protection should be given.	Clear policies should be defined after which records should be maintained regarding any issues with the data.	Huang Peng	1. /5 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 5. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A12.4	Logging and monitoring: To record events and generate evidence											
12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	1. % of data included out of all the fields necessary for automated moniroting systems 2. Frequency of review	1. Include all necessary fields available for automated monitoring systems and reviewed regularly.	Necessary fields should be included to the standards for automated monitoring systems.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (half a month, one month, 2 months, 3 months, half a year)	5	3			
12.4.2	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	1. % of controls set to prevent changes to information	1. Controls set to prevent unauthorized changes to log information	Unauthorized changes to log information should be properly taken care of.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
12.4.3	Administrator and operator logs	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	1. % of completeness of the logs 2. % of events that are traceable to the privileged users	1. Protect and review the logs to maintain accountability for the privileged users.	Logs should provide necessary information to track events to privileged users.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	1. % of completeness of documentation 2. Whether approach is documented 3. % of time that the approach is implemented	1. External and international requirements for time representation, snchronisation and accuracy should be documented. 2. Approach to obtain referenced time and cynchronise internal clocks should be documented and implemented.	Requirements should be properly documented.	Huang Peng	1. /5 (100%, 80%, 60%, 40%, 20%) 2. /2 3. /5 (100%, 80%, 60%, 40%, 20%)	5	4			
A12.5	Control of operational software: to ensure the integrity of operational systems											
A12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.	1. Clearness of the guidelines 2. % of old versions that are archived together	1. Clear guidelines being developed about installation, updating, configuration, rollback strategy of software. 2. Old versions of software should be archived rogther with configurations.	Policies should take care of installation of the software.	Huang Peng	1. /5 2. /5 (100%, 80%, 60%, 40%, 20%)	5	2			
A12.6									3			
A12.6.1	Management of technical vulnerabilityes	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	1. Whether rols and responsibilities are identified 2. Frequency of store and update 3. The lag time between identification and remedy 4. % of time the risk monitors is running	1. Clear roles, responsibilities identified with technical vulnerability management. 2. Information resources should be stored and updated frequently. 3. On identification of technical vulnerability, actions and risks should be identified quickly with analysis of remedy actions. 4. Risk monitoring runs continuously and priorities are identified.	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Huang Peng	1. /5 2. /5 (one week, 2 weeks, one month, 2 months, 3 months) 3. /5 (2 hours, 6 hours, half a day, one day, two days) 4. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A12.6.2	Restrictions on software installation		1. Whether the policies are specified 2. % of time the policies are followed	1. The organization should define and enforce strict policy on which types of software users may install.	Rules governing the installation of software by users should be established and implemented.	Huang Peng	1. /5 2. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A12.7	Information systems audit considerations: to minimise the impact of audit activities on operational systems											
A12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.	1. Whether requirements and scope are identified 2. Whether special and additional processing are identified 3. % of audit tests that only have read-only access	1. Agreed audit requirements and scope of technical tests 2. Special and additional processing should be identified and agreed 3. Audit tests should only have read-only access.	Audit activities should be properly carried out to minimize their influence on the daily operations.	Huang Peng	1. /2 2. /2 3. /5 (100%, 80%, 60%, 40%, 20%)	5	3			

A.13	**Communications security**									**4**	**2**	**0.12**
A13.1	Network security management: to ensure the protection of information in networks and its supporting information processing facilities											
A13.1.1	Network controls	Networks should be managed and controlled to protect information insystems and applications	1. Whether responsibilities and procedures are established 2.No of times data passing over public networks got trouble 3. % of times logging are recorded 4. % of duration monitoring is carried out 5. % of restricted connections are adopted	1. Clearly established responsibilities and procedures 2. Special considerations for data passing over public networks 3. Appropriate logging and monitoring 4. Restricted connections to the networks if appropriate	Networks should be properly defined and taken care off to protect information.	Huang Peng	1. /2 2. /5 (0%, 10%, 15%, 20%, 30%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 (100%, 80%, 60%, 40%, 20%) 5. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	1. Whether abilities and rights are agreed	1. Abilities to managed agreed services clearly defined, and the right to audit should be agreed.	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Huang Peng	1. /2	5	3			
A13.1.3	Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	1. Whether network domains are clearly defined 2. % of perimeters well defined 3. % of times communications are controlled 4. No. of technics used in wireless networks segregation	1. Separate network domains clearly defined based on trust levels, organizational units or combinations of both. 2. Perimeter of each domain should be well defined and communications controlled. 3. Wireless networks segregated seperately with proper authenticatoin, encryption and user level network access control technologies.	Groups of information services, users and information systems should be segregated on networks.	Huang Peng	1. /2 2. /5 (100%, 80%, 60%, 40%, 20%) 3. /5 (100%, 80%, 60%, 40%, 20%) 4. /5 (5, 4, 3, 2, 1)	5	3			
A13.2	Information transfer: To maintain the security of information transferred within an organization and with any external entity.											
A13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.	1. No. of areas the procedures targeted at 2. % of facilities covered under the policies	1. Procedures clearly desinged to reduce interception, copying, modification mis-routing and destruction. 2. Policies outlining acceptable use of communication facilities. 3. Good adversing personnel about problems of usage facsimile machines or services.	Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.	Huang Peng	1. /5 2. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A13.2.2	Agreements on information transfer	Agreements should address the secure transfer of business information between the organization and external parties.	1. No of areas covered in the agreements 2. Whether minimum technical standards are defined 3. % of responsibilities and liabilities defined out of all the possible security incidents	1. Agreements clearly defined for controlling and notiying transmission, dispatch and receipt to ensure traceability and non-repudiation. 2. Minimum technical standards and courier identification standards clearly defined. 3. Responsibilities and liabilities defined in the event of	Agreements should address the secure transfer of business information between the organization and external parties.	Huang Peng	1. /3 2. /1 3. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A13.2.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected.	1. Happenings of the unwanted incidents in a week 2. % of correct addressing and transportation of message 3. % of times service are available	1. Protecting messages from unauthorized access, modification and denial of services. 2. Correct addressing and transportation of message. Reliability and availability of the service.	Information involved in electronic messaging should be appropriately protected.	Huang Peng	1. /5 (0, 1, 2, 3, 4) 2. /5 (100%, 80%, 60%, 40%, 20%)	5	3			
A13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization 's needs for the protection of information should be identified, regularly reviewed and documented.	1. No of areas covered in the agreement	1. Agreement clearly identify inforation to be protected, duration, actions of termination, responsibilities, ownership of different information, permitted use of confidential information, right to audit and monitor activities, process for notification and reporting, actions in case of breach.	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.	Huang Peng	1. /9	5	4			
A.14	**System acquisition, development and maintenance**									**4**	**2**	**0.076923077**
A.14.1	Security requirements of information systems Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.											
