Author-Rajib Das
Cyber Security Practices
TCS 231462
Name: ISO Organisations IT GRC automation SELECTION evaluation Matrix.
Project: Diligenta (UK)
Email-rajib2.d@tcs.com

Introduction: *This article highlights how and what are the ISO 27001 framework based criteria for the organisation to select proper IT GRC Automation Tool Vendor for effective implementation and meet expected requirements from compliance point of view*

Must have/Should have/ Nice to have Criteria

	MoSCoW	Description
Support Capability/SLA	**Must**	The vendors ability to provide a reliable service for supporting the product but not to (this is covered under enhancement capability)
Analysts view	**Must**	Product is rated by market analysts? e.g. features in Gartner Magic Quadrant (Leader Challenger 3, Niche Player 2 else max of 1)
Install Base	**Must**	Vendor install base/ market penetration is acceptable i.e. we are not the first client
Market Sector	**Must**	Is the product in use by relevant market sector
Existance in Wider Geography	**Must**	Product is installed by other organisations in the UK and US
User Base	**Must**	Companies clients are reputable
Vendor Quality standards	**Must**	Vendor develops to any industry quality standards? e.g. ISO 9001
Vendor Feedback / experience	**Must**	Meetings with vendor have given us confidence in the product
Support	**Must**	Support is provided by the vendor (i.e. not through a 3rd party or reseller)
Company Culture	**Should**	We expect the vendor to work well with Organisation
Reference Sites	**Nice to have**	Reference sites use the technology in the same way we plan to
Proprietary Technology	**Not applicable**	Products use industry standard technology (not proprietary)? How much lock-in is th
Total for Vendor		

	MoSCoW	Description
IPR	**Must**	The product fits with our Commercial Strategy
Financial Security	**Must**	The vendor is financially stable over the last few years, recent quarters? Do they have Completed for IT GRC Product
Service Level	**Must**	What Service levels are the vendor offering? How are problems identified, escalated a
Partnership Potential	**Nice to have**	There a long term benefit for Client Organisation to be commercially associated with t
Influence on Product Direction	**Not applicable**	Are Client Organisation or the vendor the main influence on product direction ? Can
Total for Commercial		

	MoSCoW	Description
Operability + Manageability	**Must**	Product is easy to manage e.g. will not have significant impact on IT, end users, expert
Current product availability / maturity	**Must**	The product version has been implemented by other clients, tried and tested
Usability	**Must**	How intuitive is the application ? How long will it take to perform a task compared w
Robustness and stability	**Must**	The vendor can demonstrate the stability in the product e.g. lack of defects
Overall Flexibility	**Must**	Product is configurable
Overall Flexibility	**Must**	Product does not require significant effort from vendor to configuration
Reporting capabilities	**Must**	Can the product meet our reporting requirements
Security	**Must**	Will the product access control meet our security guidelines either through integratio Access within the product

Build Compliance	**Must**	Product can be installed onto Client Organisation CIS compliant OS platform builds w
Pen Test	**Must**	Have the products been assessed by a 3rd party in terms of how secure they are or us
Application Patch Management	**Must**	Vendor has a process in place to rollout patches for vulnerabilities
Application Vulnerability Management	**Must**	Vendor discloses all vulnerabilities that affect the software - IT GRC Product will com Client Organisation
Client Organisation Control	**Must**	Solution has taken into account data processed / stored in the product and complies v Organisation security policies and standards
Resource requirements - Client Organisation	**Must**	Resources required for development, implementation and support are inline with our
N-1	**Must**	Clients are expected to upgrade to the latest versions in acceptable timescales
N-1	**Must**	What is the lifecycle for N-1 versions supported - 99% are on the latest version - we d with last version
Scalability	**Should**	Evidence of scalability. (see reference sites) How much will it scale. How are the vend (VM - IT GRC Product - 10000 hosts / IP)
Vendor Specific	**Should**	Have the products been developed to secure coding standard e.g. OWASP (SDLC - IT GRC Product - Platform Coding ; Configuration of Modules)
Vendor Specific	**Should**	Vendor uses automated tools for security testing and/or code reviews
Interface capability with other solutions	**Should**	Product will integrate with Client Organisation in scope solutions (e.g SIEM, VM, AD, C
Product lifecycle	**Should**	Product upgrades/versions released are released at an acceptable frequency
Third party product support	**Should**	How easy to bolt in 3rd party products or tools e.g. monitoring or integration
	Could	Vendor employs security specialists
Online Performance	**Not applicable**	Product has on-line transactional performance guarantee. Vendor can evidence this
Batch Performance	**Not applicable**	Product has a batch performance guarantee. Vendor can evidence this
Total for Quality		

