Sri Lanka Institute of Information Technology

IE3102-Enterprise Standards for Information Security

ISO 27001 Implementation for an Organization

Assignment 01

Submitted by:

Student Registration Number	Student Name
IT 20250256	Liyanarachchi H.L.C. L
IT 20250324	Piyumal W.R. A

Table of Contents

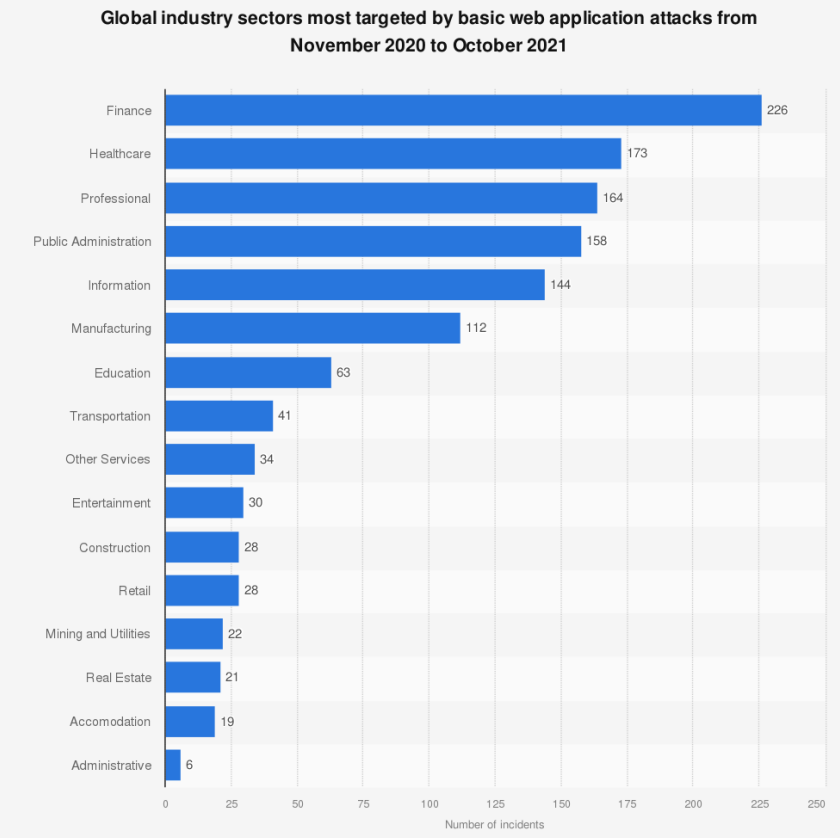
Overview

Bringing information security under formal management control is the goal of ISO 27001:2013. It comprises more than a hundred precise needs that are all-encompassing, adaptable, and beneficial to different sorts of companies. This standard is compatible with various management systems, including those for quality control, business continuity, and other topics. Information Security Management Systems are subject to the globally recognized standard ISO 27001. (ISMS). It offers a reliable framework to safeguard data that can be customized for different shapes and sizes of enterprises. Employing an ISMS that adheres to these criteria is becoming more popular among businesses.

Introduction to the Standard

The majority of the time, organizations are in possession of confidential information. The potential for significant damage to the organization exists in the case that any data is lost or stolen. In this case, it is of the utmost need to adhere to the appropriate standards in order to keep the information safe. The International Organization for Standardization (ISO) 27000 policy was released with the goal of bringing information systems closer to information security. Guidelines for the implementation, monitoring, and maintenance of information security are offered by ISO 27001 for all types of organizations and systems.

The applicability of ISO 27001 to organizations of any size and operating in any sector makes it the most valuable component of this information security standard. Its primary objective is to protect sensitive and confidential data. For the purpose of this assignment, we are going to assume that we are putting ISO 27001 into practice at the Asian Bank that has a significant number of locations all throughout the country. [1]Every day, banks must deal with a vast amount of confidential and sensitive data. Because the majority of those data are financially valuable, cybercriminals will attempt to acquire access to the data by exploiting any vulnerabilities that may exist in the system.



[2]According to the data that was compiled by Verizon, the financial industry will be the sector that suffers the most attacks on basic web applications between the months of November 2020 and October 2021.

People in today's world are understandably concerned about the privacy of their personal information. Consumers will be concerned about the privacy of their data due to the sensitive nature of their financial information held by banks and the fact that banks have customers' financial information. [3]In that case bank is able to reassure their stakeholders about the safety of their data if they comply with the requirements established by ISO 27001 and get a certificate recognizing compliance with those standards. It will also provide a competitive advantage for the bank, which will help it stand out from the other financial institutions. ISO 27001 certification is not a onetime process. Following the issuance of the ISO 27001 certificate to the financial institution, the organization that provided the certificate checks the efficiency of the bank's installed security measures and also performs annual audits.

Benefits of implementing ISO 27001

The only internationally recognized standard that can be audited and outlines the specifications for an ISMS is ISO 27001 (information security management system). Your information will be kept safe with the help of an effective information security management system (ISMS),

which offers a management framework of rules and guidelines. By implementing an ISO 27001 system, your company will have a system that will assist to either eliminate or significantly reduce the chance of a security breach. Risks may be recognized and minimized by creating and maintaining a formalized system of controls and management. [4]

Your firm will be strengthened across the three pillars of cyber security—people, procedures, and technology—if you are certified to ISO 27001. This means you may avoid paying expensive fines for failing to comply with data protection laws like the GDPR. It won't take long for employees to lose sight of their obligations related information security when firms change and expand. Data breaches and the hazards they pose are both continually increasing. To demonstrate to clients and stakeholders your dedication to upholding the highest standards of information security, obtain an ISO 27001 accreditation. It also implies that prospective consumers will see that you have a clearly defined information security management procedure in place. For the most part, enterprises may comply with these criteria without the need to implement additional procedures. No matter how and where information is kept and exchanged, putting in place an ISO-compliant ISMS will assist develop solid, tried-and-true processes and policies for protecting it. [5]

Your firm is effectively future proofed against these ever-growing security dangers with an ISO 27001 accreditation. Your business will be well-positioned to benefit from the structure, seizing expansion prospects and confidently continuing to serve your current clients for a very long time. Finding possible weak points and preventing breaches before they have an impact on your organization is made simpler. The hazards associated with cyber security and data breaches of any type are too high to rely just on a handshake and a new supplier's assurance that they are handling information sensibly. Even within their own organizations, businesses need to be protected, and this includes the security of their supply chains. On May 25, 2019, the General Data Protection Regulation (GDPR) goes into force. The lowest fine, according to statistics gathered by Privacy Affairs. A precise framework for thinking about information security threats, management procedures, and crucial operational components is provided by the ISO 27001 standard. This covers the need to keep IT systems current, antivirus software, data backup and storage, IT change management, and event tracking. [6]

Your consumers will see that you have taken precautions to secure their data if you are certified as an ISO 27001 ISMS. Few firms have the funds to spend on minimizing losses of that magnitude, and the average cost of a data breach has increased to roughly $4 million. Being ISO 27001 certified will guarantee the selection of suitable and proportional security measures,

which will also aid in fulfilling other criteria such as the Sarbanes-Oxley Act (SOX), NIST CSF (Cybersecurity Framework), and the General Data Protection Regulation (GDPR). [7]

Asset Register

Asset Register

Document Control

Reference: REC 8.1
Classification: In Restricted
Version: 1

Note: The Document control is on this page only and not on the additional worksheets that make up this plan. Therefore users of this plan should be aware that when printed, the sheets will not contain the document control on each subsequent worksheet