A.14.1.1	Information security requirements analysis and specification	The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.	- Information security requirements are considered in information systems. - Guidances on security evaluations and use of risk management processes to identify controls to meet information security requirements. - Formal testing and acquisition process for acquired information systems/ products.	- The information security requirements for new information systems need to be defined, documented and reviewed by all stakeholders. - Formal acquisition, testing and assurance processes need to be performed prior to acquiring the information systems/products. - Organization needs to define the information security criteria for accepting third-party information systems.	- Consideration of information security requirements in design phase for new information systems or enhancements to existing information systems. - Identified information security requirements using threat modelling, incident reviews, use of vulnerability thresholds or deriving compliance requirements from standard policies and regulations, are reviewed by all stakeholders. - Prior to information system/ product acquisition, formal evaluation and testing on the provided information security controls against the identified information security criteria. Intensive functional testing shall be conducted to ensure the acquiring information system does not introduce unacceptable risks.	Jit Seah	5 : Business Impact Analysis (BIA) and Risk Assessment (RA) are performed if identified information security requirements cannot be readily satisfied. 4 : For unsatisfied information security requirements, the associated risks and interim controls should be carefully evaluated and documented. 3 : Ensure formal acquisition, testing and assurance processes are followed for acquired information systems. 2 : Information security requirements analysis is performed and the identified security requirements are documented and reviewed by all the stakeholders. 1 : No information security requirements are included in the requirements for information systems.	3	3			
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	- Defined service agreements between partners receiving and sending the application data. - Protection of transactions or data transfers over public networks. - Considerations of liability costs associated with fraudulent transactions by both parties.	- Identify security goals for securing the transmitted assets and agreed among both parties. - Mechanisms and information security controls (eg. cryptographic controls) used to protect application services over public network. - Associated risks and liability costs for failure of protection by the implemented information security controls.	- Application service agreements are sign-off by both sending and receiving parties in meeting the defined security goals for protecting the transmitted assets. Also providing information security controls to protect application servers against attacks (eg. DDoS). - The application of cryptographic controls have taken into account compliance with legal requirements. - Business Impact Analysis (BIA) and Risk Assessment (RA) are performed to identify liability costs associated with any fraudulent transactions.	Jit Seah	5 : Application service agreements that commits both parties to agreed terms of securing data transfer and having resilience requirements against attacks (eg. include application server protections and ensuring network availability at all times). 4 : Both sending and receiving parties uses strong authentication methods (eg. Asymmetric 512-bit cryptography with digital signatures, Trust third party Public Key Infrastructure) to fulfil the security goals (ie. Confidentiality , Integrity, Authenticity, Authorization and Non-repudiation). 3 : Using 2-factor authentication with basic cryptography methods for authentication and securing data transfer. 2 : Using compression algorithms with password for application service transactions over public networks. 1 : No protection methods are available for application services passing over public networks.	5	3			
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	- Ability to secure the application services transactions to avoid tampering of the transmitted data. - Clear separations between private and public access. - Availability of Trusted Computing Module, Tampered Resistance hardware and air-gap segregation of storage medium.	- Using appropriate cryptographic controls to secure application service transactions so as to maintain confidentiality, integrity, availability, non-repudiation and authenticity. - Separation of the storage medium in De-Militarized Zone (DMZ) and preventing public access.	- The storage of the transaction details resides in De-Militarized Zone (DMZ) and air-gapped whereby it is inaccessible from public networks. - Both parties implemented the challenge response protocols to prevent reply attacks (eg. Man-In-The-Middle attack). - All application services transactions are encrypted using RSA (2048 bits or higher) with SHA-512 (or higher).	Jit Seah	5 : Define process, procedures and implementations in securing application services transactions with the relevant security controls that commensurate with the level of associated risks. 4 : Implementation of trusted computing module, tamper resistant hardware and air-gap segregation to accomplished organization transaction security goals. The storage medium of application transaction details are inaccessible from Internet. 3 : Trusted third party security certificates used to secure the application service transactions are integrated and embedded throughout the entire end-to-end certificate/signature management process. 2 : Securing application services transactions in compliance with legal and regulatory requirements. 1 : No protection for application services transactions.	4	3			

A.14.2	Security in development and support processes Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.											
A.14.2.1	Secure development policy	Rules for the development of software and systems should be established and applied to developments within the organization.	- Secure development policy is implemented in the software development lifecycle. - Code inspection to ensure compliance with the rules of secure development. - Developer capability of avoiding, finding and fixing vulnerabilities.	- Ensure secure development policy is followed in the software development process and secure programming is consistent with the current best practices. - Code reviews and testing procedures with respect to secure programming are to be exercised for both in-house developed and re-use/open-sourced codes. - Outsourced development shall comply with the rules of secure development defined in the supplier development policy.	- Secure development policies are followed by trained developers in secure programming techniques within the entire software development lifecycle. - Code reviews and testing of the implemented security controls both for new development codes and re-use codes (ie. open-sourced). - For outsourced development, the organization shall obtain assurance that the third-party codes complies with the rules of secure development and appropriate legal regulations.	Jit Seah	5 : Software development policies and processes incorporate the secure programming techniques for both new developments and code re-use cases (especially for open-source codes). - 4 : Security checkpoints are defined within the project milestones, secure repositories, security in the version control and peer-to-peer review to ensure the necessary security controls are well implemented. - 3 : Provide coding guidelines for implementing security requirements within the software development cycle. - 2 : Establish a secure development environment. - 1 : There is no secure development policy.	5	3			
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	- Systems change control processes and procedures are well defined. - Discretionary access control with least privilege principles are implemented. - Version control, quality control, unit/system/integration testings before implementing system changes to ensure existing security and control procedures are not compromised. - Systems downtime required for changes/upgrades/patches are not affecting normal businesses.	- Users/owners of the systems/applications are required to place requests/updates via the organization's Change Request process. - Maintain restricted access on system modification with discretionary access given only to the responsible support engineers/programmers. - Ensure that existing security and control procedures are not compromised by introducing the new changes to the information systems. - Normal business should not be disturbed with the implementation of system changes/updates.	- Systems requests/changes are submitted only by authorized owners and formal approvals on detailed proposals are required before system changes/implementations are made. - Discretionary access control with least privilege provided to the support engineers/programmers for access to only those parts of information systems necessary for their work. - Vigorous testing of the new software updates/changes needs to be carried out outside the development and operation environments. Operating documents and user procedures are updated with respect to the new changes. - Implementation of changes should takes place during planned system maintenance period so that the normal business is not disturbed.	Jit Seah	5 : Change control process should include Business Impact Analysis(BIA) and Risk Assessment (RA) for changes on the specifications of security controls. - 4 : Appointed technical team to assess the software components/database entities/hardware that require amendments with respect to the change requests. Security impacts need to be observed for the identified changes. - 3 : Formal change control procedures are documented and enforced (with audit trails) to ensure integrity of new information systems and major changes to existing systems. - 2 : Change request and approval processes are defined together with the appropriate authorization levels (ie. who should make requests, approve, develop, test and implement). - 1 : No formal change control procedures for managing changes to information systems.	3	2			
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	- Technical reviews are conducted after operating platform changes. - Business critical applications are reviewed and tested to ensure integrity is maintained.	- Technical reviews and testings are imposed to ensure that application controls and integrity procedures are not compromised by the operating platform changes. - No adverse impacts on organizational operations or security after operating platform changes.	- After changes in operating platforms, technical team with the right information security skills must review and evaluate to ensure that the security controls remains intact and no new security risks are introduced. - Corresponding updates in the Business Continuity Plan might be needed. - If adverse impacts on organizational operations or security are created after operating platform changes, escalation must be made immediately to all stakeholders with the appropriate risk mitigations. Potentially, systems roll back with reference to Business Continuity Plan (BCP) will be required.	Jit Seah	5 : Risk Assessment (RA) with corresponding risk mitigations have to be made for application changes in End-Of-Support (EOS) platforms during the interim period. - 4 : Competent technical team to evaluate the applications are in compliance with regulations after operating platform changes. Corresponding changes may also be required in the Business Continuity Plan (BCP). - 3 : Review and test the application security controls and integrity procedures to ensure that they have not been compromised by the operating platform changes. - 2 : Identify the business critical applications and verify that the changes do not cause adverse impacts on organizational operations or security. - 1 : No technical review of applications after operating platform changes.	4	2			
