Information security

Disclaimer

Document Version Control			
Document Owner	Jonathan Bloomfield		
Approving Committee			
Document Review and Revision History			
Version	**Reviewer**	**Description of Revision**	**Date of Revision**
V1.0	**Jonathan Bloomfield, Dan Turner, Ali Dove**		20/04/2016
Related documents	None		

Contents

1 Introduction 5

1.1 Background and purpose of document 5

1.2 What is PPL 5

1.3 Security testing 5

2 PPL InfoSec 6

2.1 Supplier Details 6

2.2 Supplier controls 8

2.2.1 Use of tabular format 8

2.2.2 Table of security controls 10

1 Introduction

1.1 Background and purpose of document

Placing Platform Limited (PPL) is currently in the process of implementing a new application to allow a more efficient and structured method to facilitate requesting and receiving quotes and firm orders in the Lloyds and London insurance market.

PPL are aware that every organisation's IT Department will require confirmation of the Information Security for the PPL platform, which we appreciate, but we are not able to complete individual questionnaires for each and every company.

In view of this, the purpose of this document is to set out the answers to the questions you may have concerning Information Security.

1.2 What is PPL

- The application is a web-based portal supported on all versions of Firefox and on Internet Explorer 8 and above.
- The PPL platform is accessible via an internet browser, but is based on a NTT hosted site in the UK with disaster recovery based in Germany. http://www.eu.ntt.com/en/index.html
- It manages the interactions between brokers and carriers from quote to bind and subsequent endorsements.
- The system contains a number of different user roles with the main ones being broker and underwriter. The broker is able to upload files documenting their requirements which are then sent out to the underwriters who can quote, request further information or reject. Underwriters can also save quotes, upload and return quotes using the system. Firm order processing and endorsements are also managed by the platform.

1.3 Security testing

- PPL and the IT Technical Sub Committee have commissioned a third party consultancy undertake the security testing of the platform.
- The scope of the Security Testing includes an Application Security assessment and an External Infrastructure assessment.
- For more details or any queries please email ppl@londonmarketgroup.com

2 PPL InfoSec

2.1 Supplier Details

The purpose of this section is to give an overview of the supplier of PPL (Ebix) including key contacts and their security certifications.

Supplier name:	Ebix Europe Ltd on behalf of Placing Platform Limited			
Description of Service:	Ebix Exchange for Placing Platform Limited			
Company Web site	www.ebixeurope.com			
Key Supplier Contacts	*Information Security Contact:*	*Mitul Patel*		
	Relationship Manager:	*Mark Challis*		
	Completed by:	*Mitul Patel*	**Date Completed:**	*04/03/2016*
Supplier Capability	*Size of Supplier Info Sec function:*	*Less than 5*		
	Size of Supplier organisation:	*Less than 100*		
Nature of Data Processed	*Highest Classification:*	*Confidential*		
Compliance Information	*PCI*	*N/A - No payment card data processed*		
	SOX	*N*		
	Data Protection Legislation	*N/A - No personal data held*		
	Safe Harbour Registered	*N*		
	HIPAA	*Y*		
	Other	*N/A*		
Data Breaches (Last 5 years)	*None*			

External Security Certifications or Independent Assurance:	Date Certified	Comments
ISO27001	*Jul-11*	*Certificate was valid until July 2014. Moved to SSAE16 based on clients' feedback*
SSAE16 Type 2	*Nov-15*	
SOC 2		*In progress with an expected completion of the SOC2 audit for the Ebix Europe office by the end of Q3 2016.*

2.2 Supplier controls

We have documented the supplier's security controls that are in place on PPL using the ISO27001 standard.

2.2.1 Use of tabular format

The table below details the table headings with a brief description of the contents of each column

Heading	Description
ISO27001 Ref	ISO27001 is a specification for an information security management system (ISMS).
ISO Subject	This is the subject area covered by ISO27001
ISO 27001 Control	This describes the control that needs to be in place for this subject
Supplier Control	Is the control in place by the supplier for this subject
Control Present	Is there a control in place for this subject? Yes, No or N/A

Heading	Description		
Maturity Rating	These are defined as follows –		
	IS Maturity Rating	**IS Maturity Definition**	**Example IS Maturity Level**
	1	*Initial*	Activities are Ad-hoc and there is some initial executive awareness in the organisation and IS is IT centric.
	2	*Developing*	There is an appointed CISO with evidence of limited user awareness and a formal IS improvement programme is in place
	3	*Defined*	There are established IS policies and processes, a defined Security organisation and improving culture of awareness
	4	*Managed*	There is an established Governance body, with effective IS metrics. The organisation adopts an information centric approach to IS and has an effective and established Security organisation.
	5	*Optimizing*	IS is embedded in the organisation and there is a Risk aware culture. Information owners are in place and are accountable and the there is a mechanism for the refinement of the organisation's IS posture triggered by changes to the business, environment, technology, economic and/or regulatory compliance.
Control Evidence	The control evidence section provides examples of the type of documentation or information that may be requested during an assurance review to validate the effectiveness of your stated controls.		
Supplier Comments	Additional information is in the “Comment” section where the controls do not meet the standard or provide security in excess of the standard.		

2.2.2 Table of security controls

This table details the information security standards on PPL, categorised by ISO27001 controls.