History

Version	Date of issue	Change
0.1	Oct-18	Initial issue
1.0	Oct-20	First published

Asset Register

Version: 1

Entity	Asset Group	Asset Type	Description (including examples)	Risk Owner	Risk Owner Name
Applications	Customer Data	Information	Personal informations of the bank customers	Product Manager	Mr. Nihal Perera
Finance	Financial data	Information	Financial Data of the bank customers	CFO	Mr. Kasun Chamara
Facilities	Premises	Building	Premises, reception, fixture & fittings, alarms, CCTV, data processing areas	Chief Branch Manager	Mr. Dasun Dissanayaka
HR	Staff Data	People	Personal data of Company Staff (Directors, Supervisors, Operational staff, temps, contractors)	HR Manager	Mr. Damitha Attalage
IT	Desktops / Laptops	Hardware	Office staff workstations (includes keyboard, mouse, screen, PCs, thin clients etc)	Internal IT	Mr. Asitha Perera
IT	Removable Media	Hardware	USB stick; CDs, Portable Hard drives...	Internal IT	Mr. Asitha Perera
IT	Server room (Internal)	Building	Room where servers are held	Internal IT	Mr. Asitha Perera
IT	Servers (Internal)	Hardware	Exchange, File, File & print, FTP, webservers, Domain Controllers	Internal IT	Mr. Asitha Perera
IT	Purchased Software	Software	Software employed; graphics; HR and associated licences etc.	Internal IT	Mr. Asitha Perera
IT	Telecommunications	Services	Landline/Fixed Phones; faxes	Internal IT	Mr. Asitha Perera
IT	Backups	Hardware	Backups of company held information (tapes, discs, server etc.)	IT Operations	Ms. Shalani Silva
IT	Servers (Datacenter)	Hardware	Customer products and applications.	IT Operations	Ms. Shalani Silva
IT	Websites (Public)	Information	Company owned public websites and online banking sites	CTO	Ms. Pawani Liyanarachchi
IT	Web Application	Information	Online Banking Web Application Of the Bank	CTO	Ms. Pawani Liyanarachchi

Katubedda	n/a	Physical	Company Secret	24	Dhammika Nuwan	E1005	2015-01-01	
Ratnapura	n/a	Physical	Company Secret	25	Dhammika Nuwan	E1005	2015-01-01	
Aluthkade	n/a	Physical	Company Secret	26	Dhammika Nuwan	E1005	2015-01-01	
Kollupitiya	n/a	Physical	Company Secret	27	Dhammika Nuwan	E1005	2015-01-01	
Haputale	n/a	Physical	Company Secret	28	Dhammika Nuwan	E1005	2015-01-01	
Bambalapitiya	n/a	Physical	Company Secret	29	Dhammika Nuwan	E1005	2015-01-01	
Borella S/G	n/a	Physical	Company Secret	30	Dhammika Nuwan	E1005	2015-01-01	
Ja Ela	n/a	Physical	Company Secret	31	Dhammika Nuwan	E1005	2015-01-01	
Hatton	n/a	Physical	Company Secret	32	Dhammika Nuwan	E1005	2015-01-01	
Maradana	n/a	Physical	Company Secret	33	Dhammika Nuwan	E1005	2015-01-01	
Peliyagoda	n/a	Physical	Company Secret	34	Dhammika Nuwan	E1005	2015-01-01	
Union Place	n/a	Physical	Company Secret	35	Dhammika Nuwan	E1005	2015-01-01	
Vavuniya	n/a	Physical	Company Secret	36	Dhammika Nuwan	E1005	2015-01-01	
Gampaha S/G	n/a	Physical	Company Secret	37	Dhammika Nuwan	E1005	2015-01-01	
Mannar	n/a	Physical	Company Secret	38	Dhammika Nuwan	E1005	2015-01-01	
Ambalangoda	n/a	Physical	Company Secret	39	Dhammika Nuwan	E1005	2015-01-01	
Puttalam	n/a	Physical	Company Secret	40	Dhammika Nuwan	E1005	2015-01-01	
Nugegoda Supergrade	n/a	Physical	Company Secret	41	Dhammika Nuwan	E1005	2015-01-01	
Nattandiya	n/a	Physical	Company Secret	42	Dhammika Nuwan	E1005	2015-01-01	
Dehiwala	n/a	Physical	Company Secret	43	Dhammika Nuwan	E1005	2015-01-01	
Kuliyapitiya	n/a	Physical	Company Secret	44	Dhammika Nuwan	E1005	2015-01-01	
Chunnakam	n/a	Physical	Company Secret	45	Dhammika Nuwan	E1005	2015-01-01	
Horana	n/a	Physical	Company Secret	46	Dhammika Nuwan	E1005	2015-01-01	
Maharagama	n/a	Physical	Company Secret	47	Dhammika Nuwan	E1005	2015-01-01	
Tangalle	n/a	Physical	Company Secret	48	Dhammika Nuwan	E1005	2015-01-01	
Eheliyagoda	n/a	Physical	Company Secret	49	Dhammika Nuwan	E1005	2015-01-01	
Beruwala	n/a	Physical	Company Secret	50	Dhammika Nuwan	E1005	2015-01-01	
Kadawatha	n/a	Physical	Company Secret	51	Dhammika Nuwan	E1005	2015-01-01	
Fifth City	n/a	Physical	Company Secret	52	Dhammika Nuwan	E1005	2015-01-01	
Moratuwa	n/a	Physical	Company Secret	53	Dhammika Nuwan	E1005	2015-01-01	
Velanai	n/a	Physical	Company Secret	54	Dhammika Nuwan	E1005	2015-01-01	
Matale	n/a	Physical	Company Secret	55	Dhammika Nuwan	E1005	2015-01-01	
Monaragala	n/a	Physical	Company Secret	56	Dhammika Nuwan	E1005	2015-01-01	