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	- Obtain consent from software vendor prior to making modifications to prevent void of software warranty. - Using software update management process for strict controls on modifications to software packages.	- Based on fulfilling the business and regulatory requirements, modifications on the commercial-off-the-shelf (COTS) or open-sourced license codes are required. - Ensure the built-in controls and integrity processes are not compromised with the functionality changes.	- At all possible times, attempt to engage the vendors to make the modifications to fulfil business objectives and compliance to regulations. - Detailed studies on necessary modifications (eg. encryption methods) of vendor-supplied software and commercial-off-the-shelf (COTS) packages to meet security requirements in compliance of policies, jurisdictions and regulations. - As last resort to make the necessary modifications on software packages, the software update management process need to strictly adhere to. - Vigorous testing to ensure that no new vulnerabilities are introduced and avoid the risk of the built-in controls and integrity processes are being compromised with these new changes.	Jit Seah	5 : Modifications of software packages shall be tested and validated by an independent evaluation body after obtaining consent from the vendor. - 4 : All changes to software packages must be fully tested against the security controls/policies/procedures, ensure compatibility with other software in use and properly documented. - 3 : Implement a software update management process to ensure approved patches and application updates are installed for only authorized software. - 2 : If changes are necessary, the original software packages should be retained and the changes are applied only to the designated copy. - 1 : No restrictions on changes to software packages.	4	2			
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	- Secure information system engineering procedures are established, documented and implemented. - Regular review of the established information system engineering procedures to ensure that they remain relevant. - Supplier's security engineering principles are rigour and comparable with its own.	- Ensure relevancy of secure system engineering principles and procedures. - System security is designed and established in all system architecture layers (business, data, applications and technologies). - The application of secure system engineering procedures to developed and outsourced information systems.	- The established secure system engineering principles and procedures are reviewed regularly (at least once a year or whenever there are major incidents) to ensure that they remain applicable and able to combat new potential threats. - Defense-in-depth strategy is used in the secure system engineering procedures. - Secure information system engineering procedures are applied to both in-house information system engineering activities and outsource information systems.	Jit Seah	5 : New technologies shall be analysed for security risks and system design reviewed to ensure its effectiveness and enhancement of security standards within the engineering process. - 4 : The secure system engineering principles and procedures are reviewed regularly to ensure that they remain effective and relevant. - 3 : Established security engineering principles are applied to outsourced information systems through contracts and agreements between the organization and the supplier. - 2 : Secure information system engineering procedures are established and documented. - 1 : No secure system engineering principles are established.	4	3			
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	- Secure development environment that includes people, processes and technology for system development and integration. - Segregation between different development environments. - Control over movement of data from and to the environment.	- Assess risk associated with individual system development efforts. - Establish secure development environments for sensitivity of data to be processed, stored and transmitted by the system. - Determine the level of protections and segregate different development environments.	- Assess and determine the risks involved in the data processing, storage and transferring of data. - Define the level of necessary protection and document the corresponding processes and procedures to secure the respective development environments and make them available to the individuals that require them. - Using discretionary access controls to provide data confidentiality and integrity for different development environments.	Jit Seah	5 : Define processes and procedures for securing the development environments at the predetermined levels of protection. - 4 : Determine the system development and integration efforts in the system development cycle to secure the development environments. - 3 : Identify the risk associated with each of the system development environments. - 2 : Identify the people, processes and technology associated with system development and integration. - 1 : No processes and procedures for secure development environment.	5	3			
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	- Define processes and procedures to ensure secure and quality deliverables. - Contractual supplier agreements with liabilities for the essential compliance with applicable laws and regulations. - Rights to audit supplier's development environment.	- Organization outsourced development processes and procedures are used to supervise and monitor the activities and deliverables of the suppliers. - Abiding to the applicable laws and regulations are of foremost importance to avoid non-compliance liabilities. - Organization shall perform regular audits on the outsourced system development.	- Organization requires the suppliers to deliver secure and quality systems in accordance to the agreed system development processes and procedures as well as the acceptance criteria (eg. security thresholds defined with no presence of malicious codes and known vulnerabilities). - All forms of outsourced system development shall strictly be legal and acceptable by the relevant jurisdictions. - Organization shall conduct an annual audit reviews on the supplier's system development processes, procedures, quality controls on deliverables as stipulated in the supplier relationship agreements. Only upon passing the audit will subsequent outsourcing contract be renewed.	Jit Seah	5 : Organization has to contractual right to audit supplier's development environment, processes and controls. Back-to-back compliance with applicable laws and control efficiency verifications are clearly defined in the supplier contractual liability agreements (reference ISO/IEC 27036). - 4 : Define unambiguous acceptance testing (against malicious contents and presence of known vulnerabilities) for the quality and accuracy of the secure deliverables. - 3 : Provision of evidences that security controls and thresholds are used to ensure minimum acceptable levels of security and privacy quality. - 2 : Contractual requirements for secure design, code and testing practices in the supplier relationship agreements. - 1 : No processes and procedures for supervising the outsourced system development.	5	3			
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	- Testing of security functionality is carried out by development and unit/system test teams during development lifecycle. - Independent acceptance testing of system security functionality is being performed.	- New and updated systems require thorough security functionality testings during the development lifecycle. - Both in-house and outsourced information systems need to be verified and ensured that the systems work as expected and only as expected.	- Detailed schedule of security testing activities are planned, documented and conducted by both the development and test teams independently during development lifecycle. - The extend of testings will be proportional to the important and nature of the information systems. - Independent acceptance testings for both in-house and outsourced information systems are carried out to ensure that the systems work as expected and only as expected prior to deployment.	Jit Seah	5 : All in-house or outsourced information systems development need to undergo thorough security testing and verifications prior to deployment (especially for mission critical systems). - 4 : Detailed schedule/conditions/test cases of security testing activities by both development and test teams are documented. The extend of testing will be commensurate with the important and nature of the information system. - 3 : Independent acceptance testing on the security functionalities of the information systems is undertaken to ensure the system works as expected and only as expected. - 2 : Basic security functionality testings are performed by development teams. - 1 : No testing of security functionality during development.	5	3			
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	- Documented testing procedures and acceptance criteria for new information systems, upgrades and new versions. - System acceptance testing include testing on identified information security requirements and adherence to secure system development procedures.	- Identify the system acceptance criteria for new information systems. - Perform thorough testing and verifications that the test systems meet the information security requirements (ie. without known defects or vulnerabilities). - Adherence to secure system development procedures in system acceptance testing .	- Document, review and sign-off the identified system test criteria (including the information security requirements) by the development and test teams. - Reliable system acceptance testing to satisfy the systems test criteria/information security requirements and strict adherence to the secure system development practices. - System acceptance testings are performed in a realistic test environment and to ensure that the test systems do not introduce vulnerabilities to the organization's development and production environments.	Jit Seah	5 : Organization leverage on automated tools (ie. code analysis tools, vulnerability scanners) for system testing and verifying the remediation of security-related defects. - 4 : System acceptance testing on the information security requirements based on the acceptance criteria and adhere to the secure system development practices/processes. - 3 : Perform system acceptance testing on received hardware/software components and integrated systems. - 2 : Establish the acceptance testing criteria for new information systems, upgrades and new versions. - 1 : No system acceptance testing on information security requirements.	4	3			

A.14.3	Test data[illegible]Objective: To ensure the protection of data used for testing.											