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
5.1.1	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	Does your CEO sponsor a comprehensive Information Security Policy that covers your whole organisation?	Y	4	(1) Signed off IS Policy by CEO or equivalent	
5.1.1	Policies for information security		Does your CISO (or an equivalent function) own the Information Security Policy, manage the policy maintenance schedule and make sure that approval deadlines are met?	Y	4	(1) Evidence that the IS policy is regularly updated - versioning. (2) A policy maintenance schedule is in place and is in operation (3) Any Policy approval deadlines have been met and/or are addressed.	
5.1.1	Policies for information security		Has your IS Governance body approved the Information Security Policy.	Y	4	Signed off IS Policy by the organisation's IS Governance body.	
5.1.1	Policies for information security		Has the CISO (or an equivalent function) signed-off on your Information Security Policy?	Y	4	Sign-off of IS policy is documented and as per stated timescales.	
5.1.1	Policies for information security		Does your CISO (or an equivalent function) make sure that the IS Policy is relevant and communicated to all employees in a form that is both understandable	Y	4	(1) IS Policy is effectively communicated via the company Intranet and by awareness messages/communiques. (2) IS Policy MI demonstrating that the	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			and accessible?			policy is understood by employees - use of business wide questionnaires or assessments?	
5.1.1	Policies for information security		Does your IS Governance body monitor the IS Policy and make sure that it has been communicated effectively?	Y	4	(1) IS Policy is effectively communicated via the company Intranet and by awareness messages/communiques.	
5.1.1	Policies for information security		Does your CISO (or an equivalent function) provide regular IS Policy adherence reports to your IS Governance body?	Y	4	(1) Regularly documented IS Policy compliance reports	
5.1.2	Review of the policies for information security	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Does your IS function liaise with appropriate SMEs to establish an annual review process to update the information security policy and to make sure that the policy complies with all relevant laws and regulations.	Y	4	(1) Documented evidence that a regular review process is in place and that appropriate SMEs have been engaged to make sure that the information security policy complies with all relevant laws and regulations.	
5.1.2	Review of the policies for information security		Do Internal Audit liaise with IS to review audit findings and identify areas of the information security policy that need to be updated?	Y	3	(1) A documented regular Audit review process, schedule and report with recommended policy enhancements, weaknesses and/or controls to be retired.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
5.1.2	Review of the policies for information security		Does your IS Governance body establish an annual review process to make sure that the modified information security policy remains effective, adequate and relevant?	Y	5	(1) A regular review process will be established to make sure that the information security policy remains effective, adequate and relevant.	
5.1.2	Review of the policies for information security		Does your IS Governance body enforce the annual information security policy review and approve any changes made?	Y	5	(1) Appropriate IS Governance bodies (e.g. IS Business Forum and/or IS Project Governance body) sign-off on the security policy review.	
6.1.1	Information security roles and responsibilities	All information security responsibilities should be defined and allocated.	Is your CEO accountable for Information Security and/or do they delegate IS responsibilities to the CISO function (or equivalent)?	Y	3	(1) Documented evidence that the CISO (or equivalent) is accountable for information security - e.g. CISO named in document header sheets as a required approver/signatory or stakeholder.) (2) Regular meeting minutes in which IS is an agenda item.	
6.1.1	Information security roles and responsibilities		Does your IS Governance body provide Information Security oversight for your Company and its business partners?	Y	3	(1) Evidence that the IS Governance body participates at a high level in the IS oversight of third parties - e.g. third party audit reports are periodically reviewed by	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						the Governance body.	
6.1.1	Information security roles and responsibilities		Has your CISO established an IS controls management framework to ensure that the implementation of security controls is consistent across your Company and its business partners?	Y	4	(1) Demonstration of an IS Management System within the organisation at least aligned to ISO 27001 principles.	
6.1.1	Information security roles and responsibilities		Does your CISO ensure that information security goals are identified, meet your company's requirements and are integrated with relevant processes?	Y	4	(1) A published IS strategy, standardised IS technology controls, and IS checklists/requirements embedded in appropriate stages of the organisations project life cycle process.	
6.1.1	Information security roles and responsibilities		Do Department Heads ensure that Information Security is documented as a key organisational risk and that compliance is reported?	Y	4	(1) Regular policy compliance and adherence reports (2) Key IS risks managed and reported	
6.1.1	Information security roles and responsibilities		Does your CISO make sure that information security roles and responsibilities are identified and assigned appropriately?	Y	3	(1) Documented, published and acknowledged (implicitly or explicitly) IS roles and responsibilities.	
6.1.1	Information security roles and		Does your CISO make sure that adequate provision is made for IS	Y	3	(1) CBT or an equivalent IS Training programme (2) Regularly updated IS	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	responsibilities		employees training.			training content - so training is relevant (3) Recourse to internal/external IS SMEs (4) Appropriate IS training materials (5) Attendance records of internal or external IS training courses. (E.g. CFHI, CISSP, Information Security etc. ...)	
6.1.1	Information security roles and responsibilities		Has your CISO approved plans and programs to maintain information security awareness?	Y	4	(1) Documented Info Sec awareness plan (2) Info Sec awareness schedules (3) Info Sec awareness materials	
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.	Do Line Managers document how duties are segregated to ensure that segregation of duties is maintained and to reduce the risk of accidental or deliberate system misuse?	Y	4	(1) Documented Roles and responsibilities (2) Documented and established processes for the segregation of duties (3) Regular access reviews (4) Independent checking of controls - anti financial crime or audit reports.	
6.1.2	Segregation of duties		Do IT Operations (or an equivalent function) segregate Wireless and internet only networks from your core network infrastructure?	Y	4	(1) Configuration settings/parameters for Wireless Access points devices (2) Internal audit report findings (3) Penetration test	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						results/reports for the wireless infrastructure (4) On-site verification of wireless infrastructure, IP address ranges and network logs	
6.1.3	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.	Do Department Heads ensure that business areas maintain contacts with the Regulatory authorities, Law enforcement agencies and emergency services (e.g. FRB, FCA, or the ICO)?	Y	4	(1) Up to date and complete external contact lists	
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.	Do representatives within the IS Governance body ensure that information from special interest groups is shared and/or communicated within their department?	Y	4	(1) IS Governance body meeting agendas and minutes	
6.1.5	Information security in project management	Information security should be addressed in project management, regardless of the type of the project.	Do Technology projects incorporate Information Security requirements into the project management process? This must require IS sign-off at specific stages of the project implementation life cycle.	Y	2	Project meeting minutes and sign-off	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
6.1.5	Information security in project management		Do non-technology projects incorporate Information Security requirements as part of change management? This must require IS sign-off at specific stages of the project implementation life cycle.	Y	2		
6.2.1	Mobile device policy	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	Are standards and guidance on the secure use of mobile devices published on your intranet or generally accessible to all your employees?	Y	3	(1) Documented and established standards for secure mobile usage and mobile device management. (2) Secure mobile working guidance and best practice (3) Signed AUPs	
6.2.2	Teleworking	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	Are standards and guidance for secure mobile working published on your intranet or generally accessible to all your employees??	Y	3	(1) Documented and established standards for secure teleworking (2) Secure teleworking guidance and best practice (3) Signed AUPs	
7.1.1	Screening	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and	Does your HR function have oversight of vetting for non-permanent employees?	Y	4	(1) MI/reports detailing CRB credit, right to work and references performed (permanent and non-permanent employees) (2) Sample CRB, credit, right to work and references for selected	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.				individuals	
7.1.1	Screening		Does your Procurement function ensure that contracts with agency firms include vetting check requirements?	Y	3	(1) Documented vetting check requirements (2) Agency vetting check process	
7.1.1	Screening		Does your HR function provide oversight of vetting checks including CRB, credit check, ID, right to work and referencing for all employees?	Y	4	(1) HR Agency vetting check process	
7.1.1	Screening		Does your HR function monitor vetting/CRB checks for contract employees employed for less than 3 months.	Y	4	(1) HR Agency vetting check process	
7.1.1	Screening		Do Building Facilities (Physical security) monitor supplier/agency checks for temporary agency employees (e.g. cleaning or security agency employees?)	Y	4	(1) HR Agency vetting check process	
7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors should state their and the organization's responsibilities for	Does your HR function ensure that all permanent employees sign terms and conditions prior to employment?	Y	5	(1) MI/Reports detailing signed terms and conditions of employment (2) Sample signed terms and conditions of employment for selected individuals.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
7.1.2	Terms and conditions of employment	information security.	Do your Line Managers liaise with your HR function to ensure that all employees have signed terms and conditions prior to employment?	Y	4	(1) MI/Reports detailing signed terms and conditions of employment (2) Sample signed terms and conditions of employment for selected individuals.	
7.1.2	Terms and conditions of employment		Does your HR function ensure that any employees with access to sensitive data sign a confidentiality clause as part of their contract of employment?	Y	5	(1) Confidentiality clause(s) in contracts (2) Sample signed terms and conditions of employment for selected individuals.	
7.1.2	Terms and conditions of employment		Does your HR function ensure that all employment contracts include clauses stipulating the adherence to your company's Security Policy, standards and guidelines?	Y	5	(1) Adherence clause(s) in contracts (2) Sample signed terms and conditions of employment for selected individuals.	
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.	Do Line Managers ensure that all employees they are responsible for have read and understood your company's Information Security Policy.	Y	3	(1) Employees induction checklist that log that employees have read and understood the minimum standards. (2) Completed on-line employees self-assessment surveys on a quarterly basis.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						(3) Completed annual CBT	
7.2.1	Management responsibilities		Do Line Managers provide their employees with guidelines stating your Company's security expectations during their period of employment?	Y	4		
7.2.1	Management responsibilities		Do Line Managers ensure that Information security training is conducted in line with Regulatory Compliance and HR employment requirements?	Y	3	(1) CBT or an equivalent IS Training programme (2) Regularly updated IS training content - so training is relevant	
7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Do Line Managers ensure that mandatory Information Security training (i.e. CBT) is undertaken by all employees and that such training takes place during their induction period?	Y	4	(1) CBT or an equivalent IS Training programme (2) Group-wide CBT completion reports for all employees.	
7.2.2	Information security awareness, education and training		Do IS monitor and ensure that all employees take the IS awareness training on induction and annually thereafter?	Y	4	(1) Group-wide CBT completion reports for all employees.	
7.2.2	Information security awareness,		Do IS maintain and publish your Company's InfoSec Policy,	Y	3	(1) Documented IS Policy, standards and guidelines	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	education and training		Standards and Guidance on the Company intranet or make it accessible to all employees?				
7.2.2	Information security awareness, education and training		Do IS (or an equivalent function) develop and drive an awareness campaign that includes: updated Intranet pages, posters, regular awareness articles and competitions?	Y	4	(1) Awareness materials: regularly updated Intranet pages, posters, regular awareness articles and competitions.	
7.2.2	Information security awareness, education and training		Do you have an IS business forum to oversee and approve all Information Security awareness activities?	Y	4	(1) Documented IS Forum (or equivalent) meeting minutes	
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.	Does HR (or an equivalent function) ensure that a commensurate and formal disciplinary process is defined, in place, and understood by all employees in the event of a policy breach?	Y	4	(1) Documented disciplinary process. (2) Disciplinary Communications to employees (3) Sample disciplinary cases	
7.2.3	Disciplinary process		Does HR (or an equivalent function) ensure that a formal disciplinary process is maintained, published, understood and followed by all Line Managers?	Y	4	(1) Documented disciplinary process. (2) Disciplinary Communications to employees (3) Sample disciplinary cases	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
7.2.3	Disciplinary process		Are IS (or an equivalent function) required to confirm that a security breach has actually occurred before any formal disciplinary process is invoked?	Y	3	(1) Documented Security Incident investigation process	
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.	Are Line Managers in your company responsible for controlling how employees are terminated or re-assigned and do they treat employee re-assignment or change of duties as an effective termination of that employee's previous employment responsibilities?	Y	4	(1) Documented access review process (2) Documented 'joiners, leavers and movers' process (3) Regular HR-IT access reconciliation reports.	
7.3.1	Termination or change of employment responsibilities		Do HR (or an equivalent function) confirm with the Line Manager that employee activities and duties have ceased within one week of re-assignment or termination?	Y	4	(1) HR-IT access reconciliation reports.	
7.3.1	Termination or change of employment responsibilities		Do Line Managers communicate any new information security requirements and/or information security	Y	3	(1) Employees induction checklist (2) IS guidance published on the Intranet.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			responsibilities to re-assigned employees?				
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.	Do IT Operations (or an equivalent function) ensure that they maintain asset registers, as stipulated in their contracts that clearly identify critical assets and all information needed to recover from a disaster situation?	Y	4	(1) Documented DR plans and DR test results (2) IT Physical asset registers	
8.1.1	Inventory of assets		Does IS (or an equivalent function) perform regular oversight of the Business/3rd party asset registers and conduct periodic sample checking to ensure quality and accuracy of each register?	Y	3	(1) Quality assurance check of 3rd Party Physical asset registers	
8.1.1	Inventory of assets		Does each Business area make available their critical asset registers to IS on request?	Y	3	(1) Business End User Computing (EUC) asset register (2) QA check of EUC asset register to confirm completeness and accuracy.	
8.1.1	Inventory of assets		Do Department Heads ensure that business areas maintain an asset register of their critical business (e.g. EUC	Y	4	(1) Business EUC asset register (2) QA check of EUC asset register to confirm completeness and	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			applications)?			accuracy.	
8.1.2	Ownership of assets	Assets maintained in the inventory should be owned.	Does your Company assign the Heads of department to be the default owner of any data generated by their department whenever said data has not been explicitly assigned an owner?	Y	3		
8.1.2	Ownership of assets		Do the Department Heads in your company explicitly assign ownership of all information assets to individuals or entities?	Y	3	(1) Information assets must be clearly labelled with an owner.	
8.1.2	Ownership of assets		Do the asset owners in your Company ensure that access restrictions and classifications of information assets are periodically reviewed?	Y	3	(1) Documented access review and data classification process (2) Access review results (2) Sample assurance checks by Information Security function to check accuracy and completeness of access reviews.	
8.1.2	Ownership of assets		Do IS (or an equivalent function) verify through sample assurance checks that business areas have identified and secured their assets?	Y	3	(1) Sample assurance checks by Information Security function to check accuracy and completeness of access reviews.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
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.	Do IS (or an equivalent function) provide guidance to all employees on the acceptable use and storage of USB devices, Laptops, CDs, DVDs, Remote access, E-mail and the Internet?	Y	4	(1) Documented guidance on acceptable use of these devices - (Intranet, Communications, AUPs) (2) Evidence of coverage in CBTs	
8.1.3	Acceptable use of assets		Do Line Managers ensure that employees sign up to your Laptop, Removable media (USBs, DVD/CDs), and Remote access Acceptable Use Practices (AUPs) before access is granted to these facilities?	Y	3	(1) Reconciled list of device users against list of signed AUPs (2) Use of a employees induction checklist	
8.1.3	Acceptable use of assets		Does your company oversee and track compliance to your AUPs and do they report compliance status to senior management?	Y	2	(1) Reported Internet and Email misuse incidents (2) Sample reports of Internet or email monitoring tools	
8.1.3	Acceptable use of assets		Do HR (or an equivalent function) discipline employees (as deemed appropriate) when they do not adhere to the company AUPs.	Y	2	(1) Reported Internet and Email misuse incidents (2) Sample reports/MI of disciplinary activities and actions taken	
8.1.3	Acceptable use of assets		Do HR (or an equivalent function) monitor and	Y	4	(1) CBT L&D completion reports across the	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			track employee understanding of the AUP (e.g. through the use of annual CBT packages)?			business (2) CBT MI	
8.1.3	Acceptable use of assets		Do IS verify, through sample assurance checks, that laptop, USB, CD/DVD AUPs are followed (e.g. that employees don't leave unsecured laptops on desktops)?	Y	4	(1) Security Incident report (2) Documented clear desk sweep process	
8.1.3	Acceptable use of assets		Do your Line Managers ensure that contractor's employees sign AUPs for USB, CD/DVD, laptops or remote access prior to being authorised to use these facilities?	Y	3	(1) Reconciled list of device users against list of signed AUPs (2) Use of a employees induction checklist	
8.1.3	Acceptable use of assets		Do IS monitor and track AUP sign-up for email and internet?	Y	3		
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	Do Line Managers adhere to your company's HR leaver's process to ensure that assets (e.g. hardcopies of documents, computer equipment and/or physical access tokens/passes) in the possession of terminated	Y	5	(1) Documented HR leaver's process (2) Line Manager leaver's checklist (3) Reconciled asset list with the HR leaver's list	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		agreement.	or re-assigned employees are returned?				
8.2.1	Classification of information	Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Do IS (or an equivalent function) review, refine and publish Data Classification Standards and Guidelines ('Asset Classification and Control') and are these published to ensure that there is awareness of data classification (Public / Internal / Confidential / Restricted)?	Y	4	(1) Documented Data Classification Standards and Guidelines	
8.2.1	Classification of information		Do IT Operations (or an equivalent function) provide controls to store data appropriately and according to its criticality and classification?	Y	4	(1) Documented folder access process	
8.2.1	Classification of information		Do Department Heads ensure that employees define, apply and record the classifications of their critical information assets?	Y	3	(1) Critical asset register (2) Recorded asset classifications	
8.2.1	Classification of information		Has IT Operations (or an equivalent function) implemented controls to perform manual or automated system-driven checking of the content of information assets	Y	3		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			(such as databases or files) to attempt to determine or infer their classification?				
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.	Do IS (or an equivalent function) provide guidance on labelling and handling of information and publish guidance on the intranet or some other method accessible by all employees?	Y	3	(1) Covered in CBT packages (2) Documented data handling guidelines	
8.2.2	Labelling of information		Do IS (or an equivalent function) monitor that IT Operations (or an equivalent function) physically label equipment?	Y	3	(1) On-site review of physical asset labelling (2) On-site reconciliation of sample physical asset registers and asset labels	
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.	Do Department Heads ensure that every information asset is stored in a folder or database with access rights or restrictions commensurate to its classification?	Y	4	(1) Documented folder access process (2) Folder access review reports	
8.2.3	Handling of assets		Do IS (or an equivalent function) publish standards for handling confidential data?	Y	4	(1) Guidance on media handling	
8.2.3	Handling of assets		Do IS (or an equivalent function) publish	Y	2	(1) Departmental guidance on use of hardcopy/output	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			standards for using printers, faxes and photocopiers?			devices such as printers, faxes and photocopiers.	
8.2.3	Handling of assets		Do Department Heads ensure that employee guidance is provided for handling information (e.g. hardcopies of documents or files on shared folders) consistent with its classification?	Y	3	(1) Minuted departmental meetings in which guidance is an agenda item (2) Guidance on using folders to share information (3) Documented and established media/data handling process	
8.2.3	Handling of assets		Do Line Managers assign asset owners to internal distribution lists to periodically review internal distribution lists and validate membership?	N	1	(1) Regularly updated internal distribution lists. (2) Assigned owner(s) to internal distribution lists	This process is not in place. Ebix implement this in next 6 months.
8.2.3	Handling of assets		Do Line Managers periodically review internal distribution lists to ensure that they are accurate?	Y	2		
8.2.3	Handling of assets		Do Department Heads ensure that employees handle information according to the published IS standards. (E.g. checking printers for confidential documents left on	Y	2	(1) Departmental guidance on use of hardcopy/output devices such as printers, faxes and photocopiers. (2) Documented and established clear desk/secure work environment	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			them.)?			policy/process	
8.2.3	Handling of assets		Do IS (or an equivalent function) mandate the use of printer PINs/passwords when employees print sensitive information?	Y	2	(1) Documented guidance on the secure use of PIN printing (2) Documented and established clear desk/secure work environment policy/process (3) On-site verification that PIN printing is enforced. (4) Sample Printer configuration	
8.2.3	Handling of assets		Do IS (or an equivalent function) mandate the use of scanning devices to require PINs/passwords?	N	1	(1) Documented guidance on the secure use of scanners (2) Documented and established clear desk/secure work environment policy/process (3) On-site verification that PIN scanning is enforced. (4) Sample Scanner configuration	This process is not in place. Ebix implement this in next 6 months.
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	Does HR (or an equivalent function) ensure that AUPs are in place and signed by any permanent employees authorised to use removable media and monitor that said AUPs are adhered to?	Y	3	(1) Documented and established AUPs and process	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
8.3.1	Management of removable media	organization.	Has IS (or an equivalent function) established guidelines for the safeguarding of data and established guidelines relating to handling hardcopy/printed materials?	Y	3	Documented guidance on media handling (hardcopy/paper)	
8.3.1	Management of removable media		Has IS (or an equivalent function) established AUPs for all employees authorised to use removable media and that these AUPs have been signed?	Y	3	(1) Documented removable media AUPs (2) Regularly maintained list of signed removable media AUPs (3) Sample review of signed removable media AUPs	
8.3.1	Management of removable media		Has your company established procedures for the management of removable media?	Y	4	(1) Documented and established process for managing removable media (2) Regularly maintained data transfer log	
8.3.1	Management of removable media		Do IT Operations (or an equivalent function) ensure that employees with access to removable media are monitored?	Y	3	(1) Regularly maintained data transfer log	
8.3.1	Management of removable media		Do IS (or an equivalent function) ensure that asset registers including all removable media are maintained?	Y	3	(1) Regularly maintained data transfer log	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
8.3.1	Management of removable media		Does your company operate controls to enforce encryption on any removable media device?	Y	2	(1) Regularly maintained data transfer log detailing encryption method and strength (2) On-site sample verification of removable media encryption process (3) Verification of control tool configuration files (4) Verification of control tool logs	
8.3.1	Management of removable media		Does your company ensure that controls are implemented that enforce restrictions on the use of personal devices within your information processing facilities?	Y	3	(1) Physical controls - CCTV camera footage, Data centre entry checks (2) Security incident MI/reports (3) Advisory/Guidance on use of personal devices	
8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures.	Do Building Facilities (or an equivalent function) provide media disposal bins (paper and electronic media) that are locked and sent for secure disposal?	Y	3	(1) On-site verification of confidential and non-confidential bins for hardcopy. (2) On-site verification of cross-shredding capability	
8.3.2	Disposal of media		Do Building Facilities (or an equivalent function) validate that confidential media has been disposed of correctly?	Y	5	(1) On-site verification of contents of confidential and non-confidential bins for hardcopy.	
8.3.2	Disposal of media		Do Building Facilities (or an equivalent function) ensure that third parties	Y	3	(1) On-site verification of confidential and non-confidential bins for	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			specialising in (paper and/or electronic media) disposal have applied appropriate security controls and have been accredited to an acceptable standard?			hardcopy. (2) On-site verification of cross-shredding capability (3) Verification of accreditation status of disposal company	
8.3.2	Disposal of media		Has IS (or an equivalent function) provided guidance to classify and identify items that require secure disposal?	Y	3	(1) Guidance on the classification of items requiring secure disposal	