Entity	Asset Group	Classification	Data Classification	Asset ID	Assigned To	Employee ID	Assigned Date	Return Date
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0001	Pasan Sadaruwan	E1156	2020-06-05	
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0002	Dilshan Silva	E1157	2020-06-05	
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0003	Siril Kulathunga	E1158	2020-06-05	
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0004	Pawan Madawa	E1159	2020-06-05	10-8-2020
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0005	Avishka Heshan	E1160	2020-06-05	
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0006	Dilshan Silva	E1157	2020-06-05	
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0007	Siril Kulathunga	E1158	2020-06-05	
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0008	Pawan Madawa	E1159	2020-06-05	10-8-2020
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0009	Avishka Heshan	E1160	2020-06-05	
Colombo	n/a	Physical	Company Secret	1	Dhammika Nuwan	E1005	2015-01-01	
City Office	n/a	Physical	Company Secret	2	Dhammika Nuwan	E1005	2015-01-01	
Kandy	n/a	Physical	Company Secret	3	Dhammika Nuwan	E1005	2015-01-01	
Galle Fort	n/a	Physical	Company Secret	4	Dhammika Nuwan	E1005	2015-01-01	
Pettah	n/a	Physical	Company Secret	5	Dhammika Nuwan	E1005	2015-01-01	
Jaffna	n/a	Physical	Company Secret	6	Dhammika Nuwan	E1005	2015-01-01	
Trincomalee	n/a	Physical	Company Secret	7	Dhammika Nuwan	E1005	2015-01-01	
Panadura	n/a	Physical	Company Secret	8	Dhammika Nuwan	E1005	2015-01-01	
Kurunegala	n/a	Physical	Company Secret	9	Dhammika Nuwan	E1005	2015-01-01	
Badulla	n/a	Physical	Company Secret	10	Dhammika Nuwan	E1005	2015-01-01	
Batticaloa	n/a	Physical	Company Secret	11	Dhammika Nuwan	E1005	2015-01-01	
Central Office	n/a	Physical	Company Secret	12	Dhammika Nuwan	E1005	2015-01-01	
Kalutara S/G	n/a	Physical	Company Secret	13	Dhammika Nuwan	E1005	2015-01-01	
Negombo	n/a	Physical	Company Secret	14	Dhammika Nuwan	E1005	2015-01-01	
Chilaw	n/a	Physical	Company Secret	15	Dhammika Nuwan	E1005	2015-01-01	
Ampara	n/a	Physical	Company Secret	16	Dhammika Nuwan	E1005	2015-01-01	
Anuradhapura	n/a	Physical	Company Secret	17	Dhammika Nuwan	E1005	2015-01-01	
Wellawatte	n/a	Physical	Company Secret	18	Dhammika Nuwan	E1005	2015-01-01	
Matara	n/a	Physical	Company Secret	19	Dhammika Nuwan	E1005	2015-01-01	
Main Street	n/a	Physical	Company Secret	20	Dhammika Nuwan	E1005	2015-01-01	
Kegalle	n/a	Physical	Company Secret	21	Dhammika Nuwan	E1005	2015-01-01	
Point Pedro	n/a	Physical	Company Secret	22	Dhammika Nuwan	E1005	2015-01-01	
Nuwara Eliya	n/a	Physical	Company Secret	23	Dhammika Nuwan	E1005	2015-01-01	

Hambantota	n/a	Physical	Company Secret	58	Dhammika Nuwan	E1005	2015-01-01	
International Division	n/a	Physical	Company Secret	59	Dhammika Nuwan	E1005	2015-01-01	
Mirigama	n/a	Physical	Company Secret	60	Dhammika Nuwan	E1005	2015-01-01	
Galle Bazaar	n/a	Physical	Company Secret	61	Dhammika Nuwan	E1005	2015-01-01	
Naula	n/a	Physical	Company Secret	62	Dhammika Nuwan	E1005	2015-01-01	
Kilinochchi	n/a	Physical	Company Secret	63	Dhammika Nuwan	E1005	2015-01-01	
Anuradhapura New Town	n/a	Physical	Company Secret	64	Dhammika Nuwan	E1005	2015-01-01	
Primary Dealer Unit	n/a	Physical	Company Secret	65	Dhammika Nuwan	E1005	2015-01-01	
Galaha	n/a	Physical	Company Secret	66	Dhammika Nuwan	E1005	2015-01-01	
Bentota	n/a	Physical	Company Secret	67	Dhammika Nuwan	E1005	2015-01-01	
Welpalla	n/a	Physical	Company Secret	68	Dhammika Nuwan	E1005	2015-01-01	
Muttur	n/a	Physical	Company Secret	69	Dhammika Nuwan	E1005	2015-01-01	
Galenbindunuwewa	n/a	Physical	Company Secret	70	Dhammika Nuwan	E1005	2015-01-01	
Padavi Parakramapura	n/a	Physical	Company Secret	71	Dhammika Nuwan	E1005	2015-01-01	
Imaduwa	n/a	Physical	Company Secret	72	Dhammika Nuwan	E1005	2015-01-01	
Weeraketiya	n/a	Physical	Company Secret	73	Dhammika Nuwan	E1005	2015-01-01	
Yatawatte	n/a	Physical	Company Secret	74	Dhammika Nuwan	E1005	2015-01-01	
Pemaduwa	n/a	Physical	Company Secret	75	Dhammika Nuwan	E1005	2015-01-01	
Tirappane	n/a	Physical	Company Secret	76	Dhammika Nuwan	E1005	2015-01-01	
Medawachchiya	n/a	Physical	Company Secret	77	Dhammika Nuwan	E1005	2015-01-01	
Rikillagaskada	n/a	Physical	Company Secret	78	Dhammika Nuwan	E1005	2015-01-01	
Kobeigane	n/a	Physical	Company Secret	79	Dhammika Nuwan	E1005	2015-01-01	
Sewagama	n/a	Physical	Company Secret	80	Dhammika Nuwan	E1005	2015-01-01	
Horowpathana	n/a	Physical	Company Secret	81	Dhammika Nuwan	E1005	2015-01-01	
Ipalogama	n/a	Physical	Company Secret	82	Dhammika Nuwan	E1005	2015-01-01	
Medagama	n/a	Physical	Company Secret	83	Dhammika Nuwan	E1005	2015-01-01	
Tawalama	n/a	Physical	Company Secret	84	Dhammika Nuwan	E1005	2015-01-01	
Malkaduwawa	n/a	Physical	Company Secret	85	Dhammika Nuwan	E1005	2015-01-01	
Thanthirimale	n/a	Physical	Company Secret	86	Dhammika Nuwan	E1005	2015-01-01	

ISO27001 SOA

			Key: BP = Business Reason / Best Practice C/L/R = Contractual / Legal / Regulatory / 27001 Required				* If location not selected for business reasons. Activity not implemented at location
Control	Control Title	Control Description	Applied?	Reason for selection			Policy / Reason for Exclusion
				BP	C/L/R	RA	
5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes	X	X		Information Security Policy
5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes	X	X		Information security policy
6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Yes	X	X		Organization of information security
6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Yes	X	X	X	Organization of information security
6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Yes	X	X		Organization of information security
6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	X	X		Organization of information security
6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Yes	X		X	Organization of information security
6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	X		X	Organization of information security
6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	No				Against Policy to work remotely.
7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	X	X	X	Human resource security
7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	X	X	X	Human resource security
7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Yes	X			Human resource security
7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	X	X		Human resource security
7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	X			Human resource security
7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	X			Human resource security

8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	X		X	Asset management
8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Yes	X		X	Asset management
8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	X		X	Asset management
8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	X	X	X	Asset management
8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes	X	X	X	Asset management
8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes		X	X	Asset management
8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	X	X	X	Asset management
8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	No				This policy is not used in bank perimeter
8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Yes	X			Asset management
8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	No				Againt policy when transfer physical media
9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes		X	X	Access control
9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Yes		X	X	Access control
9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes		X	X	Access control
9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes		X	X	Access control
9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	X	X	X	Access control
9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Yes		X	X	Access control
9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Yes	X	X		Access control
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 shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes		X		Access control
9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes		X	X	Access control
9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	X	X		Access control

9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes		X	X	Access control
9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Yes		X	X	Access control
9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes		X		Access control
9.4.5	Access control to program source code	Access to program source code shall be restricted.	Yes		X		Access control
10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	No				No any cryptographic tools used in protection
10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	X	X		Cryptography
11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes		X	X	Physical and environmental security
11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes		X	X	Physical and environmental security
11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Yes		X	X	Physical and environmental security
11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes		X		Physical and environmental security
11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	No				Against policy when working
11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	No				This policy is not applicable for banking system
11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes	X	X		Physical and environmental security
11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	X		X	Physical and environmental security
11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	X	X	X	Physical and environmental security
11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	X	X	X	Physical and environmental security
11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Yes		X		Physical and environmental security
11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Yes		X	X	Physical and environmental security
11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes		X		Physical and environmental security
11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Yes		X		Physical and environmental security
11.2.9	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 shall be adopted.	No				This policy is not used in bank perimeter