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	- Access control procedures are applied in test environment.[illegible] Data protection in accordance to the privacy laws and related regulations.	- Strict adherence to the data privacy policy for the protection of operational data.[illegible] Systematic control and usage of operational data from creation to destruction in the test environment.	- Formal data protection and privacy policies are defined for the protection and usage of operational data in accordance to the relevant regulations and jurisdictions.[illegible] Obfuscation of the Personally Identifiable Information (PII) in the operational data must be carried out in accordance to the related policies prior to its use in information systems testing.[illegible] Formal information systems testing procedures are strictly followed from the creation of test data with operational data, removal of sensitive contents, data processing/transfer and destruction of the data in the test environment. All performed testing activities are logged for traceability and future audit purposes.	Jit Seah	5 : Access controls procedures used in development and operational application systems are also applicable to test application systems. Authorized transfer and use of operational data are logged accordingly. Operational information is erased from test environment after testing is complete.[illegible]4 : Protection of user privacy should be strictly adhered to related process/procedures during the information system testings.[illegible]3 : Formal process or policy for the use of test data are defined with legal for the data protection in accordance to the privacy laws and related regulations (eg. PDPA, GDPR).[illegible]2 : Personally Identifiable Information (PII) or confidential information should have the sensitive details and contents removed or modified (reference to ISO/IEC 29101) before using them in testing.[illegible]1 : No process is available for the protection of test data.	4	3			
A.15	**Supplier relationships**									**4**	**3**	**0.2**
A.15.1	Information security in supplier relationships [illegible]Objective: To ensure protection of the organization's assets that is accessible by suppliers.											
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	- Organization policies, processes and procedures that will require the supplier to implement appropriate security controls for the information access.[illegible] Awareness training program for personnel in handling the supplier relationships.[illegible] Agreed documentations between the organization and supplier to meet the information security goals and mitigate the risks associated with the supplier's access to the organization's assets.	- The organization information security goals must be maintained and associate risk mitigated when supplier access to the organization assets.[illegible] Organization personnel handling the supplier relationships should be trained on handling acquisitions, incidents and contingencies.[illegible] Both the organization and supplier agreed with the defined policies, processes and procedures to implement the necessary security controls on both sides.	- Organization provide processes and procedures that will require the supplier to implement accurate and completeness controls to ensure the data confidentiality, integrity and availability of the information access.[illegible] Organization use the applicable policies, processes and procedures to train personnel in handling acquisitions, incidents and contingencies.[illegible] Defined policies, processes, procedures are adhered to sure the information security is maintained throughout the transition period between both the organization and supplier information processing facilities.	Jit Seah	5 : A supplier relationship agreement stating the information security requirements, processes and controls to be signed by both the organization and supplier.[illegible]4 : Awareness training for the organization's personnel involved in acquisitions, handling incidents and contingencies associated with supplier access.[illegible]3 : Identify the standardised process and lifecycles for managing supplier relationships that require the supplier to implement the security controls in order to allow to access its information.[illegible]2 : Identify and mandate information security controls in the organization supplier management policy to address supplier access to organization's information.[illegible]1 : No information security policy for supplier relationships.	4	3			
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	- Established agreements on the fulfilment of information security responsibilities between the organization and supplier.[illegible] Joint efforts for both the organization and supplier in protecting the accessed information, incident management and contingencies.[illegible] Periodic independent report from supplier to the organization on the effectiveness of its security controls and timely responses to reported issues.	- Both the organization and supplier must establish agreements to ensure that there is no misunderstanding on both parties' obligations to fulfil relevant information security requirements.[illegible] Establish the rules of acceptable and unacceptable use of information between the organization and supplier together with the respective implementation of information security controls.[illegible] Annual reporting from the the supplier to the organization on its fulfilment of data protection in terms of its effectiveness and efficiencies in implementing the required information security controls.	- Organization needs to explicitly defined the information security requirements (eg. information classification, access controls, reviews, audits, sub-contracting) for the information access (ie. processing, in transit, storage and disposal) in the supplier agreement.[illegible] Organization needs to use the agreed policies, processes and procedures to work with suppliers in incident remediation and contingencies.[illegible] Supplier is obliged to periodically (at least annually) provide an independent report on the effectiveness of its security controls and agreement on timely correction of relevant issues raised by organization.	Jit Seah	5 : Explicit information security policies, processes and procedures are addressed in the supplier agreements including legal and regulatory requirements (eg data protection, intellectual property rights, copyrights).[illegible]4 : Implementation of information security controls for incident management, remediation and contingencies are addressed in the supplier agreement.[illegible]3 : Descriptions of accessed information and methods of accessing the organization's information (ie. acceptable and unacceptable use of information).[illegible]2 : Classifications of information according to the organization's classification scheme and also its mapping with the classification scheme of the supplier.[illegible]1 : Information security is not addressed in supplier agreements.	4	2			
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	- Supplier agreement shall include appropriate information security controls in handling of risks associated with information and communication technology services and product supply chain.[illegible] Assurance that critical components/products with only needed features and their origins can be traced throughout the supply chain.[illegible] Implementation of specific processes for managing information and communication technology component lifecycle and its availability together with the associated security risks.	- Agreements with suppliers shall include the implementation of monitoring process and acceptable controls for validating the delivered information and communication technology products and services adhere to the organization's information security requirements.[illegible] The top tier supplier responsibilities to implement the appropriate information security controls to address associated security risks are propagated throughout the supply chain.[illegible] The assurance for identifying the critical supplied components in the information and communication technology supply chain.	- The suppliers/subcontractors must strictly adhere to the supplier agreements on the implementations and validations of the security controls for the delivered information and communication products and/or services.[illegible] The organization supplier agreement on the information and communication technology products and/or services requires the suppliers to propagate the organization's information security requirements throughout the supply chain for suppliers that subcontract parts of information and communication technology product and/or services provided to the organization.[illegible] The organization supplier management process incorporates the need to identify the critical supplied technology or service components and assure that these critical components with the maintained functionalities are traceable throughout the supply chain.	Jit Seah	5 : Explicit supplier responsibilities (including subcontractors with appropriate back-to-back agreements) on associated security risks on information and communication technology supply chain are documented in supplier agreements.[illegible]4 : Specific processes for managing information and communication technology component lifecycle and availability with the associated security risks (eg. End of Support).[illegible]3 : Traceability of the origins of suppliers' information and communications technology products/services in the product supply chain.[illegible]2 : Defining information security requirements to apply to information and communication technology product or service acquisition in supplier agreements (including cloud computing services).[illegible]1 : No security requirements on information and communication technology supply chain.	3	2			
A.15.2	Supplier service delivery management[illegible]Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.											