8.3.2	Disposal of media		Has IS (or an equivalent function) established formal procedures to log disposal of information consistent with its classification?	Y	3	(1) Documented and established media disposal process (2) Regularly maintained media disposal log (3) Certification embedded in the media disposal process	
8.3.2	Disposal of media		Has IS (or an equivalent function) provided guidance to all employees advising how to differentiate between non-confidential and confidential waste and how to treat these differently to avoid separation mistakes?	Y	3	(1) Guidance on the classification of items requiring secure disposal	
8.3.3	Physical media transfer	Media containing information should be protected	Has IS (or an equivalent function) established and published standards and	Y	3	(1) Documented and established guidance on data transportation	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		against unauthorized access, misuse or corruption during transportation.	guidance for the safe and secure physical transportation of data (to cover courier identification, trace delivery, encryption, and packaging methods).				
8.3.3	Physical media transfer		Has your company implemented a transfer register detailing how the safe and secure physical transportation of data is achieved (this should cover courier identification, trace delivery, encryption, and packaging methods)?	Y	3	(1) Regularly updated/maintained data transfer register	
8.3.3	Physical media transfer		Do Department Heads ensure that employees perform periodic checks to verify that (where applicable) the media transport standards have been followed?	Y	3	(1) Documented and established media transport checking process	
9.1.1	Access control policy	An access control policy should be established, documented and reviewed based on business and information security	Has IS (or an equivalent function) defined and published an access control standard?	Y	4	(1) A published access control standard for applications, data and the network.	
9.1.1	Access control policy		Has your Company implemented access controls for applications, data and the networks?	Y	4	(1) Documented processes and procedures to implement the access control standard.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
9.1.1	Access control policy	requirements.	Have your Department Heads established a robust and comprehensive access review process in line with your company guidelines for systems, network folders, applications, and data?	Y	3	(1) Documented and established access review process that implements the access control standard.	
9.1.1	Access control policy		Do Business areas enforce the access authorisations process for their area?	Y	3	(1) Documented and established authorisation process that implements the access control standard. (2) List of approvers/authorisers	
9.1.1	Access control policy		Do Business areas conduct periodic reviews of access for the IT systems and network folders they use?	Y	3	(1) Access review reports (2) Reconciled HR current employee list with current access rights review report	
9.1.1	Access control policy		Do Business areas enforce an access removal process for leavers?	Y	4	(1) Access review reports (2) Reconciled HR leavers lists with current access rights review report	
9.1.1	Access control policy		Does IS (or an equivalent function) work with the business to define and implement Role based Security Profiles, where appropriate and applicable?	Y	4	(1) Documented and established roles based access profiles	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
9.1.1	Access control policy		Do Department Heads ensure that, where applicable, role based security profiles are used to set up user access permissions?	Y	4	(1) Documented and established roles based access profiles (2) Meeting minutes/departmental guidance on the use of RBAC/security profiles	
9.1.1	Access control policy		Do Business areas implement access reviews on critical IT systems they use on a 6 monthly basis?	Y	4	(1) Bi-annual access review reports	
9.1.1	Access control policy		Has your Strategy & Architecture team (or an equivalent function) conducted a feasibility study on the use of Single sign on technologies?	Y	5		
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.	Does your company manage access rights/permissions on network services to prevent unauthorised access?	Y	4	(1) Documented and established network access/secure management processes (2) Configuration settings/parameters for network devices (3) Internal audit report findings (4) Penetration test results/reports	
9.1.2	Access to networks and network		Has your company implemented Firewalls to control access to network	Y	5	(1) Documented and established Firewall access/secure	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	services		services and prevent unauthorised access to internal and external networked services?			management processes (2) Configuration settings/parameters for firewall devices (3) Internal audit report findings (4) Penetration test results/reports	
9.1.2	Access to networks and network services		Has your company implemented IDS/IPS systems to prevent unauthorized access to internal and external networked services?	Y	4	(1) Documented and established IDS/IPS access/secure management processes (2) Configuration settings/parameters for IDS/IPS devices (3) Internal audit report findings (4) Penetration test results/reports	
9.1.2	Access to networks and network services		Does your company restrict the visibility of network services only to authorised users?	Y	4		
9.1.2	Access to networks and network services		Has your company implemented network access control lists to limit network access from unauthorised users or systems?	Y	4	(1) Evidence of a layered security architecture/design	
9.2.1	User registration and de-registration	A formal user registration and de-registration process should be	Does IS (or an equivalent function) reconcile that redundant user accounts have been removed from	Y	4	(1) Review of business bi-annual access review reports	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		implemented to enable assignment of access rights.	all critical IT systems?				
9.2.1	User registration and de-registration		Do Department Heads ensure that, where applicable, robust user registration and authentication processes are established for critical applications?	Y	3	(1) Documented and established roles based access profiles (2) Meeting minutes/departmental guidance on the use of RBAC/security profiles	
9.2.1	User registration and de-registration		In your company, is the authorising Line Manager responsible for ensuring segregation of duties?	Y	3	(1) Regular review of business access review reports	
9.2.1	User registration and de-registration		Do Department Heads ensure that, where appropriate, conditions of use are provided to employees whenever access is changed or granted?	Y	3	(1) Documented and established process on changes to roles and responsibilities (2) Meeting minutes/departmental guidance on changes to roles and responsibilities	
9.2.1	User registration and de-registration		Does your company retain an up to date record of registered users on all critical systems?	Y	3	(1) Regular review of business access review reports	
9.2.1	User registration and de-registration		Do IS (or an equivalent function) monitor IT Operations (or an equivalent function) to ensure this control is effectively implemented?	Y	3	(1) Regular review of 3rd Party business access review reports	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
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.	Do IS (or an equivalent function) reconcile that redundant user accounts have been removed from critical IT systems?	Y	3	(1) Review of business bi-annual access review reports	
9.2.3	Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	Do your Line Managers define and approve privileged user access rights before they are granted and at all subsequent stages of the access life cycle?	Y	3	(1) Documented and established Line managers 'privileged access' approval process.	
9.2.3	Management of privileged access rights		Are your Line managers responsible for defining privileged access rights for the business applications their employees use?	Y	3	(1) Documented and established Line managers 'privileged access' definition process.	
9.2.3	Management of privileged access rights		Does your company implement controls to enforce administrator rights restrictions on Desktop PCs and laptops?	Y	4	(1) Microsoft AD Group definitions (2) On-site verification of user access capability on a sample set of laptops	
9.2.4	Management of secret authentication information of	The allocation of secret authentication information should	Has IS (or an equivalent function) established and published a formal new password request	Y	4	(1) Documented and established new password request process.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	users	be controlled through a formal management process.	process?				
9.2.4	Management of secret authentication information of users		Do all your employees change passwords periodically, where this is technically feasible, or obtain an exception/waiver where not possible?	Y	4	(1) Sample of issued waivers (2) System password logs demonstrating passwords resets have occurred (3) Password reset parameters/configuration	
9.2.4	Management of secret authentication information of users		Does your company implement controls to ensure that a forced password change occurs on first use or immediately after a password reset?	Y	4	(1) System password logs demonstrating passwords resets have occurred (2) Password reset parameters/configuration	
9.2.4	Management of secret authentication information of users		Do all your employees acknowledged the receipt of passwords from security administrators, and are they aware that they must not share passwords and must keep passwords confidential?	Y	4	(1) Documented guidance on password handling (2) Validate that topic is adequately covered in CBT, awareness, guidance	
9.2.4	Management of secret authentication information of users		Has IS (or an equivalent function) implemented assurance checks to ensure that IT Operations change the default vendor, system and administrator passwords following the	Y	3	(1) Internal audit reports (2) Internal penetration testing results (3) On-site review of system password files/password logs	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			installation of systems or software?				
9.2.4	Management of secret authentication information of users		Are all your employees aware that they must never store passwords in an unprotected form?	Y	3	(1) Internal audit reports (2) Internal penetration testing results (3) On-site review of system	
9.2.4	Management of secret authentication information of users		Do your Security Administrators verify the identity of employees prior to the issue of temporary passwords and is the communication of said passwords done in a secure manner?	Y	3	(1) Documented guidance on password handling (2) Validate that topic is adequately covered in CBT, awareness, guidance (3) Documented and established password issuance process	
9.2.5	Review of user access rights	Asset owners should review users' access rights at regular intervals.	Have your Department Heads established procedures to review employee's access on company systems are enforced?	Y	3	(1) Regular review of business access review reports	
9.2.5	Review of user access rights		Have your Department Heads established procedures to review network drive folder permissions under their control?	Y	3	(1) Regular review of business access review reports for network folders (2) Identified folder owners/gatekeepers	
9.2.5	Review of user access rights		Have your Department Heads established a process to review access rights after a user role/function changes?	Y	3	(1) Documented and established process on changes to roles and responsibilities (2) Meeting	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						minutes/departmental guidance on changes to roles and responsibilities (3) Regular review of business access review reports	
9.2.5	Review of user access rights		Have IS (or an equivalent function) established a process for reviewing access rights on critical systems?	Y	3	(1) Documented and established process on changes to roles and responsibilities (2) Meeting minutes/departmental guidance on changes to roles and responsibilities (3) Regular review of business access review reports	
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.	Do Line managers ensure that IT Operations (or an equivalent function) are informed to allow them to remove users access rights to information and information processing systems before employment terminates and as dictated by the assessed risk?	Y	4		
9.3.1	Use of secret authentication	Users should be required to follow	Do IS (or an equivalent function) provide advice	Y	4	(1) Documented guidance on password management	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	information	the organization's practices in the use of secret authentication information.	(via annual CBT and intranet guidelines) on the selection of strong passwords, the need to change them regularly, not to share them and to secure them appropriately?			(2) Validate that topic is adequately covered in CBT, awareness, guidance (3) Documented and established password management process	
9.3.1	Use of secret authentication information		Has IS (or an equivalent function) provided advice on how password security is achieved (e.g. using the annual IS CBT and/or intranet guidelines?)	Y	4	(1) Documented guidance on password management (2) Validate that topic is adequately covered in CBT, awareness, guidance	
9.3.1	Use of secret authentication information		Do IT Operations (or an equivalent function) review the password capabilities across all your IT systems?	Y	4		
9.3.1	Use of secret authentication information		Have IT Operations (or an equivalent function) implemented tools to ensure that strong passwords are enforced and supported using a single sign-on system?	Y	5		
9.4.1	Information access restriction	Access to information and application system functions should be restricted in accordance with	Do IT Operations (or an equivalent function) enforce the principle of least privilege to restrict access to systems as dictated by business	Y	4	(1) Documented and established approval process (at line manager level) to approve systems access before it is given (2) Documented and	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		the access control policy.	needs?			established online facilities exist to review access rights of employees on all systems.	
9.4.1	Information access restriction		Do IS (or an equivalent function) coordinate with the business to conduct regular network folder and system access reviews.	Y	3	(1) Documented and established folder review process (2) Reconciled folder access review reports	
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.	Has IS (or an equivalent function) defined OS logon controls to prevent unauthorized access to operating systems.	Y	4	(1) Documented and established OS access controls (2) Internal audit report findings (3) Sampling/On-site verification of OS access logs	
9.4.3	Password management system	Password management systems should be interactive and should ensure quality passwords.	Has IT Operations (or an equivalent function) implemented robust OS password management controls to enforce password quality, maintain a record of previous passwords and enforce password changes?	Y	5	(1) Documented and established process for user account password management, quality and strength (2) OS specific password configuration settings/parameters (3) Sampling/On-site verification of OS/application account logs	
9.4.4	Use of privileged	The use of utility programs that	Do IT Operations (or an equivalent function)	Y	5	(1) Documented and established process for	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	utility programs	might be capable of overriding system and application controls should be restricted and tightly controlled.	ensure that access to system utilities is restricted to authorised users?			restricting access to System utilities (2) Access configuration settings (3) Reconciled user access list (i.e. evidence that access is restricted to authorised users only.) (4) Evidence to support that employees with access to systems utilities do not have access to the application.	
9.4.4	Use of privileged utility programs		Do IT Operations (or an equivalent function) ensure that employees with access to systems utilities do not have access rights allowing them to update production application data?	Y	5	(1) Documented and established process for restricting access to System utilities (2) Access configuration settings (3) Reconciled user access list (i.e. evidence that access is restricted to authorised users only.) (4) Evidence to support that employees with access to systems utilities do not have access to the application.	
9.4.5	Access control to program source code	Access to program source code should be restricted.	Has IS (or an equivalent function) defined appropriate mechanisms to ensure that access to program source code is controlled (e.g. using a code version control	Y	4	(1) Documented and established source code maintenance process (2) Entitlement reports detailing who has access to critical source code (3) Examples of code	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			system)?			review reports by qualified external agencies (4) Manual reports/automated logs evidencing when and by whom access was requested/given	
10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	Has IS (or an equivalent function) documented and published a policy on the use of cryptographic controls to protect information classified as confidential or higher?	Y	4	(1) Documented and established risk assessment process (2) Sample review of new system requirements detailing encryption controls	
10.1.1	Policy on the use of cryptographic controls		Do IS (or an equivalent function) carry out a security risk assessment for new or system enhancements to determine if encryption controls are required and to specify what controls should be implemented?	Y	4		
10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	Do IT Operations (or an equivalent function) securely manage cryptographic keys to protect them from modification, loss, and/or disclosure?	N/A	1		
10.1.2	Key management		Has IS (or an equivalent function) defined the validity period for keys as	N/A	1	(1) Documented and established change controls process	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			determined by the technology used and the assessed risk employed with the information to be protected?			(2) Sample checking of documented evidence detailing when installation of software has occurred on critical systems.	
11.1.1	Physical security perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Does your company ensure that appropriate physical methods are used to prevent unauthorized access, damage or interference with any information you process, transport or otherwise handle?	Y	5	(1) On site verification of physical access controls e.g. CCTV, physical barriers, Concierge/reception desks, Security Guards, Card controlled entry systems	
11.1.1	Physical security perimeter		Has your Building Facilities (or an equivalent function) clearly defined (layered) security perimeters and provide protective controls commensurate to the criticality of the physical asset and the assessed risk?	Y	5	(1) On site verification of physical access controls e.g. CCTV, physical barriers, Concierge/reception desks, Security Guards, Card controlled entry systems	
11.1.1	Physical security perimeter		Do Building Facilities (or an equivalent function) provide a manned reception area to control physical access to your company's site(s) or building(s) so as to restrict access to authorised personnel only?	Y	5	(1) Presence of Concierge/reception desks (2) Visitors sign in and are met by a permanent company employee	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
11.1.1	Physical security perimeter		Has your Building Facilities (or an equivalent function) implemented a process to segregate physical access for those areas they are responsible for where multiple organisations occupy the same building?	Y	5	(1) Presence of Concierge/reception desks (2) Swipe card entry controls are applied to sensitive areas	
11.1.1	Physical security perimeter		Do IT Operations (or an equivalent function) ensure critical or sensitive information processing facilities are located in high security areas?	Y	5	(1) Access logs demonstrating that access to sensitive areas such as the computer room are restricted to authorised employees	
11.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Do Building Facilities (or an equivalent function) regularly monitor compliance with this control?	Y	5		
11.1.2	Physical entry controls		Do Building Facilities (or an equivalent function) ensure that front desk security personnel make any visitors sign in and ensure that visitors are met by a company employee before entering the facility?	Y	5	(1) Presence of Concierge/reception desks (2) Visitors sign in and are met by a company employee	
11.1.2	Physical entry controls		Do Line Managers monitor the mandatory	Y	5	(1) Incident management reports identifying	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			use of, and actively promote that employees visibly display their ID badges while on your company's facilities?			occurrences where badges are not worn. (2) Line Manager guidance/advisories that wearing ID badges is mandatory	
11.1.2	Physical entry controls		Do Building Facilities (or an equivalent function) manage the issuance of ID badges to all employees and oversee the issuance of temporary ID badges?	Y	5	(1) Presence of Concierge/reception desks (2) Visitors sign in and are met by a company employee (3) Temporary badges issued to non-visitors are logged and return of same is tracked/logged.	
11.1.2	Physical entry controls		Do Department Heads ensure (except for special concessions e.g. maintenance arrangements) that employees always escort visitors while on the premises?	Y	5	(1) Incident management reports identifying occurrences where badges are not worn.	
11.1.2	Physical entry controls		Do Building Facilities (or an equivalent function) ensure that the date, time of entry and time of departure of visitors are recorded at all times?	Y	5	(1) Presence of Concierge/reception desks (2) Visitors sign in and are met by a company employee (3) Completeness of visitors log covering date, entry and exit time of visitor, company and the name of the person being	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						visited.	
11.1.2	Physical entry controls		Do Building Facilities (or an equivalent function) regularly review, update and revoke access rights to high security areas?	Y	5	(1) Physical access rights lists (2) Reconciled access rights lists with access logs.	
11.1.2	Physical entry controls		Do IT Operations (or an equivalent function) restrict access to high security areas (e.g. Company Datacentres or computer rooms) only to authorised employees?	Y	5	(1) Physical access rights lists (2) Reconciled access rights lists with access logs.	
11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and applied.	Do Building Facilities (or an equivalent function) ensure (as appropriate) that logos on ID badges or building signage are removed so as to minimise information leakage relating to their nature or purpose?	Y	5	(1) On site verification of building signage	
11.1.3	Securing offices, rooms and facilities		Do Building Facilities (or an equivalent function) ensure that employees take account of the relevant health and safety regulations and standards?	Y	5	(1) Health and safety CBT (2) Health and safety incident reports	
11.1.3	Securing offices, rooms and facilities		Do Line Managers ensure that sensitive information is not readily	Y	4		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			accessible to unauthorised personnel?				
11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	Do Building Facilities (or an equivalent function) ensure that hazardous or combustible materials are stored at a safe distance from a high security area and that appropriate controls are in place to detect or prevent water/fire/smoke hazards?	Y	5	(1) On site verification of building/general environment and facilities: (a) Smoke/Fire/Intruder alarms (b) Fire suppression in key areas (2) Recording of fire alarm tests	
11.1.4	Protecting against external and environmental threats		Do Building Facilities (or an equivalent function) ensure that firefighting equipment is suitably placed, operational and has clearly visible signage?	Y	5	(1) On site verification of building/general environment and facilities	
11.1.4	Protecting against external and environmental threats		Do IT Operations (or an equivalent function) ensure that they protect fall-back equipment and back up media (e.g. encrypt and site at a safe distance from the main facility) to allow recovery from a disaster affecting a main site?	Y	5	(1) On site verification of building/general environment and facilities (2) Tape transfer logs (3) IT DR and Business Continuity plans	
11.1.5	Working in secure areas	Procedures for working in secure areas should be	Do Building Facilities (or an equivalent function) ensure that appropriate	Y	5	(1) On site verification that defined secure areas are implemented where	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		designed and applied.	guidance and controls are implemented for employees working in high security areas?			necessary i.e. lockable rooms and lockable filing storage. (2) Guidance is provided on the intranet for secure working areas	
11.1.5	Working in secure areas		Do Line Managers ensure that working in high security areas is supervised for safety reasons and to minimise opportunities for malicious activities?	Y	5		
11.1.5	Working in secure areas		Do Building Facilities (or an equivalent function) ensure that access to high security areas is restricted and that vacant high security areas are physically locked and periodically checked?	Y	5	(1) On site verification that defined secure areas are implemented where necessary i.e. lockable rooms and lockable filing storage. (2) Guidance is provided on the intranet for secure working areas	
11.1.5	Working in secure areas		Do Line Managers enforce restrictions on the use of cameras or mobile phones where access to sensitive data is possible?	Y	3		
11.1.5	Working in secure areas		Do Line Managers undertake regular checks to ensure that the Clear Desk Policy is in effect in their area of supervision?	Y	3	(1) Clear desk/secure working environment guidance (2) Incident management logs reporting Clear desk	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						infringements (3) Documented and implemented Clear desk sweep process.	
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 should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Do Building Facilities (or an equivalent function) ensure that access to delivery and/or loading areas from outside the building is restricted to authorised personnel?	Y	5	(1) On site verification that access via public areas (e.g. loading bay) is controlled by security guards/cameras	
11.1.6	Delivery and loading areas		Do Building Facilities (or an equivalent function) ensure that loading areas do not provide a means of access to any other part of the building and that all external access areas are segregated from any internal areas?	Y	5	(1) On site verification that access via public areas (e.g. loading bay) is controlled by security guards/cameras	
11.1.6	Delivery and loading areas		Do Building Facilities (or an equivalent function) ensure that materials are inspected for hazardous materials/threats before moving the consignment from the loading bay into the working area?	Y	5	(1) On site verification of working practice	
11.1.6	Delivery and loading areas		Do Building Facilities (or an equivalent function) ensure that, wherever possible, in-coming and out-going materials are	Y	5	(1) On site verification of working practice	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			physically segregated?				
11.1.6	Delivery and loading areas		Do Building Facilities (or an equivalent function) ensure that in-coming materials are recorded as defined and documented in their asset management procedures?	Y	5	(1) On site verification of working practice (2) Logging/registration of incoming materials	
11.2.1	Equipment siting and protection	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Do IT Operations (or an equivalent function) (or an equivalent function) locate critical equipment in high security, environmentally controlled data centres?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas	
11.2.1	Equipment siting and protection		Do IT Operations (or an equivalent function) site equipment so as to restrict unnecessary access to high security work areas?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas	
11.2.1	Equipment siting and protection		Do IT Operations (or an equivalent function) position information processing facilities that handle sensitive data, out of line of sight of unauthorised persons?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas	
11.2.1	Equipment siting and protection		Do Building Facilities (or an equivalent function) enforce robust	Y	5	(1) On site examination of secure and environmentally controlled	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			Datacentre controls to minimise the risk of potential threats such as fire, theft, chemical attack or vandalism?			data centres or areas	
11.2.1	Equipment siting and protection		Do IT Operations (or an equivalent function) prohibit eating, drinking and smoking in information processing facilities?	Y	5	(1) On site verification of employees behaviour at secure and/or environmentally controlled data centres or areas (2) Signage at information processing facilities.	