12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Yes	X	X		Operations security
12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	X	X	X	Operations security
12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	X	X		Operations security
12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Yes		X	X	Operations security
12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes		X	X	Operations security
12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	X	X	X	Operations security
12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes		X	X	Operations security
12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes	X	X	X	Operations security
12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	X	X	X	Operations security
12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Yes		X		Operations security
12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Yes		X	X	Operations security
12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes		X		Operations security
12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	No				Against policy to install softwares to users
12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Yes	X	X	X	Operations security
13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Yes		X	X	Communications security
13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes		X	X	Communications security
13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Yes		X		Communications security
13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	X	X	X	Communications security
13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	X	X	X	Communications security
13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Yes	X	X		Communications security

13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	X	X	X	Communications security
14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes		X	X	System acquisition, development and maintenance
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.	Yes		X		System acquisition, development and maintenance
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.	Yes	X	X	X	System acquisition, development and maintenance
14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes		X		System acquisition, development and maintenance
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.	No				This policy is not applicable for banking system
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.	Yes		X		System acquisition, development and maintenance
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.	Yes		X		System acquisition, development and maintenance
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.	Yes		X		System acquisition, development and maintenance
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.	Yes		X		System acquisition, development and maintenance
14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Yes		X		System acquisition, development and maintenance
14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Yes		X	X	System acquisition, development and maintenance
14.2.9	System acceptance criteria	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes		X		System acquisition, development and maintenance
14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	No				There is no policy to test data just for testing
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.	Yes	X	X	X	Supplier relationships
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.	Yes	X	X	X	Supplier relationships
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.	Yes	X	X	X	Supplier relationships

15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	X	X		Supplier relationships
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.	Yes	X	X		Supplier relationships
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.	Yes		X	X	Information security incident management
16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes		X	X	Information security incident management
16.1.3	Reporting information security weaknesses	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.	Yes		X	X	Information security incident management
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.	Yes		X	X	Information security incident management
16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes		X	X	Information security incident management
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.	Yes		X		Information security incident management
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.	No				This policy is not applicable for banking system
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.	Yes		X	X	Information security aspects of business continuity management
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.	Yes		X	X	Information security aspects of business continuity management
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.	Yes		X	X	Information security aspects of business continuity management
17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	X	X	X	Information security aspects of business continuity management
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.	Yes		X		Compliance
18.1.2	Intellectual property rights (IPR)	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.	No				This is not a company with intrducing products
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.	Yes	X	X	X	Compliance

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.	Yes	X	X	X	Compliance
18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	No				This policy is not used in bank perimeter
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.	Yes		X		Compliance
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.	Yes		X	X	Compliance
18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards	Yes		X		Compliance

CLAUSE 1: Scope

It is highly important to determine the extent to which the standard must be applied since it poses a significant threat to the business if vital assets are discovered to be outside of the scope of the standard. [8]In order for the organization to be certified, it is necessary to determine both the objective of the standards and the specific parts of those standards that apply to the organization. This clause's primary focus is on accomplishing this goal. As a result, the most essential objective is to create a holistic risk-based program for the bank that is based on ISO 27001 framework.

Commonly following assets comes within the scope of standard,

1. Digital Banking Department
2. Data Center
3. IT Operations Department
4. CISO Office
5. Disaster Recovery Site
6. Business Continuity Plan

Additionally, the scope includes all employees, the location of the organization, business operations, and other data sources.

CLAUSE 2: Normative references

The purpose of this clause is to acquaint users with the meaning of the terminology that are used throughout the standard. The majority of the time, this section contains terms that are relevant when discussing the information security management system of the bank and its assets.

CLAUSE 3: Terms and Conditions

The purpose of this is to educate employees on the information security responsibilities that are not only their own but also those of the organization. [9]Before beginning their employment, every employee at Asian Bank is required to sign a Non-Disclosure Agreement (NDA), and all other stakeholders are also required to sign NDAs before beginning commercial relationships with Asian Bank.

An example of a non-disclosure agreement can be found below (NDA).

BARCLAYS

NON-DISCLOSURE AGREEMENT

Note: *This document is a Non-Disclosure Agreement only. A separate contract will be required whenever:*

- **goods or services** *are being provided by or to Barclays;*
- *any* **payment** *is being made by or to Barclays;*
- *any* **personal data** *is being transferred by or to Barclays; or*
- *any* **intellectual property** *is being created or licensed by either party to the other* **(including any rights to use Barclays' name or logo)**.

Barclays:	*Name and company registration number: (choose the applicable Barclays contracting entity)*	Barclays Services Limited (Registered Number 01767980) Barclays Bank PLC (Registered Number 1026167) Barclays Bank UK PLC (Registered Number 09740322)
	Registered address:	1 Churchill Place, London, E14 5HP
Counterparty:	*Name:* *(Full corporate or personal name of other party)*	
	Registered address: (or home address where individual)	
	Country of registration: (leave blank where counterparty is an individual)	
	Company registration number: (leave blank where counterparty is an individual)	
Effective Date: *(Date from which information is first being disclosed under this agreement – this can start before, after or on the date of signature)*		
Project: *(Details of the proposal/project to which this agreement applies, e.g. "Evaluations by Barclays of the Counterparty's [X] product", "Discussions for the development of an alternative [Y] system", "Discussions on how Barclays can collaborate with [X] for the purposes of [Y]")*		

Barclays and the Counterparty have entered into discussions regarding the Project and it is envisaged that each party may from time to time receive Information (as defined below) relating to the other in respect thereof. The parties have agreed that any dealings between them shall be subject to this Agreement, the terms of which are contained on the following pages.

Executed by the parties or their respective duly authorised representatives on the date of this Agreement.

	For and on behalf of Barclays:	**For and on behalf of the Counterparty:**
Signature:		
Name:		
Title:		
Date:		

TERMS OF NON-DISCLOSURE AGREEMENT

1 Definitions and Interpretation

1.1 In this Agreement the following definitions shall apply:

Affiliate means, in relation to a party, any person or entity Controlling, Controlled by or under common Control with such party from time to time;

Barclays Competitor means any bank or building society, or any other entity that carries on banking services, insurance services, credit or debit card issuing, card acquiring services, payment services, asset management or investment banking, or any entity Controlled by, Controlling, or under common Control of, any such entity;

Confidential Information means Information relating to one party or any of its Related Parties (**Disclosing Party**) (and/or the business carried on or proposed or intended to be carried on by the Disclosing Party) which is made available in connection with the Project to the other party (**Receiving Party**) (or any of its Related Parties) by the Disclosing Party (or any of its Related Parties), whether on or after the Effective Date, including any information, analysis or specifications derived from, containing or reflecting such information, but excluding any Information that the Receiving Party could not reasonably be expected to consider to be confidential or commercially sensitive;

Control means the power, direct or indirect, to direct or cause the direction of the management and policies of such entity whether by contract, ownership of shares, membership of the board of directors, agreement or otherwise and, in any event and without limitation of the foregoing, any entity owning more than 30% of the voting securities of a second entity shall be deemed to control that second entity. The terms **Controlling** and **Controlled** shall have a corresponding meaning;

Information means all information including, without limitation, any Intellectual Property Rights, information relating to systems, operations, plans, intentions, market opportunities, customers, suppliers, know-how, trade secrets and business affairs, business methods and business concepts in whatever form, whether in oral, tangible or in documented form and, if in tangible or documented form, whether marked or identified as being proprietary or not;

Intellectual Property Rights means:

(a) any copyright, design rights, patents, Inventions, logos, business names, service marks and trade marks, Internet domain names, moral rights, rights in databases, data, source codes, reports, drawings, specifications, know how, business methods, trade secrets, semi-conductor rights, topography rights, whether registered or unregistered, rights in the nature of unfair competition and the right to sue for passing off;

(b) applications for registration and the right to apply for registration for any of these rights; and

(c) all other intellectual property rights and equivalent or similar forms of protection,

existing anywhere in the world;

Invention means any invention, idea, discovery, development, improvement or innovation made, whether or not patentable or capable of registration, and whether or not recorded in any medium;

Permitted Purpose means any discussions or negotiations between the parties concerning the Project;

Related Party means, in relation to either party, any Affiliate of that party, or any director, officer, employee, agent, professional adviser (including solicitors, auditors, insurers and accountants), contractor or subcontractor of that party or of any Affiliate of that party.