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	- Monitoring and review of supplier services to ensure that the information security terms and conditions are adhered as per agreements.[illegible] Service performance levels should be maintained as per supplier service agreements.	- Monitoring and review of supplier services to verify adherence to the supplier service agreements so that security incidents and problems are managed properly.[illegible] Proper management of information security incidents at agreed service continuity levels following major service failures or disasters.[illegible] Conduct regular reviews on information security aspects of the suppliers' service delivery with the abilities to resolve and manage any identified problems.	- The responsibility for managing supplier relationships should be assigned to a service management individual or team to review compliance with the supplier service agreements.[illegible] A service management relationship process between the organization and the supplier to review information security controls and ensure that the supplier maintains appropriate service capability with workable plans designed for agreed service levels are maintained during service disruptions.[illegible] The service management team shall review the supplier audit trails and records of information security incidents, operational problems, failures, tracing of faults and disruptions related to the service delivered.	Jit Seah	5 : Well-defined reporting process for organization to retain overall control and visibility into all security activities managed by supplier (ie. change management, vulnerabilities identifications, information security incident reporting and response).[illegible]4 : Obtain information about information security incidents and review this information (ie. audit trails, operational problems, failures, faults and service disruptions) as documented in the supplier service agreements, procedures and other supporting guidelines.[illegible]3 : Conduct annual audits of suppliers in conjunction with review of independent auditor's reports and follow-up on identified issues.[illegible]2 : A service management relationship process between the organization and the supplier to monitor service performance levels to verify adherence to the supplier service agreements.[illegible]1 : No disciplined monitoring and review of supplier services.	4	3			
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	- Supplier service management adapted for changes in supplier agreements.[illegible] Supplier service management adapted for enhancement of offered services made by organization.[illegible] Supplier service management adapted for changes in supplier provided services (eg. adoption of new technologies/products/tools, network enhancements, change of physical location of service facilities).	- Require changes in supplier service agreements due to adoption of new technologies to mitigate information security risks.[illegible] Managing changes to the provision of new services by suppliers.	- The service management team will evaluate and validate that the new technologies provided by the supplier to mitigate the identified security risks.[illegible] New supplier service agreement has to be agreed, signed off by both the organization and the supplier pertaining to adoption of advanced security controls and new offered services.	Jit Seah	5 : New supplier service agreements are created and agreed between organization and the suppliers whenever there are changes in the provisioning of supplier services.[illegible]4 : Appoint service management team with the technical skills to manage changes in supplier services (eg. adoption of new technologies/products, new development tools/environments, enhancement to networks, change of suppliers).[illegible]3 : Organization realign supplier service management policies and procedures to implement enhancements and improve security controls to resolve information security incidents.[illegible]2 : Define formal process to manage changes in supplier agreements.[illegible]1 : No formal process for managing the changes in supplier services.	4	2			

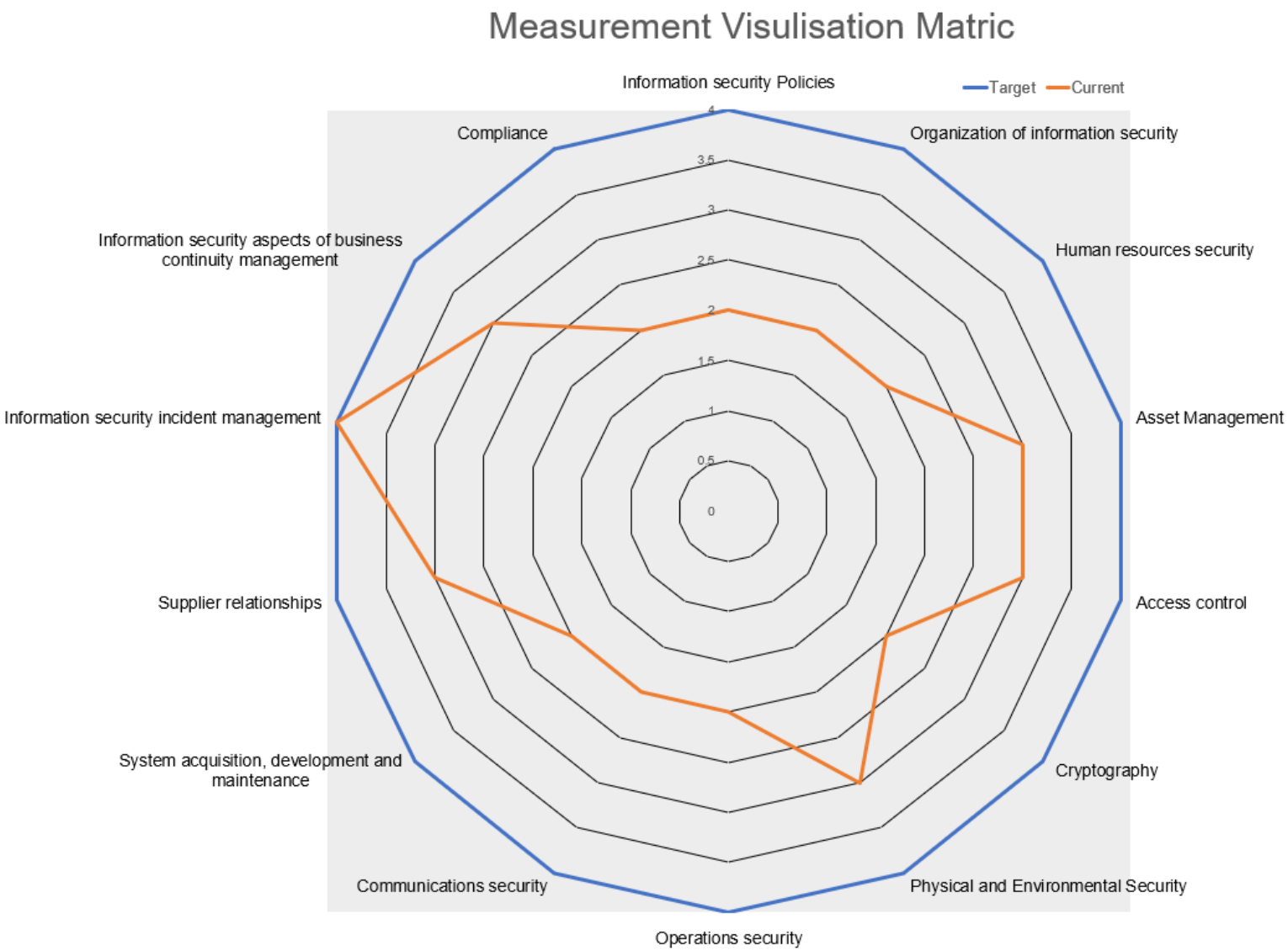
A.16	**Information security incident management**									**4**	**3**	**0.18**
A.16.1	Management of information security incidents and improvements Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.											