11.2.1	Equipment siting and protection		Do Building Facilities (or an equivalent function) ensure that environmental conditions that might adversely affect information processing facilities (e.g. temperature or humidity) are monitored and controlled?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas (2) Environmental logs of machine room humidity, temperature etc. …	
11.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	Do Building Facilities (or an equivalent function) ensure that all supporting utilities (electricity, heating, water supply, air conditioning are stable and adequate for the systems they support?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas (2) Operational incident reports detailing outages, spillages, flooding etc. …	
11.2.2	Supporting utilities		Do IT Operations (or an equivalent function) ensure that controls exist	Y	5	(1) On site examination of secure and environmentally controlled	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			to protect equipment from power failures through the provision of UPS devices and backup generators that conform to equipment manufacturer's specifications?			data centres or areas	
11.2.2	Supporting utilities		Do IT Operations (or an equivalent function) ensure that controls exist to inspect and test UPS devices and backup generators to ensure proper functioning?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas to review: (a) UPS devices are implemented (b) Generators are implemented and maintained (2) IT DR test plans and/or current results	
11.2.2	Supporting utilities		Do IT Operations (or an equivalent function) ensure that telecommunications equipment is connected using at least two diverse routes to allow failover?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas	
11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from	Do IT Operations (or an equivalent function) ensure that all network and power cabling going into information processing facilities is protected. (E.g. they are	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		interception, interference or damage.	buried, armoured or subject to adequate alternative protection)?				
11.2.3	Cabling security		Do IT Operations (or an equivalent function) ensure that network and power cabling is physically segregated to prevent unauthorised interception or damage?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas: labelled cabling	
11.2.3	Cabling security		Do IT Operations (or an equivalent function) ensure that they document and label cables (e.g. In comms cabinets) to minimise handling errors?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas: labelled cabling	
11.2.3	Cabling security		Do IT Operations (or an equivalent function) ensure that they restrict access to patch panels and cables rooms to authorised personnel?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas	
11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.	Do IT Operations (or an equivalent function) ensure that they maintain all equipment in accordance with the suppliers recommended service programme?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas (2) Equipment maintenance schedule.	
11.2.4	Equipment maintenance		Do IT Operations (or an equivalent function) ensure that they repair	Y	5	(1) On site examination of secure and environmentally controlled	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			and/or service equipment using authorised and qualified personnel?			data centres or areas (2) Equipment maintenance schedule.	
11.2.4	Equipment maintenance		Do IT Operations (or an equivalent function) ensure that the maintain records of all faults (suspected or actual) along with any corrective/preventative maintenance carried out?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas (2) Equipment maintenance schedule. (3) Regularly updated and current fault logs	
11.2.4	Equipment maintenance		Do IT Operations (or an equivalent function) ensure that they remove sensitive information from any equipment sent off-site for maintenance by a third party?	Y	5	(1) On site examination of secure and environmentally controlled data centres or areas (2) Regularly updated and current fault logs	
11.2.5	Removal of assets	Equipment, information or software should not be taken off-site without prior authorization.	Do IT Operations (or an equivalent function) undertake periodic spot checks to detect recording devices (e.g. key loggers) on company premises?	Y	2	(1) Key logger spot check report findings (2) Documented sweep process	
11.2.5	Removal of assets		Do IS participate in a formal process to approve and validate any requests to take data or equipment off-site?	Y	3	(1) Data transfer log stating that authority has been granted to remove data/information.	
11.2.5	Removal of assets		Does your CISO (or an equivalent function) approve any request to	Y	3	(1) Data transfer log stating that authority has been granted to remove	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			take equipment, information or removable media off the premises?			data/information.	
11.2.5	Removal of assets		Do IT Operations (or an equivalent function) ensure that they maintain records of all equipment removed off-site, with a return time limit, and an actual date of return?	Y	3	(1) Equipment maintenance log stating that authority has been granted to remove data/information. (2) IT Physical asset registers	
11.2.5	Removal of assets		Do Building Facilities (or an equivalent function) check that employees leaving with equipment are authorised to do so?	Y	4		
11.2.6	Security of equipment and assets off-premises	Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Do Departmental asset owners (or their delegate) authorise any request to remove confidential information?	Y	3	(1) Data transfer log stating that authority has been granted to remove confidential information.	
11.2.6	Security of equipment and assets off-premises		Do IS (or an equivalent function) conduct a risk assessment for any request to remove equipment or media from the company's premises?	Y	3	(1) Documented risk assessment process (2) Documented data classification process (2) Data transfer log stating risk assessment and data classification of information.	
11.2.6	Security of equipment and assets off-premises		Do IS (or an equivalent function) provide advice to all off-site workers regarding the use of laptops, USBs and	Y	3	(1) Documented guidance on remote working (2) Signed UAPs by all remote access workers (3) Intranet websites	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			remote access/teleworking?			providing access to guidance	
11.2.6	Security of equipment and assets off-premises		Do Line Managers ensure that all employees understand their responsibilities and have signed Acceptable Use Policies (AUPs) for Laptops, Remote access and use of removable media (e.g. USBs or DVDs) ?	Y	3	(1) Signed UAPs by all remote access workers (2) Intranet websites providing access to guidance	
11.2.6	Security of equipment and assets off-premises		Do IT Operations (or an equivalent function) implement controls to protect (e.g. encrypt) removable data storage devices (e.g. USBs, PDAs, iPhones or Blackberry's) using approved technologies?	Y	3	(1) Application device logs (registration, de-registration) (2) Application configuration screen-shots/files (3) Sample testing of removable media devices (4) Documented device management process	
11.2.6	Security of equipment and assets off-premises		Do IT Operations (or an equivalent function) periodically check IT controls for equipment taken off-site to ensure it has been appropriately secured?	Y	3	(1) On-site visit inspection of 3rd Party documentation (2) 3rd Party equipment destruction certificates (3) 3rd Party DR test results	
11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media should be	Do IT Operations (or an equivalent function) securely dispose of storage media containing	Y	5	(1) Documented data classification process (2) IT maintained equipment destruction	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	company data (i.e. it is physically destroyed) using certified disposal firms?			certificates	
11.2.7	Secure disposal or re-use of equipment		Do IT Operations (or an equivalent function) securely dispose of storage media devices?	Y	5	(1) Documented data classification process (2) 3rd Party equipment destruction certificates (3) On-site review of third party providing disposal/destruction capability	
11.2.8	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.	Do Departmental asset owners (or their delegate) authorise any request to remove confidential information?	Y	3	(1) Data transfer log stating that authority has been granted to remove confidential information.	
11.2.8	Unattended user equipment		Do IS conduct a risk assessment for any request to remove equipment or media from company premises?	Y	3	(1) Documented risk assessment process (2) Documented data classification process (2) Data transfer log stating risk assessment and data classification of information.	
11.2.8	Unattended user equipment		Do IS provide advice to all off-site workers regarding the use of laptops, USBs and/or remote access/teleworking?	Y	3	(1) Documented guidance on remote working (2) Signed UAPs by all remote access workers (3) Intranet websites providing access to guidance	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
11.2.8	Unattended user equipment		Do Line Managers ensure that all employees understand their responsibilities and have signed Acceptable Use Policies (AUPs) for Laptops, Remote access and use of removable media (e.g. USBs or DVDs)?	Y	3	(1) Signed UAPs by all remote access workers (2) Intranet websites providing access to guidance	
11.2.8	Unattended user equipment		Do IT Operations (or an equivalent function) implement controls to encrypt removable data storage devices (e.g. USBs or Blackberry's) using technologies approved by IT Operations (or an equivalent function)?	Y	3	(1) Application device logs (registration, de-registration) (2) Application configuration screen-shots/files (3) Sample testing of removable media devices (4) Documented device management process	
11.2.8	Unattended user equipment		Do IT Operations (or an equivalent function) periodically check IT controls for equipment taken off-site to ensure it has been appropriately secured?	Y	3	(1) On-site visit inspection of 3rd Party documentation (2) 3rd Party equipment destruction certificates (3) 3rd Party DR test results	
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	Do IS (or an equivalent function) publish guidelines mandating clear desks and screens re-inforced by an awareness programme and the annual	Y	4	(1) Clear screen policy (2) Documented guidance on clear screen policy (3) Validate that topic is adequately covered in CBT, awareness, guidance	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		facilities should be adopted.	awareness training (e.g CBT) ?			(4) employees self-assessment (5) InfoSec policy breach reports	
12.1.1	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.	Do IS (or an equivalent function) provide guidance on how information processing facilities should be managed and operated to ensure that they are always secured and operated correctly?	Y	3	(1) Documented guidance on the secure management of information processing facilities.	
12.1.1	Documented operating procedures		Do Line Managers document their operating procedures in relation to the usage of critical systems, as deemed appropriate by their Department Head? Note: these should be treated as formal documents and any changes must be authorised by an appropriate manager?	Y	3	(1) Defined responsibilities that explain how information processing facilities should be managed and operated. (2) Assigned responsibilities for the management and operation of the organization's information processing facilities. (3) Established procedures to operate and control the information processing facilities. (4) Documented procedures to ensure that information processing facilities are always secure and operated correctly.	
12.1.1	Documented		Do IT Operations (or an	Y	3	(1) Established procedures	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	operating procedures		equivalent function) ensure that they have documented system housekeeping and operating procedures for all critical company systems?			to operate and control the information processing facilities. (2) Documented procedures to ensure that information processing facilities are always secure and operated correctly.	
12.1.1	Documented operating procedures		Does Product Management (or an equivalent function) document procedures for system development, maintenance and testing?	Y	4		
12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.	Do Change Management (or an equivalent function) provide a forward schedule of change to IT Operations (or an equivalent function) on a weekly basis to detail significant changes and assess potential security impacts?	Y	3	(1) Documented and established change management process (2) Change management schedule	
12.1.2	Change management		Do Change Management (or an equivalent function) define change management responsibilities and procedures (e.g. roll back, root cause analysis) to ensure	Y	4	(1) Documented and established change management process (2) Documented Change management roles and responsibilities	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			satisfactory change to business processes?				
12.1.2	Change management		Does Change Management (or an equivalent function) ensure that a formal change control process is in place for all critical company systems?	Y	4	(1) Documented and established change management process	
12.1.3	Capacity management	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Do IT Operations (or an equivalent function) ensure that they monitor and optimise company systems to ensure that resources are available to meet business processing requirements and to detect problems in advance?	Y	4	(1) System performance reports and MI (2) Documented current and projected capacity/processing findings (3) Documented and established process for identifying and agreeing future capacity/processing requirements.	
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.	Do Product Management (or an equivalent function) define and document controls for the transfer of code and data from development to operational status?	Y	4	(1) Documented and established process for the transfer of code or data from development to operational status	
12.1.4	Separation of development, testing and operational environments		Does Product Management (or an equivalent function) ensure that development and test environments are separated from the	Y	5	(1) Documented test and production environments (2) On-site visit to validate location and logical/physical segregation of	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			production environment?			environments	
12.1.4	Separation of development, testing and operational environments		Does Product Management (or an equivalent function) ensure that sensitive production data is not copied to test system environments without prior data obfuscation/cleansing?	Y	5	(1) Documented Data handling/transfer guidelines (2) Documented and established data cleansing process (3) Data redacting/obfuscation tools (4) On-site validation of data used in test environments	
12.1.4	Separation of development, testing and operational environments		Does Product Management (or an equivalent function) implement controls to monitor potentially fraudulent activity where developers have access to the production environment?	N/A	5	(1) Use of data mining techniques to identify fraudulent activity	Developers do not have access to production environments
12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Have IS (or an equivalent function) established a formal policy prohibiting the use of unauthorised software to prevent employees obtaining files and software from external sources?	Y	3	(1) Unauthorised software use is coverage in CBT packages (2) Guidance on risks employed with the use of unauthorised materials (3) Guidance on controls that could be implemented to prevent the use of unauthorised materials e.g. content monitoring, AV scanning, USB access restrictions and USB	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						encryption.	
12.2.1	Controls against malware		Do Department Heads ensure that authorised users of DVDs/CDs and USB devices have scanned these using their local AV software before opening or processing any files or data on them.	Y	3	(1) Automated controls to scan USB/DVD/CD devices (2) Centralised scan logs	
12.2.1	Controls against malware		Has IT Operations (or an equivalent function) deployed (at least 2) different vendor AV products for scanning emails and is scanning automatically performed prior to delivery?	Y	5	(1) Documented configurations for AV products (2) AV detection/quarantine reports (3) AV incident reporting/MI (4) AAV Architecture diagram	
12.2.1	Controls against malware		Has IT Operations (or an equivalent function) implemented AV controls on all exchange servers, gateways, web servers, general servers and other endpoints?	Y	5	(1) Documented infrastructure installation notes and/or configurations for AV products (2) AV detection/quarantine reports (3) AV incident reporting/MI	
12.2.1	Controls against malware		Do IT Operations (or an equivalent function) configure AV to	Y	5	(1) Documented installation notes and/or configurations for AV	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			automatically scan DVD/CDs and other removable media (e.g. USB sticks)?			products (2) AV detection/quarantine reports (3) AV incident reporting/MI	
12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	Do IT Operations (or an equivalent function) back up data on a daily basis and that tapes are verified during annual or biannual DR tests?	Y	5	(1) Daily backup log/schedule (2) Periodic DR test results (3) Scheduled testing of file restoration (4) On-site verification that data real-time replication occurs	
12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Has IS (or an equivalent function) identified critical audit logs and assigned a retention period in accordance with local legislation/regulations on data retention (as directed by local Legal and Compliance SMEs in your company)?	Y	5	(1) List of audit logs (2) Data retention specification for audit logs (3) Sample of audit log content	
12.4.2	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	Has IT Operations (or an equivalent function) established controls to protect log information from general view/update/delete access?	Y	3	(1) System monitoring configuration/set up (2) Documented and established system log access review process (3) Documented and established role based	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						access controls	
12.4.2	Protection of log information		Has IS (or an equivalent function) identified critical audit logs and assigned a retention period in accordance with local legislation on data retention (as directed by local Legal and local Compliance SMEs)?	Y	5	Duplicate	
12.4.2	Protection of log information		Has IT Operations (or an equivalent function) implemented controls to verify that that logging is switched on and that logs are protected from administrator modification or deletion?	Y	4	(1) System monitoring configuration/set up (2) Documented and established privileged log access review process (3) Documented and established log on-line and off-line retention controls	
12.4.3	Administrator and operator logs	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	Do IT Operations (or an equivalent function) identify all critical business systems for which administrator logging is applied?	Y	3	(1) List of systems to which administrator access controls are applied	
12.4.3	Administrator and operator logs		Do IT Operations (or an equivalent function) implement checks to verify that that administrator/operator activity logging is switched on and that logs are protected from	Y	4		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			administrator modification/deletion?				
12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	Do IT Operations (or an equivalent function) ensure that the clocks on all critical systems are synchronised with a reliable time source?	Y	3	(1) On-site verification that system clocks are synchronised (2) Documented and established procedures for use of NTP (3) NTP time service configuration (4) Reconciled events using a representative log sample.	
12.4.4	Clock synchronisation		Do IT Operations (or an equivalent function) monitor systems to ensure that clock synchronisation has taken place?	Y	3	(1) On-site verification that system clocks are synchronised (2) Documented and established procedures for use of NTP (3) NTP time service configuration (4) Reconciled events using a representative log sample.	
12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.	Have Change Management (or an equivalent function) documented a change management process to control the installation of operational software/code on critical systems?	Y	4	(1) Documented and established change controls process (2) Sample checking of documented evidence detailing when code has been released on critical systems	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
12.6.1	Management of technical vulnerabilities	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.	Do IS (or an equivalent function) monitor that vulnerabilities on critical or externally facing systems are regularly patched?	Y	5	(1) Review of contracts to demonstrate IPR has been accommodated	
12.6.1	Management of technical vulnerabilities		Do IT Operations (or an equivalent function) regularly patch vulnerabilities on critical or externally facing systems?	Y	5	(1) Asset lists of critical external systems - OS release, versions, patch levels (2) OS Vulnerability assessment reports (3) Planned/implemented patch schedule	
12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented.	Have Change Management (or an equivalent function) documented a change management process to control the installation of operational software/code on critical systems?	Y	5	(1) Documented and established change controls process (2) Sample checking of documented evidence detailing when code has been released on critical systems	
12.6.2	Restrictions on software installation		Do IT Operations (or an equivalent function) adhere to the agreed change management procedures to enforce the controlled release of operational software/code on critical systems?	Y	5	(1) Documented and established software roll-back process (2) Sample checking of documented evidence detailing roll-back occurrences and circumstances	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
12.6.2	Restrictions on software installation		Do IT Operations (or an equivalent function) implement rollback procedures covering the installation of operational software/code on critical systems?	Y	5	(1) Asset repository containing all supported software (2) Valid licenses for all listed software	
12.6.2	Restrictions on software installation		Do IT Operations (or an equivalent function) always provide services using supported and appropriately licensed software?	Y	5	(1) General policy stating that live data is not to be used. (2) Live data is redacted/anonymised to scramble personal elements. (3) Documented and established procedures detailing how access to test system data is controlled (4) Manual reports or automated logs detailing instances where live data has been extracted to a test system. (5) Where unavoidable, a risk assessment on the use of live data is to be conducted. (6) Evidence that review and approval for live-data testing (and applied controls) has occurred and been provided by qualified SMEs	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
13.1.1	Network controls	Networks should be managed and controlled to protect information in systems and applications.	Do IT Operations (or an equivalent function) implement processes that allow for the management of remote facilities?	Y	5	(1) Documented and established process for the management of remote facilities. (2) On-site verification/demonstration that off-site management is possible.	
13.1.1	Network controls		Do IT Operations (or an equivalent function) implement “private" network links to secure the data in transit between company sites.	Y	5	(1) Documented network configurations (2) Sample network device configuration files (3) Network Performance test reports	
13.1.2	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.	Do IT Operations (or an equivalent function) implement controls to manage networks securely?	Y	5	(1) Documented network configurations (2) Sample network security device configuration files	
13.1.3	Segregation in networks	Groups of information services, users and information systems should be	Do IT Operations (or an equivalent function) segregate Wireless and internet only networks from the core company	Y	4	(1) Configuration settings/parameters for Wireless Access points devices (2) Internal audit report	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		segregated on networks.	network infrastructure?			findings (3) Penetration test results/reports for the wireless infrastructure (4) On-site verification of wireless infrastructure, IP address ranges and network logs	
13.2.1	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.	Has IS (or an equivalent function) published standards and guidelines for the safe and secure transportation of data?	Y	4	(1) Documented and established secure transportation of data standards and guidelines	
13.2.1	Information transfer policies and procedures		Has IS (or an equivalent function) published policies for the acceptable usage of electronic communication facilities?	Y	4	(1) Documented and established secure transportation of data standards and guidelines	
13.2.1	Information transfer policies and procedures		Has IS (or an equivalent function) provided training and guidance to all employees on the need to secure telephone calls and to protect against eavesdropping (e.g. when in public areas) ?	Y	3	(1) Verification that topic is adequately enforced in CBT (2) Minuted departmental meetings in which guidance is an agenda item	
13.2.1	Information transfer policies and procedures		Has IT Operations (or an equivalent function) implemented email encryption controls/capabilities for	Y	4	(1) Documented and established encryption of email guidelines (2) On-site sample verification of email	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			external emails containing sensitive information?			encryption process (3) Verification of email control tool configuration files (4) Verification of email control tool logs	
13.2.1	Information transfer policies and procedures		Have IT Operations (or an equivalent function) implemented controls to prevent the automatic forwarding of messages to external (e.g. personal) email addresses?	Y	3	(1) Documented and established use of email policy (e.g. AUP) (2) On-site sample verification of email blocking process (3) Verification of email blocker configuration files (4) Verification of email blocker tool logs	
13.2.2	Agreements on information transfer	Agreements should address the secure transfer of business information between the organization and external parties.	Has IS (or an equivalent function defined protocols for the exchange of information between your company and external parties; this includes notifying the recipient on dispatch, as well as providing traceability and non-repudiation of the exchange.	Y	3	(1) Documented and established exchange of information process. (2) Document transfer log (3) Guidance on security best practices for data exchange	
13.2.2	Agreements on information transfer		Has IS (or an equivalent function) defined responsibilities and liabilities in the event of information security incidents - such as data	Y	4	(1) Documented (and agreed) roles and responsibilities	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			loss.				
13.2.2	Agreements on information transfer		Has Product Management (or an equivalent function) established a formal process so that the exact nature, existence and quality of the exchange agreements is clear and unambiguous such as labelling for sensitive/critical information, packaging standards, notification of dispatch/receipt, cryptographic controls, licensing and courier identification protocols?	Y	3	(1) Documented and established exchange of information process. (2) Document transfer log (3) Guidance on security best practices for data exchange: labelling for sensitive/critical information, packaging standards, notification of dispatch/receipt, cryptographic controls, licensing and courier identification protocols.	
13.2.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected.	Has IS (or an equivalent function) mandated that external Instant Messaging is prohibited?	Y	4	(1) Prohibited activities identified in the IS standards and guidelines	
13.2.3	Electronic messaging		Has IS (or an equivalent function) mandated in the Information Security standards that all emails leaving the organisation must contain legal disclaimers?	Y	5	(1) Sample verification of email disclaimers	
13.2.3	Electronic messaging		Has IS (or an equivalent function) mandated in the Information Security standards that remote	Y	4	(1) Requirement stated in the IS standards and guidelines	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			access to company services requires two-factor authentication?				
13.2.3	Electronic messaging		Has IT Operations (or an equivalent function) implemented controls (e.g. encrypted in software or sent via private or encrypted links) so that emails containing confidential information are protected?	Y	4	(1) Documented and established process for the deployment of controls to encrypt emails. (2) Sample verification of encrypted emails	