2 Confidential Information

2.1 The Receiving Party shall treat and keep all Confidential Information as secret and confidential and will not, without the Disclosing Party's written consent, directly or indirectly communicate or disclose (whether in writing or orally or in any other manner) Confidential Information to any other person other than in accordance with the terms of this Agreement.

2.2 The Receiving Party shall only use the Confidential Information for the Permitted Purpose.

2.3 Notwithstanding clauses 2.1 and 2.2, the Receiving Party may disclose Confidential Information to its Related Parties (subject to clause 2.8), but only:

(a) to those Related Parties who strictly need to know the Confidential Information for the Permitted Purpose; and

(b) where such Related Parties are made aware prior to the disclosure of any part of the Confidential Information that that information is confidential and where the Receiving Party ensures that they owe a duty of confidence on materially the same terms as contained in this Agreement.

2.4 The Receiving Party shall at all times remain liable for any actions of any Related Parties in relation to any Confidential Information.

2.5 If any Confidential Information is copied, disclosed or used otherwise than as permitted under this Agreement then, upon becoming aware of the same, without prejudice to any rights or remedies of the Disclosing Party, the Receiving Party shall as soon as practicable notify the Disclosing Party of such event and, if requested by the Disclosing Party, take such steps (including the institution of legal proceedings) as shall be necessary to remedy (if capable of remedy) the default and/or to prevent further unauthorised copying, disclosure or use.

2.6 Notwithstanding whether or not the Receiving Party (or any Affiliate or Related Party) uses the Confidential Information in accordance with this Agreement (including modifying or further developing any Confidential Information), all Confidential Information shall remain the property of the Disclosing Party (or its licensors) and its disclosure shall not confer on the Receiving Party any rights of the Disclosing Party (or its licensors), including Intellectual Property Rights, over the Confidential Information whatsoever beyond those contained in this Agreement.

2.7 The Disclosing Party warrants and represents that, so far as it is aware, it has the right to distribute the Confidential Information to the Receiving Party in the format it provides it.

2.8 If there is a change of Control of the Counterparty to a Barclays Competitor then the Counterparty will not, without Barclays' prior written consent, directly or indirectly communicate or disclose (whether in writing, orally or in any other manner) Confidential Information disclosed to it by Barclays (or any of its Related Parties) to that entity.

3 Exceptions

3.1 The provisions of clause 2 (Confidential Information) above shall not apply to any Confidential Information which:

(a) is publicly available at the time of its disclosure or becomes publicly available (other than as a result of disclosure by the Receiving Party or any of its Related Parties contrary to the terms of this Agreement);

(b) was lawfully in the possession of the Receiving Party or any of its Related Parties (as can be demonstrated by its written records or other reasonable evidence) free of any restriction as to its use or disclosure prior to its being so disclosed;

(c) following such disclosure by the Disclosing Party, becomes available to the Receiving Party or any of its Related Parties (as can be demonstrated by its written records or other reasonable evidence) from a source other than the Disclosing Party (or any of its Related Parties), which source is not bound by any duty of confidentiality owed, directly or indirectly, to the Disclosing Party in relation to such information; or

(d) is required to be disclosed by law or governmental regulation or by any competent body or authority to which the Receiving Party submits, provided that the Receiving Party shall (to the extent permitted by applicable law) notify the Disclosing Party of the information to be disclosed (and of the circumstances in which the disclosure is alleged to be required) as early as reasonably possible before such disclosure must be made and shall take all reasonable action to avoid and limit such disclosure.

3.2 Confidential Information shall not be exempted under clause 3.1 from the confidentiality obligations in clause 2 (Confidential Information) by reason only that:

(a) some or all of its features (but not the combination and principle thereof) are or become publicly available or are in the possession of or become available to the Receiving Party in the manner stated in clause 3.1; or

(b) such information could be derived or obtained from information which is or becomes publicly available or is in the possession of or becomes available to the Receiving Party in the manner stated in clause 3.1 if to obtain or derive it would require substantial skill, labour or expense.

4 Records and return of information

4.1 The Receiving Party agrees to ensure proper and secure storage of all Confidential Information and any copies thereof to a reasonable standard and to at least the same standard as the Receiving Party keeps its own Confidential Information. The Receiving Party shall not make any copies or reproduce in any form any Confidential Information except for the purpose of disclosure or use as permitted in accordance with this Agreement, or reasonable backups (any such copies being subject to the provisions of this Agreement to the same extent as the original).

4.2 The Receiving Party shall keep a written record, to be supplied to the Disclosing Party upon request, of the Confidential Information received and any copies made thereof and, so far as is reasonably practicable, of the location of such Confidential Information and any copies thereof.

4.3 The Receiving Party shall, within seven days of receipt of a written demand from the Disclosing Party:

(a) return all written Confidential Information (including all copies); and

(b) expunge or destroy any Confidential Information from any computer, word processor or other device whatsoever into which it was copied, read or programmed by the Receiving Party or on its behalf (including by any person to whom disclosure has been made as permitted under clause 2.3 (Confidential Information)).

4.4 The obligations in clause 4.3 shall not apply to the extent that (and only for so long as):

(a) it is necessary to retain copies for the purpose of providing information to any regulatory authority or complying with any applicable regulatory requirements; or

(b) expunging or destroying any Confidential Information from any form of electronic storage would require an unreasonable degree of effort and/or expense,

in both cases, provided that any such Confidential Information shall be retained in accordance with the terms of this Agreement and no further commercial use (whether internal or involving external transmission) shall be made of any such Confidential Information.

4.5 The Receiving Party shall on request supply a certificate signed by a director as to its full compliance with the requirements of clauses 4.3 and 4.4.

5 Announcements

5.1 Neither party will make or permit to be made any announcement or disclosure of its prospective interest in the Project without the prior written consent of the other party.

5.2 Neither party shall make use of the other party's name or any information acquired through its dealings with the other party for publicity or marketing purposes without the prior written consent of the other party.

6 Duration

The obligations of each party and its Related Parties under this Agreement shall continue and shall survive the termination of any discussions or negotiations between the parties regarding the Project. In relation to each item of Information disclosed, they shall continue until the latter of:

(a) that Information ceasing to be confidential information by virtue of clauses 3.1(a) to 3.1(d) (subject to clause 3.2) applying to that Information; or

(b) five years from the date of disclosure by the Disclosing Party.