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	- Procedures are available for incident response planning, preparation, monitoring, detecting, analysing and reporting of information security incidents - Assigned point of contacts and priorities for handling the reported security incident.	- Clear responsibilities and procedures in incident management are established to handle incidents from reporting to closure - The identified security incident needs to be reported to the point of contact immediately, and communicated within organization on the same day of its detection.	- Whenever an information security incident is discovered, it will be promptly reported to the point of contact - The point of contact will investigate the reported security incident, prioritise accordingly and attempt to contain the incident.	Jit Seah	5 : Detailed documentations, assigned responsibilities and maintaining internal/external communications on prioritised security incidents 4 : Have clearly defined forms for reporting security incidents (eg. Document all evidence, escalations and all necessary actions) 3 : The point of contacts for security incidents' detection and reporting is implemented 2 : Clear procedures in the incident response plan to monitor, detect, analyse, and report of information security incidents with activities logs 1 : No clear incident management responsibilities and procedures for information security incidents.	3	2			
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	- No. of reported security events / incidents per month - Time to report from discovery of security events.	- All employees are encourage to report security events (eg. phishing emails, system breaches, virus/worms) to the Information Security Groups - Department managers need to submit security events report on the first working day of every month.	- Whenever a security event has been discovered, it will be promptly reported via the reporting channel - The information security lead will be assigned to follow up till closure of the reported security events.	Jit Seah	5 : Reporting channel is being used regularly and promptly (eg. weekly) 4 : Reporting channel is being only with reminders from management 3 : Have a clearly defined system for reporting security events (eg. Raise Alert/Alarm tickets) 2 : Ad-hoc created reporting of security events (eg. email) 1 : No reporting channel for security events.	3	4			
A.16.1.3	Reporting information security weakness	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	- No. of reported security weaknesses per month - Time to report from discovery of security weaknesses.	- All employees/contractors are require to report security weaknesses (eg. Application, Network, Operating Systems) to the Information Security Groups - Department managers need to submit an identified security weaknesses report on the first working day of every month.	- Whenever a security weakness has been discovered, it will be promptly reported via the established management channel - The information security lead will be assigned to follow up with responsive patching of the identified vulnerabilities - If there are no available patches, an Impact Analysis and temporary remediation actions on relevant vulnerabilities have to be done and stated in the monthly security report.	Jit Seah	5 : Reporting of system weaknesses and potential impacts is being done on a weekly basis 4 : Reporting of security weaknesses is irregular, depending on availability/urgency 3 : Have a clearly defined process for reporting security weaknesses (eg. Raise Trouble tickets) 2 : Ad-hoc reporting of security weakness (eg. email, verbal) 1 : No reporting of security weaknesses.	4	5			
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	- Information security event and incident classification scale is established - Point of contacts to assess the reported security event and decide whether to classify the event as an information security incident.	- Clear and agreed information security event and incident classification scale must be established so that it can be used for security incident assessment - The reported security event needs to be assessed quickly by the responsible point of contact and whether to classify the event as information security incident.	- The point of contact will perform the assessment based on the established information security event and incident classification scale - Whenever an information security event is reported, the point of contact will perform assessment and determine whether to classify the event as an information security incident.	Jit Seah	5 : Results of the assessment and decision are recorded in detail for future references and verifications 4 : Competent Information Security Incident Response Team (ISIRT) assessed and classified the reported security incidents 3 : The point of contacts for assessing and prioritising the reported security events based on incident classification scale 2 : Information security event and incident classification scale are not clearly defined 1 : No clear security incident assessments and classifications for the reported information security events.	3	2			
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	- Information security incident response procedures are readily available - Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are used to determine the necessary response strategy and resource for the security incident - Internal/External communication on the security incident is also clearly documented in the information security incident response plan.	- The data evidence of the information security incident are collected and analysed - The Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the information security incident are followed in accordance to the information security incidents procedures.	- After information system recovery in accordance to the information security incident response plan, the nominated point of contact will perform the information security forensics analysis on the collected evidence - He/She will identify the weakness in the information system that causes information security incident; followed through till closure - He/She will escalate and report the detailed findings to the higher management - After post-incident analysis is performed, the Information Security management will communicate the need-to-know details to both the internal/external people or organisations.	Jit Seah	5 : Post-incident analysis is performed to identify the source of the incident and communications are made after necessary recovery 4 : Perform information security forensics analysis on the collected evidence, and process escalation made according to the security incident response plan 3 : Evidence data are collected and preliminary analysis is performed on the information security incident 2 : Documented incident response procedures for resumption of operation to "normal security level" and recovery plan are available in the security incident response 1 : No documented incident response procedures are available for the information security incidents.	5	4			
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	- Percentage of information security employees trained in analysing and resolving information security incidents - How often are training conducted on security awareness?	- All information security employees should be trained within first week of joining the organization - Quarterly updates from each team on how they avoid/resolve security risks/incidents.	- Information security incident response training is part of New Employee Orientation programme for Information Security new-hires - Regular communication of up-to-date information security incidents and remediations.	Jit Seah	5 : The incident response repository are updated regularly with new incidents and remediation methods (eg. monthly) 4 : Repository for incident response plans and reports, that can be used to reduce likelihood of impact from security incidents 3 : Have a clearly defined incident response plan and regular updates and reviewed by team (eg. monthly team meeting) 2 : Ad-hoc sharing of information security incident response (eg. verbal) 1 : No information sharing on information security incidents.	3	4			
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	- Procedures to identify collect, acquire and preserve evidence in accordance with different types of media, devices and status of devices - Internal procedures are strictly following to avoid contamination/tampering of evidence - Legal needs to be involved in the process of evidence collection.	- Currently there are internal procedures on the identification, collection, acquisition and preservation of evidence on information security incident - But, there are improvements needed in the handling of collected evidence on information security incident.	- The investigating personnel need to be certified and professional tools need to be used in the process of evidence collection - Legal needs to be involved early in the evidence collection process so that different jurisdictions can be considered in order to maximise the chances for admission of the collected evidence.	Jit Seah	5 : Evidence reports of security incidents are created together with legal and shared with internal/external need-to-know parties 4 : Internal procedures on handling the evidence (eg. chain of custody, safety of evidence/personnel, competency of investigators) are strictly followed for the purposes of disciplinary and legal action 3 : Clearly defined procedures for the identification, collection, acquisition and preservation of the evidence in the security incidents 2 : Unstructured/incomplete collection of evidence in the information security incidents (eg. System logs/audit trails) 1 : No procedures are available or allocated resource for collecting evidences in security incidents.	3	1			
A.17	**Information security aspects of business continuity management**									**4**	**3**	**0.25**
A.17.1	Information security continuity Objective: Information security continuity should be embedded in the organization's business continuity management systems.											