13.2.3	Electronic messaging		Has IT Operations (or an equivalent function) implemented controls so as to content scan every email to determine if it contains unencrypted confidential information?	Y	4		DLP has been implemented for the Classified Employees who have an access to client data
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 should be identified, regularly reviewed and documented.	Do Line Managers liaise with HR to ensure that confidentiality agreements have been signed by company employees?	Y	4	(1) Signed confidentiality agreements	
13.2.4	Confidentiality or non-disclosure agreements		Has Group Procurement (or an equivalent function) identified the need for a Non-disclosure Agreements(NDA) for	Y	4	(1) Documented NDAs	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			Third parties - identifying what is to be protected, for how long, and detailing mutual responsibilities on contract termination and breach?				
13.2.4	Confidentiality or non-disclosure agreements		Has Group Legal (or an equivalent function) provided a standard NDA form with terms including what is to be protected, for how long, and mutual responsibilities on contract termination and breach?	Y	4	(1) Standardised NDA templates	
13.2.4	Confidentiality or non-disclosure agreements		Is it your company's policy that all contracts that need to be signed by the sponsoring Business Area and Group Legal to sign off respectively that the contract is commercially and legally suitable before it is signed?	Y	5	(1) Legal NDA sign-off process (2) Sample signed-off NDAs.	
13.2.4	Confidentiality or non-disclosure agreements		Do Group Compliance (or an equivalent function) review legal agreements relating to data processing and provide sign-off as required by the	Y	3	(1) Compliance legal agreement sign-off process (2) Sample signed-off legal agreements.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			business?				
13.2.4	Confidentiality or non-disclosure agreements		Does Group Procurement (or an equivalent function) ensure that appropriate NDAs are applied to all procurement / contractual activity?	Y	4	(1) NDAs included in the business's Procurement and/or contractual process	
13.2.4	Confidentiality or non-disclosure agreements		Has IS (or an equivalent function) defined a process to interface with the group incident management process to report and manage situations where the disclosure of confidential information occurs?	Y	5	(1) Documented company incident management process (2) Incident tracking logs to evidence that the incident process has been followed.	
13.2.4	Confidentiality or non-disclosure agreements		Does the IS Governance body chairman ensure that the Group Procurement and Group Legal departments are represented on the IS Governance body so as to advise on legal or contractual issues affecting Information Security?	Y	3	(1) IS Forum (or its equivalent) membership list.	
13.2.4	Confidentiality or non-disclosure agreements		Does your information security policy and relevant contracts dictate that your company has the right to audit and	Y	4	(1) Appropriate audit/monitoring clause in contract.	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			monitor any activity that may involve classified information?				
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.	Has Product Development (or an equivalent function) adopted a risk based process when evaluating software packages for business applications to ensure that any security requirements and controls applied reflect the business value of the information assets involved, and the potential business damage that might result from a failure or compromise?	Y	3		
14.1.1	Information security requirements analysis and specification		Do IS (or an equivalent function) specify controls and security requirements at an early stage of the requirements definition process commensurate with the value of the information assets and the potential damage that might result from compromise of the system?	Y	3	(1) Documented and established processes showing how IS requirements are embedded in the project life-cycle. (2) Sample project documentation showing IS requirements	
14.1.1	Information		Has Product	Y	3	(1) Documented input	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	security requirements analysis and specification		Development (or an equivalent function) made use of independently evaluated and certified products approved by the company's Strategy and Technical Architect (or equivalent) function?			validation controls (2) Test data and test results used to check effectiveness of input validation controls.	
14.1.2	Securing application services on public networks	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Do Business areas ensure that, where applicable, robust user registration and authentication processes have been established for e-commerce applications?	Y	5		
14.1.3	Protecting application services transactions	Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized	Do Department Heads ensure that employees do not make confidential company data accessible to the public (e.g. facing web sites or on personal blogs, or twitter)?	Y	4	(1) Any request to expose company data to the public must be validated by line managers and by the IS function	
14.1.3	Protecting application services transactions		Has IT Operations (or an equivalent function) implemented robust authentication controls for access to/by third party systems?	Y	3	(1) Documented and established (strong) authentication controls. (2) Access control review reports	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
14.1.3	Protecting application services transactions	disclosure, unauthorized message duplication or replay.	Has IT Operations (or an equivalent function) implemented encryption and/or message integrity controls to protect confidential data in transit for third party systems?	Y	4	(1) Documented and established message integrity controls	
14.1.3	Protecting application services transactions		Do Business departments use digital signatures (or an equivalent data integrity mechanism) for all on-line transactions?	Y	3		
14.1.3	Protecting application services transactions		Have Business departments implemented a process to verify that all on-line transactions are appropriately protected?	Y	3		
14.2.1	Secure development policy	Rules for the development of software and systems should be established and applied to developments within the organization.	Has IS (or an equivalent function) published rules for the development of applications and system software?	Y	3	(1) Documented and established risk assessment process for software development and application security (2) Sample review of new system requirements detailing IS controls	
14.2.2	System change control procedures	Changes to systems within the development lifecycle should be	Does Change Management (or an equivalent function) define the formal change	Y	4	(1) Documented and established change management process (2) Documented asset	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		controlled by the use of formal change control procedures.	control procedures needed to manage change?			owner and assets list (3) Authorised change test sign-offs are obtained prior to implementation (4) Evidence that the business impact of any change is managed appropriately - gap analysis, stakeholder review.	
14.2.2	System change control procedures		Has IT Operations (or an equivalent function) implemented agreed formal change procedures to manage changes to IT systems?	Y	4	(1) Documented and established change risk assessment process (2) Sample change risk assessments	
14.2.2	System change control procedures		Has IT Operations (or an equivalent function) established commensurate procedures to undertake risk assessments prior to change implementation?	Y	4	(1) Sample of authorised change/test sign-offs are obtained prior to implementation (2) Change test results	
14.2.2	System change control procedures		Has IT Operations (or an equivalent function) established procedures to review and sign-off change test results prior to implementation?	Y	4	(1) Documented and established change management process (2) Documented asset owner and assets list (3) Authorised change test sign-offs are obtained prior to implementation (4) Evidence that the business impact of any change is managed	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						appropriately - gap analysis, stakeholder review.	
14.2.2	System change control procedures		Has IT Operations (or an equivalent function) established procedures to monitor compliance with change control for all critical projects?	Y	4		
14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Do IT Operations (or an equivalent function) regularly monitor operating system vulnerabilities and that arising issues are acted upon in a timely fashion (e.g. patches are applied to fix issues)?	Y	4	(1) Asset lists of critical systems - OS release, versions, patch levels (2) OS Vulnerability assessment reports (3) Planned/implemented patch schedule	
14.2.3	Technical review of applications after operating platform changes		Do Product Development (or an equivalent function) test applications (although not specifically for security vulnerabilities) before implementing major O/S upgrades?	Y	4	(1) Sample Test plans (2) Sample Test results (3) Vulnerability patch reports/MI	
14.2.3	Technical review of applications after operating platform changes		Do IT Operations (or an equivalent function) solicit participation and/or guidance from Strategy and Architecture and Change Management (or equivalent functions)	Y	3	(1) SME and stakeholder sign-off of test plans	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			prior to any major O/S upgrades?				
14.2.4	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.	Do IT Operations (or an equivalent function) log all modifications to software packages so as to ensure that modifications are limited to controlled instances?	Y	4		
14.2.4	Restrictions on changes to software packages		Do IT Operations (or an equivalent function) ensure that only IT staff are used to support system modifications or upgrades?	Y	5	(1) Software change log (2) Software change approval records	
14.2.5	Secure system engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.	Has IT (or an equivalent function) documented and implemented principles for engineering secure systems?	Y	3	(1) Documented and established risk assessment process for software development and application security (2) Sample review of new system requirements detailing IS controls (3) Hardened system build standards	
14.2.6	Secure development environment	Organizations should establish and appropriately protect secure development environments for system	Has IS (or an equivalent function) documented and published requirements and guidance for engineering secure systems?	Y	3	(1) Documented and established risk assessment process for software development and application security (2) Sample review of new system requirements	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		development and integration efforts that cover the entire system development lifecycle.				detailing IS controls	
14.2.7	Outsourced development	The organization should supervise and monitor the activity of outsourced system development.	Has IS (or an equivalent function) documented an agreed software escrow policy to ensure that software development is supervised and monitored when development activities are outsourced?	Y	5	(1) Provision of data leakage guidance (2) System logs evidencing that outbound email is monitored for prohibited file types e.g. Images (3) AV software logs/reports (4) Ad hoc checks on emails containing sensitive data.	
14.2.7	Outsourced development		Where applicable, do Group Legal (or an equivalent function) provide advice on software escrow to ensure that legal requirements are included in contracts with third parties to protect the company's right to use said software if a supplier becomes insolvent or subject to a material breach?	Y	5	(1) Oversight of major IT changes is in place and captured (2) Escrow arrangements are implemented (3) Code/Audit reviews and checks in place (4) UAT takes place on systems (5) Review of contracts to demonstrate IPR has been accommodated	
14.2.8	System security	Testing of security functionality	Does Product Development (or an	Y	5	(1) Test scripts and results	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	testing	should be carried out during development.	equivalent function) perform rigorous testing during the development phase of the SDLC?				
14.2.8	System security testing	Testing of security functionality should be carried out during development.	Do IS (or an equivalent function) arrange for independent testing of high risk applications to ensure that the system works as specified?	Y	4	(1) Independent software review reports	
14.2.9	System acceptance testing	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.	Do IT Operations (or an equivalent function) ensure that they perform levels of testing on new or changed systems?	Y	3	(1) Documented and established process for new/changed systems acceptance (2) Changed/new system acceptance test plan results (3) Test plans covering: system testing, integration testing, user acceptance testing, business acceptance testing and non-functional testing.	
14.2.9	System acceptance testing		IT Operations (or an equivalent function) will monitor compliance for key business activities	Y	3		
14.3.1	Protection of test data	Test data should be selected carefully, protected and controlled.	Has IS (or an equivalent function) defined and documented any mechanisms needed to support the use of non-live data on test	Y	4	(1) Documented and established procedures to redact/anonymise personal data. (2) Data redaction configuration	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			systems?			(3) Sample redaction data output	
14.3.1	Protection of test data		Has IT Operations (or an equivalent function) implemented mechanisms needed to anonymise or scramble personal data elements whenever live data is used on test systems?	Y	5	(1) Manual reports or automated logs detailing instances where live data has been extracted to a test system.	
14.3.1	Protection of test data		Does Product Development (or an equivalent function) have mechanisms in place to control and log the extraction of live data into test systems?	Y	5	(1) Where unavoidable, a risk assessment on the use of live data is to be conducted. (2) Evidence that review and approval for live-data testing (and applied controls) has occurred and been provided by qualified SMEs	
14.3.1	Protection of test data		Do IS (or an equivalent function) review and sign-off the supporting controls and the use of live data for testing purposes for all significant projects?	Y	5	(1) Documented and established version control process (2) Sample logs/extracts from versioning control tool	
15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access	Do IS (or an equivalent function) review and sign-off the supporting controls needed to secure the use of live data for testing purposes	Y	3		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		to the organization's assets should be agreed with the supplier and documented.	for all significant projects?				
15.1.2	Addressing security within supplier agreements	All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Do IS (or an equivalent function) work with third parties to determine how any information/data security is managed, to identify what level of security risks exist, and to agree what controls need to be applied?	Y	3	(1) Risk assessment of third party access (2) List of agreed IS controls to be applied	
15.1.2	Addressing security within supplier agreements		Does Group Procurement (or an equivalent function) include the security requirements in any third party agreement, including liability of each party (and down-stream third parties if appropriate)?	Y	3	(1) Documented security requirements in third party agreements (2) Documented liabilities for all involved parties	
15.1.2	Addressing security within supplier agreements		Do Group Legal (or an equivalent function) engage with your Group Procurement function to identify where provisions (including liability) relating to information security are required in any contract with a third	Y	3	(1) Documented liabilities for all involved parties	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			party (including such provisions to be included in down-stream sub-contracts entered into by said third party) and are appropriate provisions included in the contract?				
15.1.2	Addressing security within supplier agreements		Has the CISO (or equivalent function) implemented procedures and plans necessary to manage the transition of IT services with any IT service provider; including plans to manage changes (e.g. renegotiation or termination) of the agreement?	Y	4	(1) IT Service transition plans	
15.1.2	Addressing security within supplier agreements		Does the CISO approve the sign-off of legal contracts involving IT solutions or Information Security?	Y	4	(1) Senior IT Management sign-off of IT related legal contracts	
15.1.3	Information and communicatio n technology supply chain	Agreements with suppliers should include requirements to address the information security risks associated with information and communications	Has IS (or an equivalent function) established a third party risk assessment process to identify what facilities are accessed by the third party, their level of sensitivity, business criticality and what controls are needed to	Y	4	(1) Third party risk assessment process (2) Non-policy compliance remediation plans	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		technology services and product supply chain.	mitigate any issues identified.				
15.1.3	Information and communication technology supply chain		Does Procurement (or an equivalent function) review, assess and sign-off all new external party relationships before access is granted to company facilities or information?	Y	3		
15.1.3	Information and communication technology supply chain		Does Procurement (or an equivalent function) define the contractual obligations and liabilities to be adhered to by any external party? Third party must sign the contract or a suitable NDA prior to granting access to company facilities or information?	Y	3		
15.1.3	Information and communication technology supply chain		Does your company ensure that any contract (including NDAs) that need to be signed by both the sponsoring Business Area and Group Legal are commercially and legally suitable before signing?	Y	5	(1) Documented Request for Document Execution process	
15.1.3	Information and communicatio		Do Group Procurement (or an equivalent function) conduct Dunn &	Y	2	(1) Evidence that D&B credit check reports have been conducted	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	n technology supply chain		Bradstreet (D&B) credit checks on key external third parties that have access to company facilities or data?				
15.1.3	Information and communicatio n technology supply chain		Do IS (or an equivalent function) define practices and procedures to manage security incidents and the potential damages resulting from third party access to your company's information facilities?	Y	3	(1) Documented Incident Management process (2) Incident management logs/reports/MI (3) Third party risk assessment	
15.2.1	Monitoring and review of supplier services	Organizations should regularly monitor, review and audit supplier service delivery.	Do IS (or an equivalent function) ensure that key 3rd parties produce a monthly scorecard reporting on Information Security control effectiveness?	Y	4	(1) Monthly scorecard/report/MI showing policy compliance	
15.2.1	Monitoring and review of supplier services		Do IS (or an equivalent function) conduct periodic meetings with 3rd party Information Security managers to review their control effectiveness?	Y	3	(1) Assurance sample checking to validate the information provided in scorecards	
15.2.1	Monitoring and review of supplier services		Do Internal Audit (or an equivalent function) have oversight of internal and external 3rd party audits	Y	3	(1) Annual external audit report and remediation tracking	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			so as to allow scope and results to be reviewed and to monitor progress against remediation plans?				
15.2.1	Monitoring and review of supplier services		Do IS (or an equivalent function) participate in the 3rd party technology planning meetings to ensure that information security developments/improvements are considered?	Y	3	(1) Technology planning steering groups findings (2) Security improvement plan detailing developments or improvements	
15.2.1	Monitoring and review of supplier services		Do Group Procurement (or an equivalent function) with support from your Group Legal department ensure that NDAs are in place with 3rd parties prior to service provision and/or engagement?	Y	4	(1) Appropriate NDAs are in place.	
15.2.1	Monitoring and review of supplier services		Has IS (or an equivalent function) established a clearly defined reporting process for 3rd parties to provide information relating to security incident response/ reports, change management, and vulnerability identification?	Y	3	(1) Documented and established security incident response process. (2) Documented and established vulnerability assessment process	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
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, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Is the CISO (or an equivalent function) required to approve the sign-off of any contractual changes involving IT solutions or Information Security?	Y	5		
15.2.2	Managing changes to supplier services		Do IT Operations (or an equivalent function) review and approve any changes to the 3rd party services that involve IT solutions or Information Security?	Y	3	(1) All changes to the 3rd party services are documented, reviewed and approved by IT Operations (or an equivalent function)	
15.2.2	Managing changes to supplier services		Do IS (or an equivalent function) risk assess any changes to the provision of the 3rd party services involving IT solutions or Information Security?	Y	3	(1) Documented and established risk assessment process (2) Documented change request/management process	
16.1.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.	Do IS (or an equivalent function) establish procedures to handle different types of information security incident such as: loss of service, malicious code, Denial of service, data integrity failures, confidentiality breaches and misuse?	Y	5	(1) Documented and established InfoSec event/incident management process (2) Defined InfoSec roles and responsibilities	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
16.1.1	Responsibilities and procedures		Has IT Operations (or an equivalent function) established procedures to gather audit trails and forensic evidence?	Y	4	(1) Documented and established weight of evidence process (2) Sample cases invoking of forensic gathering (3) Samples of forensic evidence to demonstrate process	
16.1.1	Responsibilities and procedures		Do IS (or an equivalent function) maintain appropriate external and industry contacts to assist with intra/inter jurisdiction security incident management?	Y	3	(1) Current contact lists of cross border security groups (e.g. ukCERT, aeCERT, SANS) (2) Current list of emergency response website that are monitored	Ebix maintains contact with multiple vendors in the security space to assist with everything from vulnerability testing to Pen testing and incident management. Most of those items are addressed in house but we have 3rd party resources available if required.
16.1.1	Responsibilities and procedures		Has IT Operations (or an equivalent function) established procedures to recover from security breaches and to correct system failures?	Y	3	(1) Documented and established InfoSec event/incident management process (2) Defined incident response roles and	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
						responsibilities	
16.1.2	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.	Has IS (or an equivalent function) implemented a formal information security event/incident reporting procedure that includes a feedback process, reporting forms, expected reportee behaviour on discovering an incident and MI reports/analysis.	Y	3	(1) Documented and established InfoSec incident reporting process (2) Incident reports/MI (3) Info Sec incident guidance	
16.1.2	Reporting information security events		Do Group Compliance (or an equivalent function) oversee the compliance breach process and support the Business owner on actual or potential breaches?	Y	3	(1) Compliance R&Rs (2) InfoSec incident/policy compliance breach escalation process	
16.1.2	Reporting information security events		Does the Group Problem Management team (or an equivalent function) evaluate each incident and identify a business owner who must then liaise between company SMEs during the lifetime of said incident?	Y	3	(1) Incident reports/MI (2) Info Sec incident guidance	
16.1.2	Reporting information security events		Has IS (or an equivalent function) implemented assurance checks that 3rd parties can operate	Y	3	(1) Documented and established InfoSec incident reporting process (2) Incident reports/MI	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			under their own security incident management process?			(3) Info Sec incident guidance	
16.1.2	Reporting information security events		Do IS (or an equivalent function) manage and publish a contact email address for reporting suspected security events/ incidents?	Y	3	(1) Documented and established/published InfoSec contact email address	
16.1.2	Reporting information security events		Do IS (or an equivalent function) provide guidance and clarity around risks, incidents and scales of breaches, example incidents, and improve awareness of responsibilities and processes?	Y	3	(1) Info Sec incident guidance covering risks, incidents and scales of breaches, example incidents, and improve awareness of responsibilities and processes (2) Covered in InfoSec CBT packages	
16.1.2	Reporting information security events		Do IS (or an equivalent function) provide guidance to ensure that employees report information security events and weaknesses to the designated point of contact?	Y	3	(1) Published and established Info Sec incident guidance	
16.1.2	Reporting information security events		Does your IS Governance body monitor, track and escalate (as required) all Information Security incidents?	Y	3	(1) Incident reports/MI (2) Evidence of info Sec incident tracking/follow up/escalation	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
16.1.2	Reporting information security events		Has Group HR (or an equivalent function) established a formal disciplinary process for dealing with employees who commit security breaches?	Y	4	(1) Documented and established disciplinary procedures	
16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.	Do Line Managers ensure that all employees understand that they are required to report any observed or suspected security incident, or weakness in systems, facilities or services as quickly as possible?	Y	4	(1) Service desk reports/logs (2) Minuted line manager meetings in which subject is minuted as an agenda item 3) Evidenced by CBT, AUPs and IS guidance published on the Intranet. 4) Group Risk Incident Management reports/MI 5) Minor Security incident management reports/MI	
16.1.4	Assessment of and decision on information security events	Information security events should be assessed and it should be decided if they are to be classified as information security incidents.	Do Line Managers ensure that their employees understand that they must never test or attempt to prove a security weakness when accessing the company's information systems and services?	Y	3	(1) Service desk reports/logs (2) Minuted line manager meetings in which subject is minuted as an agenda item 3) Evidenced by CBT, AUPs and IS guidance published on the Intranet.	
16.1.4	Assessment of and decision on		Do IS (or an equivalent function) manage and publish a generic	Y	3		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	information security events		Security contact email address for reporting security events and/or incidents?				
16.1.4	Assessment of and decision on information security events		Do IS (or an equivalent function) monitor and track closure of Information Security incidents?	Y	3	(1) Documented and established security event/incident reporting process (2) Security Incident Report/MI	
16.1.5	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Have IS (or an equivalent function) established procedures to handle different types of information security incident such as: loss of service, malicious code, Denial of service, data integrity failures, confidentiality breaches and misuse?	Y	3	(1) Documented and established InfoSec event/incident management process (2) Defined InfoSec roles and responsibilities	
16.1.5	Response to information security incidents		Have IT Operations (or an equivalent function) established procedures to gather audit trails and maintain forensic evidence in a secure manner?	Y	4	(1) Documented and established weight of evidence process (2) Sample cases invoking of forensic gathering (3) Samples of forensic evidence to demonstrate process	
16.1.5	Response to information security incidents		Do IS (or an equivalent function) maintain appropriate external and industry contacts to	Y	4	(1) Current contact lists of cross border security groups (e.g. ukCERT, aeCERT, SANS)	Ebix maintains contact with multiple vendors in the