7 Representations

7.1 Each party agrees that any Information made available to the Receiving Party or any of its Related Parties for the purpose of negotiations or discussions in relation to the Project will not form the basis of, or any representation in relation to, any contract, nor constitute an offer or invitation by the Disclosing Party unless the parties expressly agree otherwise.

7.2 Except in the case of fraudulent misrepresentation and subject to clause 2.7 above, the Disclosing Party accepts no responsibility for, nor makes any representation or warranty, express or implied, with respect to, the accuracy, reliability or completeness of any Information made available to the Receiving Party or any of its Related Parties.

8 Adequacy of Damages

8.1 Without prejudice to any other rights or remedies of the Disclosing Party, the Receiving Party acknowledges and agrees that damages would not be an adequate remedy for any breach by it of the provisions of this Agreement and that the Disclosing Party shall be entitled to seek the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of any such provision by the Receiving Party or any of its Related Parties, and no proof of special damages shall be necessary for the enforcement of the rights under this Agreement.

9 Third Party Rights

9.1 Subject to clause 9.2, a person who is not a party to this Agreement may not enforce any of its terms under the Contracts (Rights of Third Parties) Act 1999.

9.2 Each and every obligation of the Receiving Party under this Agreement is owed to the Disclosing Party and to each of its Affiliates. Such Affiliates may enforce the terms of this Agreement under the Contracts (Rights of Third Parties) Act 1999. References to the Disclosing Party in the context of the Receiving Party's obligations shall be construed accordingly.

9.3 If a person who is not a party to this Agreement is stated to have the right to enforce any of its terms under the Contracts (Rights of Third Parties) Act 1999, the parties may rescind or vary this Agreement (and any documents entered into pursuant to or in connection with it) without the consent of that person.

10 General

10.1 Neither party may assign the benefit of this Agreement or any interest hereunder without the prior written consent of the other, save that Barclays may assign or novate any or all of its rights and obligations under this Agreement in whole or in part to any of its Affiliates or to the successor to the whole or a part of Barclays business.

10.2 This Agreement may be entered into by any number of counterparts and by the parties on separate counterparts, all of which taken together will constitute one single agreement between the parties. Counterparts executed by facsimile shall be sufficient for these purposes. An electronic copy of a signed copy of this Agreement (received in a Portable Document Format (PDF) or other, easily legible, suitable electronic format) or a copy of a signature received via a fax machine shall be deemed to be of the same force and effect as an original signature on an original executed document.

10.3 Delay in exercising, or failure to exercise, any right or remedy in connection with this Agreement shall not operate as a waiver of that right or remedy. The waiver of a right to require compliance with any provision of this Agreement in any instance shall not operate as a waiver of any further exercise or enforcement of that right and the waiver of any breach shall not operate as a waiver of any subsequent breach. No waiver in connection with this Agreement shall, in any event, be effective unless it is in writing, refers expressly to this clause, is duly signed by or on behalf of the party granting it and is communicated to the other party.

10.4 If any term of this Agreement is or becomes illegal, invalid or unenforceable in any jurisdiction, that shall not affect:

(a) the legality, validity or enforceability in that jurisdiction of any other term of this Agreement; or

(b) the legality, validity or enforceability in other jurisdictions of that or any other provision of this Agreement.

10.5 Each party shall at the request and cost and expense of the other party, sign all documents and do all other acts, which may be necessary to give full effect to this Agreement.

10.6 This Agreement (together with all other documents to be entered into pursuant to it) sets out the entire agreement and understanding between the parties, and supersedes all proposals and prior agreements, arrangements and understandings between the parties, relating to its subject matter.

10.7 Each party acknowledges that in entering into this Agreement it has not relied on any representation, warranty, collateral contract or other assurance (except those set out in this Agreement and the documents referred to in it and any other documents entered into on the date of this Agreement) between the parties made by or on behalf of any other party before the date of this Agreement. Each party waives all rights and remedies which, but for this clause 10.7 might otherwise be available to it in respect of any such representation, warranty, collateral contract or other assurance.

10.8 This Agreement and any non-contractual obligation arising out of or in relation to this Agreement shall be governed by and will be interpreted in accordance with English law. All disputes arising out of or relating to this Agreement or any non-contractual obligations arising out of or relating to this Agreement shall be submitted to the exclusive jurisdiction of English courts. Nothing in this clause limits the right of either party to bring interim proceedings arising out of or in connection with this Agreement:

(a) in any other court of competent jurisdiction; or

(b) concurrently in more than one court of competent jurisdiction.

CLAUSE 4: Context of the organization

The determination of the management scope in an exact manner is the goal of this clause. The context of the organization can be broken up into two parts, and the target area of each part can be determined using the information that follows.

Internal Context	External Context
Organization Culture	Competition
Management	Regulators and enforcement bodies
Resource Size	Economic Conditions
Information Asset Formats	Political Conditions
Resource Maturity	Environmental Considerations
Consistency	Shareholders
Physical Space	
Maturity	
Systems	
Systems Complexity	

CLAUSE 5: Leadership

The primary goal of this phase is to ensure and demonstrate the support and commitment of the top management of the Asian Bank. [10]The highest level of management at the Asian Bank is responsible for ensuring that the organization are committed to protecting the information security management system's(ISMS) availability, integrity, and confidentiality. The information security policy is something that can be implemented by the Asian Bank. The Bank of Bhutan's policy regarding the protection of customer information can be seen below.

Information Security Policy

Bank of Bhutan Limited

Code:	ISP
Version:	V 1.0
Date of version:	15th April 2020
Created by:	Head, ISD
Approved by:	ISSC
Distribution List:	ISSC, All employees
Confidentiality level:	**Public**

Version control

Version	Date	Short description modification
1.0	27th February 2020	Final

Review and Approval

Review / Approval Date	Approver	Review / Approval Notes
15th April 2020	Information Security Steering Committee	5th ISSC MoM

CONTENTS

A. OBJECTIVE

This policy ensures that the information assets of the Bank are appropriately protected against the breach of confidentiality, failures of integrity and/ or interruptions to their availability. The Information Security Policy (hereinafter referred to as the IS Policy) provides management direction and support towards information security for the Bank.

This policy is an apex document, which mandates the Information Security Management System at the Bank. It demonstrates Senior Management's commitment towards all security controls and mechanisms as given out in the subordinate policy documents and lays down the structure of information security in the Bank.

B. SCOPE

IS Policy is applicable to all information assets of Bank of Bhutan (BoB) that are electronically stored, processed, documented, transmitted, printed and/ or faxed. The policy applies to all employees and external parties (the term external parties in this document is used for third party users, contract staff, outsourced service providers, suppliers, vendors and consultants) of the Bank having logical and/ or physical access to Bank's facilities and supporting assets, either directly or indirectly.

C. POLICY OWNER AND POLICY CUSTODIAN

The owner of IS Policy will be the "Information Security Steering Committee" (hereafter referred to as ISSC) and the Head, Information Security Officer (Head, IS) will be the custodian of the policy.

D. RESPONSIBILITY

The ISSC of the Bank is responsible for approving IS Policy and any subsequent modifications in it. Head, IS along with Chief Information Officer (CIO) is responsible for ensuring that the policies constituting IS Policy are regularly updated and reflect the Bank's requirement. The Information Security Division along with respective Department Chiefs/Division Heads/Functional Heads/Location Heads of the Bank is responsible for implementation of security policy and they are also responsible for dissemination of IS Policy across all relevant business functions. The Heads of Business Units/ Functional Heads/ Location Heads are responsible for enforcing the implementation of IS Policy within their jurisdiction. However, it is

the responsibility of every individual, with access to information assets of the Bank, to adhere to IS Policy.