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	- Information security continuity requirements are defined in the Business Continuity Management (BCM) systems - Business Impact Analysis (BIA) and Risk Assessment (RA) are presence in the Business Continuity Plan (BCP) - BCP strategies and plan are tested and regularly maintained.	- Well defined information security requirements for continuity in the adverse situations are presence the business continuity management systems - BIA and RA are conducted to determine the business recovery priorities, timescales and Maximum Tolerable Downtime (or minimal acceptable level of service).	- The BIA is used to access the impacts over time of not performing the services (eg. damage to physical assets, loss of life, denial of service) - Set prioritised timeframes for resuming the services/activities based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).	Jit Seah	5 : Business Impact Analysis (BIA) and Risk Assessment (RA) in the Business Continuity Plan (BCP) are tested, reviewed and revised regularly (eg. annually) in a Plan-Do-Check-Act (PDCA) cycle 4 : Information security requirements are explicitly formulated in the normal business continuity management and/or disaster recovery management process 3 : Establish and implement Business Continuity Procedures based on the defined information security requirements in adverse situations 2 : Perform a Business Impact Analysis to determine the information security requirements that are applicable to adverse situations 1 : No information security requirements are defined in the Business Continuity Plan.	3	3			
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	- Information security continuity objectives are defined by management - Appropriate information security controls are identified to ensure the required level of information security during adverse situation - Documented plans, response and recovery procedures are developed to manage a disruptive event and maintain information security at a predetermined level.	- Information security controls have been identified and documented in the business continuity and disaster recovery procedures - Competent information security personnel has been nominated to manage the disruptive event with the respective procedures.	- The identified information security controls has to be maintained and aligned with the predetermined level of business objectives during adverse situations - The information security controls within the business continuity or disaster recovery processes, procedures and supporting systems need to be revised and reviewed regularly - The compensating information security controls in the business continuity procedures need to be tested regularly to ensure their effectiveness to maintain the acceptable level of continuity for information security.	Jit Seah	5 : Using the exercised/tested information security controls in the business continuity or disaster recovery processes to ensure information security continuity in an adverse situation 4 : Appropriate management structure and nominate the information security personnel with the necessary responsibility, authority and competency to manage an incident in accordance to the documented plans, response and recovery procedures 3 : Create the documented plans, response and recovery procedures on how to manage a disruptive event and maintain the information security at a predetermined acceptable level based on management-approved information security objectives 2 : Establish, implement and maintain information security controls to ensure acceptable level of information security during adverse situation 1 : No processes, procedures, controls to ensure continuity of information security during an adverse situation.	4	3			
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	- Regular review, verification and evaluation of the information security continuity controls - The validity and effectiveness of the information security continuity controls during adverse situation.	- Ensure information security continuity controls are valid and effective during adverse situations - Business Continuity procedural changes affecting the information security continuity controls.	- The information security continuity controls are reviewed on a half-yearly basis to ensure consistency with the information security continuity objectives during adverse situations - When there are changes in the Business Continuity or Disaster Recovery procedures, the information security continuity controls are reviewed for their continual validities and effectiveness.	Jit Seah	5 : Integrate the evaluation of information security continuity controls with regular Business Continuity and Disaster Recovery tests 4 : Review the validity and effectiveness of information security continuity measures every half-yearly 3 : Verify the knowledge and routine to operate information security continuity processes/procedures/controls to ensure consistency with the information security continuity objectives 2 : Exercise and test the information security continuity controls when there are changes in organisation, technical, procedural and process 1 : No regular verification, review and evaluation of information security continuity controls.	4	3			
A.17.2	Redundancies Objective: To ensure availability of information processing facilities.											
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	- Business requirements for the availability of information systems are defined - System architectures with redundant components are used to support system failover - Confidentiality and Integrity security goals are designed in the Information systems with the implementation of redundancies.	- Business objectives that required redundancies are identified - Regular testing of high availability information systems to ensure failover as intended.	- Service Level Agreements for business offerings change over time and the business requirements for availability need to be revised and reviewed annually - The supporting redundant information systems are tested on a regular basis (eg. quarterly) to ensure failover from one system to another system works as required in order to satisfy the business availability.	Jit Seah	5 : Ensure integrity and confidentiality security goals are maintained while meeting the business availability requirements 4 : High availability information systems need to be tested regularly to ensure failover from one component to another component that works as intended 3 : All mission-critical information systems are implemented with redundancy to meet business availability requirements 2 : Identify the business requirements for the availability of information systems 1 : No redundancy in the information processing facilities.	4	3			

A.18	Compliance									4	2	0.15
A.18.1	Compliance with legal and contractual requirements Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.											
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative, statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	- Identification of all relevant legislative, statutory, regulatory, contractual requirements for each information system and the organization. - Document and maintain the organization approach in meeting all the relevant regulatory requirements.	- The need to identify all relevant legislative, statutory, regulatory, contractual requirements for each information system and the organization. - Agreement to an organization approach to meet all the relevant regulatory requirements.	- The Information Security team will work with the legal to identify and review all relevant legislative, statutory, regulatory, contractual requirements for each information system in the organization. - Agreement on the organization approach meet all the relevant regulatory requirements have to be documented and reviewed annually.	Jit Seah	5 : Business Impact Analysis needs to be performed for all regulatory requirements that are partially or not met due to resource limitations. 4 : Identify all relevant regulatory requirements for all the businesses operating in their respective countries. 3 : Document the organisation's approach to meet the relevant regulatory requirements for each information system and the organization. 2 : Identify the relevant legislative, statutory, regulatory and contractual requirements to the information systems and organization. 1 : No attention is given to legislative, statutory, regulatory and contractual requirements in the organization information systems.	3	2			
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	- Identification of all relevant legislative, statutory, regulatory, contractual requirements related to intellectual property rights and use of proprietary software products. - Intellectual property rights compliance policies are available and make aware in the organization.	- Ensure that all use of proprietary software products meet the legislative, statutory, regulatory, contractual requirements. - Compliance policies and respect for intellectual property rights are highlighted in the organization.	- Intellectual property rights training is part of New Employee Orientation programme for all new-hires. - Regular compliance awareness programs (via short talks, bulletins, intranet portals) are conducted for all employees with reminders that violators will have disciplinary actions taken against them. - Information Technology staffs need to perform bi-yearly system reviews to ensure that only authorized software and licensed products are installed.	Jit Seah	5 : Regular reviews and communications that only authorized software and licensed products are installed. 4 : Maintain awareness of the compliance policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them. 3 : Publish an intellectual property rights compliance policies that define the legal use of software and information products. 2 : Identify the relevant legislative, statutory, regulatory and contractual requirements to intellectual property rights and use of proprietary software products. 1 : No attention is given to intellectual property rights.	4	2			
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	- Record safeguarding objectives and guidelines. - Compliance policies for the protection of records in accordance with national or regional legislatory, regulatory, contractual and business requirements.	- Security goals (Confidentiality, Integrity and Availability) are applicable to the protection of records. - Compliance policies for record retention, storage, handling and disposal of records in accordance with national or regional legislatory, regulatory, contractual and business requirements.	- Policies/procedures for storage and handling of records are defined and reviewed annually in accordance with national or regional legislatory, regulatory, contractual and business requirements. - Ensure that stored records can be retrieved in an acceptable timeframe and format. - A retention schedule is maintained for records with respect to the national or regional legislations or regulations.	Jit Seah	5 : Define record safeguarding objectives and guidelines for the retention, storage, handling, disposal of records. 4 : Processes are defined for the protection of records in all states, namely during transit, under processing and permanent storage. 3 : Storage and handling (include timely retrieval) procedures of records with consideration to the media type and retention period as defined by national or regional legislations or regulations. 2 : Record classifications and protection of organization records in accordance with legislatory, regulatory, contractual and business requirements. 1 : No procedures for the protection of records.	3	2			