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			assist with intra/inter jurisdiction security incident management?			(2) Current list of emergency response website that are monitored	security space to assist with everything from vulnerability testing to Pen testing and incident management. Most of those items are addressed in house but we have 3rd party resources available if required.
16.1.5	Response to information security incidents		Do IT Operations (or an equivalent function) establish procedures to recover from security breaches and to correct system failures?	Y	3	(1) Documented and established InfoSec event/incident management process (2) Defined incident response roles and responsibilities	
16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	Has IS (or an equivalent function) established procedures to analyse information security events/incidents to help identify recurring or high impact incidents and to develop enhanced controls to reduce similar information exposures going forward?	Y	3	(1) Current list of information security events/incidents (2) Root cause analysis work to help learn from incidents (3) Documented set of improvements/recommendations to enhance the InfoSec incident management process	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
16.1.7	Collection of evidence	The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Is IS (or an equivalent function) responsible for the collection of evidence in relation to incidents leading to legal action?	Y	3	(1) Documented and established weight of evidence process	
16.1.7	Collection of evidence		Where an information security incident involves actual or potential litigation (or other forms of dispute resolution) does your company policy require Group Legal to be notified and does Group Legal provide advice, as necessary, on relevant issues including the obtaining of evidence?	Y	3	(1) Legal notifications/evidence of engagement with legal for incidents involving litigation	
16.1.7	Collection of evidence		Has IS (or an equivalent function) with advice from Group Legal and Group HR , documented and established robust procedures for collecting evidence and to ensure that these are followed?	Y	2	(1) Documented and established InfoSec event/incident management process (2) Defined incident response roles and responsibilities	
16.1.7	Collection of evidence		Do IT Security (or an equivalent function)	Y	4		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			ensure that company information systems comply with the local codes of practice for the production of admissible evidence?				
16.1.7	Collection of evidence		Do IT Security (or an equivalent function) ensure that they can provide robust 'chain and/or weight of evidence' such that your company can demonstrate that any recorded evidence is supported by a strong evidence trail? (i.e. secure or tamper evident storage, witnessed, original copy retention etc.)	Y	2	(1) Documented and established InfoSec event/incident management process (2) Defined incident response roles and responsibilities	
17.1.1	Planning information security continuity	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Do IT Operations (or an equivalent function) assess BCP requirements to ensure they understand the risks your company faces in terms of likelihood and impact in time; including identification and prioritisation of critical business processes?	Y	3	(1) Documented evidence that Information Security is included within the business continuity process. (2) Current InfoSec Business continuity plans (3) Tested Business continuity plans (4) Evidence that Business continuity plans/objectives are regularly reviewed	
17.1.1	Planning		Have Department heads	Y	3	(1) Documented evidence	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	information security continuity		identified and documented all the assets involved in your company's critical business processes?			that Change Management is included in the business continuity process.	
17.1.1	Planning information security continuity		Do IS and IT Security (or equivalent functions) periodically assess the impact that interruptions caused by information security incidents are likely to have on the business and do they identify solutions to minimise any impacts?	Y	3		
17.1.1	Planning information security continuity		Do IT Operations (or an equivalent function) make provision for the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management?	Y	3		
17.1.1	Planning information security continuity		Does the CISO make available sufficient financial, organizational, technical, and environmental resources to address the identified information security requirements of the BCP?	Y	4		