E. Policy Statement and Objective

"IS Policy of Bank of Bhutan aims at protecting all critical information, information processing and supporting service assets in order to ensure secure provision of services to its customers and business continuity."

The policy states:

- *that all forms of electronic/ print information, etc on servers, desktops, networking and communication devices, tapes, CDs and information printed or written on paper or transmitted by facsimile or any other medium will be covered.*
- *that procedures will be created and followed at various levels to ensure the protection of information security and objectives set for its continual improvement.*

The Information Security Policy provides management directives towards information security within the Bank and recommends appropriate security controls that need to be implemented to maintain and manage the information security in the Bank. Bank shall strive to secure information by:

i. Establishing and organising an information security governance framework;
ii. Developing and maintaining an effective security management system;
iii. Establishing and managing Information Security Policies, Procedures and Risk Management framework;
iv. Critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional;
v. Deploying appropriate technology and infrastructure;
vi. Continually monitoring, reviewing, exception reporting and taking actions thereof for improving the effectiveness of the Information Security Management System;
vii. Provide a framework for promoting 'best practices' relative to our information systems and infrastructure;
viii. All legal and contractual requirements with regard to Information Security are met wherever applicable;
ix. Any security incidents and infringement of the Policy, actual or suspected, are reported and investigated;

x. Awareness programs on Information Security are available to all employees and wherever applicable to third parties viz. Subcontractors, Consultants, Vendors etc and regular training imparted to them;
xi. Taking appropriate actions for the violation(s) of IS Policy; and
xii. Creating and maintaining a security conscious culture in the Bank.
xiii. Information Security Policy should provide a framework for setting of Information Security Objectives.
xiv. Continual improvement of ISMS should be emphasized in the Information Security Policy.
xv. Information security in project management: All the new project in the Bank should include the Information Security relevant aspect.

1. Review and Evaluation

The IS Policy document shall be reviewed at the time of any major change(s) in the existing environment affecting policies and procedures or *at least once a year*. The IS Policy document shall be reviewed and approved by the ISSC. The reviews will be carried out for assessing the following:

1.1 Impact on the risk profile in the Bank due to, but not limited to, the changes in the information assets, deployed technology/ architecture, regulatory and legal requirements; and
1.2 The effectiveness of the policies.

As a result of the reviews, additional policies could be issued and / or the existing policies could be changed / updated, as required. These additions and modifications would be incorporated into the IS Policy document. The Head, IS is responsible for the communication of the updated version of the IS Policy. Policies that are identified to be redundant will be withdrawn.

2. Disciplinary Measures for Non-Compliance

2.1 All employees and external parties are required to comply with IS Policy.
2.2 Non-compliance to IS Policy will attract disciplinary actions.

3. Exceptions

The IS Policy is intended to be a statement of Information Security requirements that needs to be met in BoB. However, the exceptions against individual controls in specific policy domains should be formally approved.

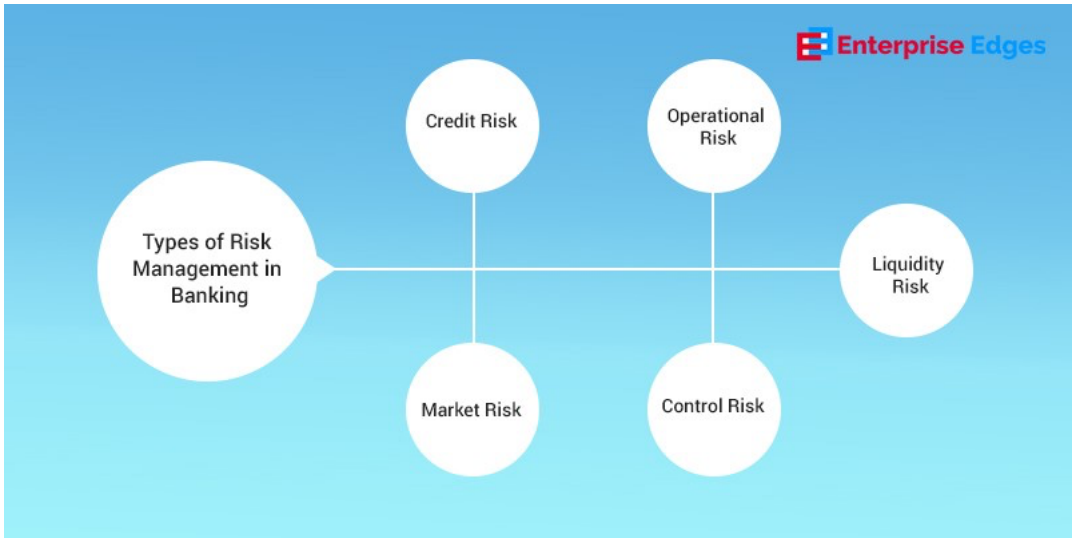
4. Definitions

4.1 **Asset:** Anything that has value to the organization.
4.2 **Assurance (Degree of):** A level of certainty that the control in place will eliminate or reduce the risks as expected. This is normally subjective and based on analysis, assessment, and experience.
4.3 **Audit:** Independent review of an activity or process to determine if it has functioned as intended.
4.4 **Availability:** The property of being accessible and usable upon demand by an authorized entity.
4.5 **Bank:** All references made in the IS Policy and subordinate policy documents will be interpreted as Bank of Bhutan only.
4.6 **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
4.7 **Control:** Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
4.8 **DRS:** Disaster Recovery Site
4.9 **Fallback:** Arrangements made to provide service in the event of the failure of computing or communications facilities.
4.10 **Information Processing Facilities:** Any information processing system, service or infrastructure, or the physical locations housing them.
4.11 **Information Security:** Preservation of Confidentiality, Integrity and Availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
4.12 **Information Security Management System:** That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
4.13 **Integrity:** The property of safeguarding the accuracy and completeness of assets.
4.14 **Media:** All devices that can electronically hold and store information. These include diskettes, CD's, tapes, cartridges and portable hard disks and any development from these.

4.15 **Policy:** Overall intention and direction as formally expressed by management
4.16 **Risk: C**ombination of the probability of an event and its consequence.
4.17 **Risk Management:** Coordinated activities to direct and control an organization with regard to risk.
4.18 **Safeguard:** This is defined as the mechanism by which a control may be implemented, optionally with others, to reduce or eliminate an identified threat.
4.19 **Security Event:** An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
4.20 **Security Incident:** A single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening Information Security.
4.21 **Security Domain:** A discrete logical or physical area of an organization that is the subject of security controls to protect it from all outside the domain. An organization may be a single domain or divided into many domains. A single computer system or communication network may be a domain.
4.22 **Third Party:** That person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
4.23 **Threat:** Threat is the potential cause of an unwanted event that may result in harm to the organization and its assets.
4.24 **Virus:** A computer virus is a piece of malicious software designed to attach itself to other programs and to replicate itself into other programs, ultimately very possibly infecting every program in a system. There is also a variant known as a macro virus, which attaches itself to the macros, which are a part of some word processor and spreadsheet programs. Other malicious software goes by such names as worms, Trojan horses or time bombs. These can all be very damaging to a system but are free standing rather than replicating attachments.
4.25 **Vulnerability:** Vulnerability is defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

CLAUSE 6: Planning

This section specifies how a company intends to manage information risks and opportunities. It emphasizes on the way a business handles information security risks and must be commensurate to their potential impact. The worldwide standard for risk management, ISO 31000, includes useful recommendations. Organizations must also prepare a "Statement of Applicability." [11] This section gives a description of considerations a company has made about risk treatment, the control goals and controls you have included and those you have omitted, as well as the reasons you have decided to include and exclude the controls in the SOA. Another important aspect of this clause is the requirement to set information security objectives, and the standard specifies the attributes that these objectives must possess. [12]



Businesses evaluate potential losses through the process of risk management and take action to reduce or eliminate them. It is a strategy that makes use of the outcomes of risk assessments, which comprise identifying potential risk factors in a company's operations, such as technical and non-technical business components, financial policies, and other worries that may have an impact on the firm's health. To manage banking risks, there are many different types of categories. They are access control, system acquisition and maintenance, information security policies, human resource security, and compliance. [12]

CLAUSE 7: Support

This part of ISO/IEC 27001 addresses the standards for information security management system competence, awareness, and communication (ISMS). Organizations must assess the amount of recorded information required to govern the ISMS. Controlling access to recorded information is prioritized, reflecting the significance of information security.