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	- Management structure and imposed controls on collection, processing and transmission of personally identifiable information. - Data policy defined for privacy and protection of personally identifiable information in relevant legislation and regulation.	- Form a management structure to implement the controls for privacy and protection of personally identifiable information. - Data policy is defined and communicated to all persons involved in the processing of personal identifiable information.	- A privacy officer is being appointed to provide guidance to employees on following the specific data privacy and protection policy. - Appropriate technical controls and organisational measures to protect personal identifiable information should be implemented with reference to the organization data policy. - Employees (eg. working in Human Resources/Sales/Marketing) should exercise responsibility when handling personally identifiable information and aware of the privacy principles in accordance with relevant legislations or regulations.	Jit Seah	5 : Implement a framework (with reference to ISO/IEC 29100) with appropriate controls on collection, processing and transmission of personally identifiable information. 4 : Structure management with an appointed person responsible (ie. privacy officer) to provide guidance to managers/users/service providers to follow the defined specific data policy and controls in handling privacy. 3 : Develop and implement controls with respect to data policy in the processing of personally identifiable information. 2 : Specific data policy for privacy and protection of personally identifiable information is created in accordance with relevant legislations and regulations. 1 : No data policy for privacy and protection of personally identifiable information.	4	2			
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	- Legal advises on the import and export of hardware or software components that perform cryptographic functions. - Compliance policy defined for cryptographic controls in accordance with all relevant agreements, legislations and regulations.	- Legal advise should be consulted prior to the import and export of developed hardware or software that perform cryptographic functions. - Compliance policy for regulations of cryptographic functions is defined and communicated to all persons involved in the development process.	- A legal officer is being appointed to provide guidance/advises pertaining to the import and export of hardware or software components that perform cryptographic functions. - Compliance policy is reviewed and updated whenever new technology, agreements, laws and regulations changes with respect to cryptographic functions. - Restrictions pertaining to the import or export of cryptographic functions is part of New Employee Orientation / re-training programme for the relevant engineers.	Jit Seah	5 : Legal administration and advice on mandatory or discretionary methods of access on encrypted information by countries' authorities (across jurisdictional borders). 4 : Appointed representative responsible (ie. legal officer) to provide guidance in the regulation of cryptographic controls. 3 : Enforce restrictions on import or export of computer hardware or software for performing cryptographic functions. 2 : Compliance policy for use of cryptographic controls in accordance with all relevant agreements, legislations and regulations. 1 : There is no use of cryptographic controls.	4	3			
A.18.2	Information security reviews Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.											
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur	- Independent review committees documented the review outcomes and assigned personnel/team to work on the amendments or take the corrective actions. - Independent review of information security management systems are conducted regularly and on the need basis.	- Annual independent review on the information security management systems is conducted by the independent review committee. - Documentations and follow up actions are assigned to the responsible individual/team to implement the corrective actions. - Upon completion of the corrective actions, the corresponding policies and processes are reviewed and updated.	- The independent review committee reviews/validates the relevancy of the control objectives, controls, policies, processes and procedures in the information security management systems. - Identified corrective measures for non-compliant areas will be assigned to the individual/team responsible in the respective implementation areas. - The responsible individual/team reports the closure and sign-off the identified changes to the review committee. This is followed by updating the respective documentations and information security policies in the information security management processes.	Jit Seah	5 : Regular independent reviews of information security management systems are based on ISO/IEC 27007 and ISO/IEC TR 27008 guidelines and conducted by the independent review committee. 4 : Review committee coordinates with the respective managers to assign resources and ensure that corrective actions are implemented. 3 : Independent review outcomes (ie. changes, improvements or additions of control objectives and controls) are documented. 2 : Independent review committee is formed to initiate independent review on information security management systems. 1 : No regular review of information security management systems.	4	3			
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	- Managers should regularly review the compliance of information security requirements within their area of responsibilities. - Automatic measurement and reporting tools should be used for efficient regular reviews.	- Managers perform quarterly review to ensure the compliance of information security requirements within their area of responsibilities. - All identified non-compliance should have corrective actions taken and documented for reporting to the independent review committee.	- Operation managers review the controls quarterly to ensure that information security requirements defined in policies, standards and other applicable regulations are properly satisfied. - All identified non-compliance should have their causes identified and implement corrective actions are documented for reporting to the independent review committee. - Verifications on the effectiveness of the corrective actions taken should be made and identifications of any other deficiencies or weaknesses.	Jit Seah	5 : Results of reviews and corrective actions taken by managers in their area of responsibilities should be recorded, maintained and reported to the independent review committee. 4 : Non-compliance causes are identified with corrective actions taken and documented. 3 : Quarterly reviews are conducted by individuals/managers to ensure the compliance of the information processing and procedures with the appropriate security policies, standards and security requirements. 2 : Managers have clearly defined roles and areas of responsibilities in ensuring that the respective information security requirements in security policies and standards are met. 1 : No regular review of information security requirements.	5	3			
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	- Technical reviews to ensure compliance with the organization's information security policies and standards. - Penetration Testing and vulnerability assessments with proper scoping are to be conducted by internal or external experts.	- Technical reviews should be conducted at least bi-yearly by specialists to ensure compliance with the organization's information security policies and standards. - Penetration Testing and vulnerability assessments should be conducted least bi-yearly or whenever major security incidents have been reported inside or outside organization.	- Technical compliance reviews should be conducted on at least half-yearly basis by technical specialists using automated tools whenever possible to general reports for subsequent interpretations. - Manual reviews by experienced system engineers are also performed. - Penetration Testing and vulnerability assessments should be conducted on at least half-yearly or whenever major security incidents have been reported inside or outside organization. They are used for inspecting how effective the hardware and software controls are implemented in preventing unauthorized access due to the identified vulnerabilities.	Jit Seah	5 : Technical compliance reviews are based on ISO/IEC TR 27008 and conducted by the qualified technical specialists. 4 : Compliance reviews with Penetration Testing (PenTest) and vulnerability assessments carried out by technical experts. 3 : Competent technical specialists perform the compliance analysis using appropriate software tools or via manual reviews. 2 : Technical specialists ensure the compliance of information security requirements with the organization's information security policies and standards. 1 : No formal internal governance for compliance with the organization's information security policies and standards.	4	2			

[C] Organization chart

	Objective	Target	Current	Weightage
A.5	Information security Policies	4	2	0.5
A.6	Organization of information security	4	2	0.14
A.7	Human resources security	4	2	0.16
A.8	Asset Management	4	3	0.1
A.9	Access control	4	3	0.07
A.10	Cryptography	4	2	0.4
A.11	Physical and Environmental Security	4	3	0.08
A12	Operations security	4	2	0.06
A.13	Communications security	4	2	0.12
A.14	System acquisition, development and	4	2	0.076923077
A.15	Supplier relationships	4	3	0.2
A.16	Information security incident manage	4	4	0.18
A.17	Information security aspects of busin	4	3	0.25
A.18	Compliance	4	2	0.15

[D] Radar chart



References

[1] ISO/IEC FDIS 27000:2012(E) (2nd edition) Information technology — Security techniques — Information security management systems — Overview and vocabulary

[2] ISO/IEC 2700 27001 - Information technology - Security techniques - Information security management systems - Requirements

[3] ISO/IEC FDIS 27002:2012(E) - Information technology — Security techniques — Code of practice for information security controls

[4] NIST Special Publication (SP) 800-27 Revision A