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
17.1.1	Planning information security continuity		Has IT Operations (or an equivalent function) published business continuity plans addressing information security requirements in line with the agreed business continuity strategy?	Y	4		
17.1.1	Planning information security continuity		Does the IT Director (or an equivalent function) ensure that the business continuity is incorporated in the organization's processes and structure and have they assigned responsibility for the business continuity management process at an appropriate level within the organization?	Y	4		
17.1.2	Implementing information security continuity	The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Do Department Heads ensure that copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site? Any other material necessary to execute the continuity plans must also be stored at the remote location?	Y	4	(1) Relevant clauses covering obligations of 3rd party/3rd Party in legal contracts	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
17.1.2	Implementing information security continuity		Do IT Operations (or an equivalent function) implement controls that allow the secure storage of business continuity plans which must be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site?	Y	4	(1) Documented BCP and DR plans for each business area (2) Documented BCP and DR SLAs	
17.1.2	Implementing information security continuity		Do Change Management (or an equivalent function) ensure that if an alternative temporary DR/BCP location is used, that the level of implemented security controls at these locations is equivalent to the main site?	Y	4		
17.1.3	Verify, review and evaluate information security continuity	The organization should 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.	Do Change Management (or an equivalent function) ensure that procedures are included within the organization's change management programme to ensure that business continuity matters are always addressed appropriately and that when new requirements are identified, any existing emergency procedures,	Y	3	(1) Relevant clauses covering BCP/DR obligations in legal contracts	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			e.g. evacuation plans or fall-back arrangements, are amended as appropriate?				
17.1.3	Verify, review and evaluate information security continuity		Do IT Operations (or an equivalent function) support the Business in testing their Business continuity plans? (The test schedule for business continuity plan(s) must indicate how and the frequency of when each element of the plan should be tested.)	Y	3	(1) Documented evidence of BCP amendments (2) Documented sign-off of BCP amendments	
17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Do Department Heads ensure that copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site? Any other material necessary to execute the continuity plans must also be stored at the remote location?	Y	3	(1) Relevant clauses covering obligations of 3rd party/3rd Party in legal contracts	
17.2.1	Availability of information processing facilities		Have IT Operations (or an equivalent function) implemented controls that allow the secure storage of business continuity plans to be	Y	3	(1) Documented BCP and DR plans for each business area (2) Documented BCP and DR SLAs	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			stored in a remote location, and at a sufficient distance to escape any damage from a disaster at the main site?				
17.2.1	Availability of information processing facilities		Does Change Management (or an equivalent function) ensure that if alternative temporary locations are used, then the level of implemented security controls at these locations is equivalent to the main site?	Y	2		
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 should be explicitly identified, documented and kept up to date for each information system and the organization.	Do Procurement (or an equivalent function) ensure that Specialist business areas (e.g. HR, Legal or Compliance) are consulted to ensure that applicable legislation is adhered to by your organisation (as part of supplier evaluation and selection)?	Y	3	(1) Documented and established process that specifies how, when and how specialist areas are consulted	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
18.1.1	Identification of applicable legislation and contractual requirements		Have Procurement (or an equivalent function) defined in their policy the minimum standards that the business must follow?	Y	3	(1) Documented and signed-off Procurement MCS/Policy	
18.1.1	Identification of applicable legislation and contractual requirements		Does Procurement (or an equivalent function) advise the Business on supplier obligations in their contracts to ensure that their information systems comply with all relevant regulatory, contractual and statutory security requirements?	Y	3	(1) Supplier obligations repository	
18.1.2	Intellectual property rights	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Does the Group Legal department (or an equivalent function) manage the creation, use and protection of your company's Trade Marks, using external Trade Mark Agents?	Y	5	(1) Documented and established IPR controls	
18.1.2	Intellectual property rights		Do IT Operations (or an equivalent function) only acquire software through known reputable sources so that copyright is not	Y	5	(1) Software asset repository (2) Current list of software licenses	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			violated?				
18.1.2	Intellectual property rights		Do IT Operations (or an equivalent function) maintain proof and evidence of license ownership, master media and manuals etc?	Y	4	(1) Software asset repository (2) Current list of software licenses	
18.1.2	Intellectual property rights		Has IT Operations (or an equivalent function) implemented controls to ensure that the maximum number of licensed users is not exceeded?	Y	4	(1) Software asset repository (2) Current list of software licenses (3) MI/Reports on existing software license take up/availability)	
18.1.3	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Has Group Compliance (or an equivalent function) defined, established, and do they maintain, the Group's data retention policy?	Y	4		
18.1.3	Protection of records		Do Group Compliance (or an equivalent function) advise and provide guidance on the Group's data retention	Y	3	(1) Documented and established Data retention guidelines	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			policy, covering the clear identification of records and their retention period as stipulated by local and EC legislation or regulations?				
18.1.3	Protection of records		Has Group Compliance (or an equivalent function) issued guidelines relating to the retention, storage, handling and disposal of records and information?	Y	4	(1) Documented and established Data retention guidelines	
18.1.3	Protection of records		Have Line Managers established local retention procedures aligned to your organisation's Data Retention guidelines?	Y	3	(1) Documented and established Data retention guidelines	
18.1.3	Protection of records		Do Line Managers maintain their own asset inventories for critical business documentation?	Y	2		
18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation	Has Group Compliance (or an equivalent function) established and communicated a data protection policy aligned to stipulated US/UK/EC legislation or local regulations?	Y	4	(1) Documented and established Data Protection Policy (2) Documented Data Protection guidance	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		where applicable.					
18.1.4	Privacy and protection of personally identifiable information		Has Group Compliance (or an equivalent function) issued guidelines detailing individual responsibilities and awareness of the data protection principles?	Y	4	(1) Documented Data Protection guidance	
18.1.4	Privacy and protection of personally identifiable information		Has your Senior Management appointed a Data Protection Officer?	N	1	(1) Formal appointment of a DPO (2) Documented and approved DPO roles and responsibilities	Ebix do not have a designated DPO whereas each employee have been given an awareness as part of the security awareness training to ensure the customer data is protected. The training will be conducted on annual basis.
18.1.4	Privacy and protection of personally identifiable information		Has IS (or an equivalent function) incorporated the organisation's Data protection policy in the IS policy and standards?	Y	4	(1) InfoSec policy and standards provide coverage of the DP policy	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
18.1.4	Privacy and protection of personally identifiable information		Does Group HR (or an equivalent function) ensure that contracts of employment contain clauses requiring employees to comply with the Data protection policy?	Y	5	(1) Employee contracts of employment	
18.1.4	Privacy and protection of personally identifiable information		Do Group Compliance (or an equivalent function) monitor and track compliance with Data protection principles?	Y	3		
18.1.5	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.	Do IS (or an equivalent function) ensure that a 3rd party's internal Information Security framework complies with local and international cryptographic regulations?	N/A	1	(1) List of Cryptographic controls employed within the organisation (2) Reconciliation of cryptographic controls and geographical areas of use to ensure that use of cryptographic algorithms is legal.	
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	Does Internal Audit (or an equivalent function) ensure that internal and external audit reviews of your organisation's IS Management Framework occur at the required frequency?	Y	3	(1) Internal/External audit schedule (2) Scheduled Internal/External audit reports	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
		information security) should be reviewed independently at planned intervals or when significant changes occur.					
18.2.2	Compliance with security policies and standards	Managers should 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.	Do Line Managers regularly review, and record findings of compliance of information processing within their area of responsibilities against the appropriate security policies, standards and legal/regulatory requirements?	Y	2	(1) Documented and established risk assessment process (2) Entry of risk in management system	
18.2.2	Compliance with security policies and standards		Does the CISO (or an equivalent function) produce a 6 monthly adherence report to your IS Governance body for review?	Y	3	(1) Policy adherence report	
18.2.2	Compliance with security policies and standards		Do Department Heads ensure that compliance is managed internally using appropriate MI? (MI should be used to determine causes of non-compliance, determine corrective action plans	Y	3	(1) Actively managed IS policy compliance scorecard (Departmental) (2) Actively managed corrective action plans	