Competence - Most firms that already utilize tools like training/skills matrices, appraisals, or supplier evaluations can meet the requirement for competence records by increasing the categories covered. The main competencies of bank industry are Customer Attention, Planning and Organizing, Increasing Communication, Detail-oriented professionalism and Collaboration Problem-Solving Achievement Orientation. [11]

Awareness - Workers, suppliers and contractors will need to be familiar with the ISMS in addition to important staff. This is crucial for creating a supportive culture inside the company. Normally, this information may be conveyed by already-existing procedures and paperwork such as onboarding and supplier agreements.

Communication - Your processes, rules, and procedures clearly describe the needs for communication. If they aren't, you should think about listing them in a table or process. Keep in mind that your personnel must also share the details of these tables and processes. Banking communication touchpoints often include things like alerts, notices, consent management, letters, origination forms, social media posts, statements, on-demand contact centre/back-office interactions, customer preference management, product and service offer, and marketing. [12]

CLAUSE 8: Operation

The completion of the planned activities and the accomplishment of the information security goals are the topics covered in this area of the ISMS. Given the growing prevalence of outsourced tasks in today's corporate environment, these must also be recognized and under control. Also covered is the requirement for documenting material to be kept on file in order to record the outcomes of these. A bank must formalize its operations into a series of understandable and consistent processes in order to manage its information security threats and achieve its goals. [11]

Many of these procedures—such as induction and training—as well as awareness campaigns, rules and regulations, contracts, and customer service plans probably already exist; they just need to be modified to include information security-related components. Supplier approvals,

for instance, may occur on a sporadic basis, and certain procedures could not even exist at this time (e.g., information audit). [12]

CLAUSE 9: Performance evaluation

Your ISMS should be monitored, measured, evaluated, and evaluated again to make sure it is and continues successful. This provision enables businesses to evaluate their performance in regard to the standard's goals on an ongoing basis. Both management reviews and internal audits must be conducted. Both of these must be carried out at predetermined intervals, and the results must be saved as documented information. The goal of monitoring and evaluating bank performance is to determine which analytical methods may be used to a bank's financial statements in order to help management and the general public identify the most important issues that each bank is now facing and come up with solutions. [11]

Monitoring and performance evaluation of a bank is divided into three types,

1. A framework for evaluating bank performance
    - Internal performance
    - External performance
    - Presentation of bank financial statements
2. Analysing bank performance with financial ratios
    - Profit ratios
    - Risk ratios
3. Internal performance evaluations based on economic profit
    - RAROC (Risk Adjusted Return on capital)
    - EVA (Economic Value Added)

CLAUSE 10: Improvement

Corrective action requirements are the focus of this section of the standard. It will be necessary for you to demonstrate how you respond to deviations, act to remedy them, and cope with the fallout. Additionally, you'll need to demonstrate whether any comparable nonconformities already exist or might potentially do so, as well as how you plan to address their root causes to prevent such occurrences. Along with establishing the ISMS' appropriateness, sufficiency, and effectiveness, it is also necessary to demonstrate that it is improving continuously. Finding the causes of issues at their core in order to find the best remedies is known as root cause analysis (RCA). RCA bases its premise on the idea that systematic prevention and root-cause analysis

yield superior results than spot-treating symptoms and putting out flames. 5 why technique is one of the most effective ways to analyse a problem and find the solution for that. [11]

Problem – banking system was attacked by phishing attack

Why – some person clicked on a link in an email or website link downloaded malware to the PC and infected.

Why – person had not any training on clicking links on emails and web link as well as malware.

Why – person is not participating the awareness program and training has not worked to cover it.

Why – the short leave and holiday process is not control in the human resource policy and change management policy and information security management system does not identify security risks. [12]

These are some modern techniques for improve the efficiency of a banking system.

1. Realigning the company
2. channel improvement
3. procedure expenses
4. Employee effectiveness
5. modern methods of automation
6. Purchasing relationships

Conclusion

We interviewed numerous key stakeholders as part of the security assessment for Asian Bank in order to evaluate the organization's current security level and study the relevant paperwork and policies. After mapping interview and document analysis results to ISO/IEC 27001:2013 controls, we assessed the present condition of the Information Security Management Framework's implementation.

In order to bring security controls up to the recommended level of maturity and hence address technical components of ISO/IEC 27001 compliance, we advise Asian Bank to begin implementing them one at a time.

Reference

[1] 15 09 2022. [Online]. Available: https://www.southindianbank.com/UserFiles/file/RFPQ-ISMS_ISO_27001_Consultancy_and_Recertification.pdf.

[2] [Online]. Available: https://www.statista.com/statistics/221293/cyber-crime-target-industries/.

[3] [Online]. Available: https://www.pjr.com/standards/iso-27001/how-iso-27001-provides-cyber-security-for-the-banking-industry.

[4] L. Irwin, "5 benefits of ISO 27001 certification," itgovernance, 9 November 2021. [Online]. Available: https://www.itgovernance.eu/blog/en/benefits-of-iso-27001-certification.

[5] N. Sahoo, "What are the benefits of implementing ISO 27001 Standards?," Linkedin, 8 June 2021. [Online]. Available: https://www.linkedin.com/pulse/what-benefits-implementing-iso-27001-standards-narendra-sahoo/.

[6] J. Heron, "4 Benefits of ISO 27001 Implementation," isms.online, 13 July 2020. [Online]. Available: https://www.isms.online/iso-27001/4-key-benefits-of-iso-27001-implementation/.

[7] J. Hicks, "5 Big Benefits to Getting ISO 27001 Certified," schellman, [Online]. Available: https://www.schellman.com/blog/benefits-to-iso-27001-certification.

[8] T. v. d. Stoop. [Online]. Available: https://advisera.com/27001academy/blog/2019/11/25/iso-27001-for-banks-a-game-changing-security-investment/.

[9] [Online]. Available: https://www.dataguard.co.uk/blog/iso-27001-annex-a.7-human-resource-security/ .

[10] P. Biswas. [Online]. Available: https://preteshbiswas.com/2019/08/01/iso-270012013-clause-5-leadership/.

[11] bsi, "ISO/IEC 27001:2013," [Online]. Available: https://www.bsigroup.com/Documents/iso-27001/resources/iso-iec-27001-implementation-guide-SG-web.pdf.

[12] NQA, "ISO 27001:2013 Information Security Implemem=ntation Guide," [Online]. Available: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27001-Implementation-Guide.pdf.