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
			and review the effectiveness of corrective actions.)				
18.2.2	Compliance with security policies and standards		Do IS (or an equivalent function) ensure that 3rd Party compliance is reported using appropriate MI? (MI should be used to determine causes of non-compliance determine corrective action plans and review the effectiveness of corrective actions.)	Y	3	(1) Actively managed IS policy compliance scorecard (3rd Party) (2) Actively managed corrective action plans	
18.2.2	Compliance with security policies and standards		Do Internal Audit (or an equivalent function) liaise with 3rd party audit functions to provide oversight of the 3rd party audit findings and to determine how well they comply with documented security control requirements?	Y	3	(1) Internal/external audit schedule (2) Internal/External audit reports	Ebix was an ISO27001 certified. Based on many clients feedback, we are moving towards the SOC2 audit.
18.2.2	Compliance with security policies and standards		Do IT Operations (or an equivalent function) define individual, role-based Information Security responsibilities within Role Profiles?	Y	2		
18.2.2	Compliance with security		Do IT Operations (or an equivalent function)	N	1		This process is not in place

ISO27001 Ref	ISO Subject	ISO 27001 Control	Supplier Control	Control Present	Maturity Rating	Control Evidence	Supplier Comments
	policies and standards		stipulate methods for monitoring controls within Role Profiles?				
18.2.3	Technical compliance review	Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.	Do IS (or an equivalent function) maintain Technical compliance MI for your company's information systems?	Y	3		
18.2.3	Technical compliance review		Do IS (or an equivalent function) undertake 3rd Party assurance reviews to test material to confirm the validity of the 3rd Party Information Security MI?	Y	3	(1) Documented and established Assurance review process (2) Approved assurance review schedule (3) Assurance review reports and findings (4) Assurance MI	
18.2.3	Technical compliance review		Has IS (or an equivalent function) implemented an IS awareness programme to supplement advisory controls in this area?	Y	3		

End