	MoSCoW	**Description**
Product Alignment	**Must**	Product alignment with Client Organisation and Technology standards and tools
Hardware	**Must**	Product runs on supportive hardware components
Operating System	**Must**	Product runs on an operating system which is listed as "active" or "target" in the techn
Database	**Must**	Product runs on a database technology which is listed as "active" or "target" in the tec
Middleware	**Must**	Product requires middleware technology which is listed as "active" or "target" in the t
Ops + Support + Training	**Must**	Product uses existing technologies supported by operations and/or requires minimal
Server Operating System / Coexistence	**Must**	Server software compatibility with current target server operating system versions ar
Server Operating System / Coexistence	**Must**	Supported on the current hypervisor \ virtualisation platforms
Server Operating System / Coexistence	**Must**	Licensed on virtual platforms without financial penalties
Backup/Recovery	**Must**	Backup regime for the service alignment with Client Organisation processes (consider
DR	**Must**	DR solution will be implemented by Client Organisation
Security	**Must**	Service is secure (never been subject to a security breach)
Testing	**Must**	Capability or access to a non-production instance for testing
Availability	**Must**	24x7x365 availability
Proof of Concept	**Must**	The vendor will provide\support a Proof of Concept at no or minimal cost
Integration to other systems	**Must**	Easy to integrate data or components with other applications*
Product vision	**Must**	Product has a roadmap for the 2 years, 5 years. Does it embrace new technologies
Test strategy	**Must**	Vendor can demonstrate they have formal testing process before product releases

Systems Management	**Must**	Product can be monitored with existing systems management tools
Backup and recovery	**Must**	Product will work with existing backup tools
Dev tools	**Should**	Product fit with current skills base within Client Organisation for application develop
Usage	**Should**	Service already being used by other clients of the vendor (we are not the first or early
Performance	**Should**	Performance Monitoring capability (usage reports or dashboard) available
Supportability	**Should**	Product can be upgraded without significant effort e.g. OS or database upgrades witho installation - Nothing stored in IT GRC Product - Stored in DB - Configuration by Clien - Modules are supported by IT GRC Product
Flexibility/Scalability	**Could**	Service capacity can be flexed e.g. for financial year ends, temporary increased usage
Flexibility/Scalability	**Could**	Existing instance of the service of the required scale and capacity in use today
Client Operating System / Coexistence	**Not applicable**	Client software compatibility with the current desktop platform (including Citrix) and
Client Operating System / Coexistence	**Not applicable**	Client software coexistence with other software products on the desktop
Client Operating System / Coexistence	**Not applicable**	Thin client (browser) based option
Hosting Options	**Not applicable**	Cloud hosting capability
Cloud / *aaS	**Not applicable**	Service provided using a Tier 1 cloud platform provider e.g. AWS, Azure, IBM (Note: if assessment of the hosting should be undertaken)
Migration	**Not applicable**	Service comes with migration tools to transition service to cloud
Termination	**Not applicable**	Access to all the data if the contract terminates for archiving / compliance or reportin
Termination	**Not applicable**	Zero or minimal cost to extract data if contract terminated
Open Source Components	**Not applicable**	If the product uses open source components the vendor themselves provides support another supplier
3rd Party Components	**Not applicable**	If the product relies on 3rd party licenceable components they are licensed with the p
3rd Party Components	**Not applicable**	The vendor provides support for 3rd party components or they have a back to back c
Software architecture	**Not applicable**	If the software is multi-tier are these supported on separate servers
Network Considerations	**Not applicable**	There are configuration options to optimise the system across certain parts of the net
Product vision	**Not applicable**	Product does not use proprietary or obsolete technologies e.g. old versions of develop environments
Total for Architecture		

	MoSCoW	**Description**
Re-usability	**Must**	The product could be rolled out to multiple clients with minimal development, reconf
Ability to integrate with upcoming/future technologies	**Could**	The vendor adopts new standards and emerging technologies for their product devel
Adaptability	**Nice to have**	The product can be used for a variety of business solutions
Product alignment to future needs / markets / products	**Nice to have**	The future direction of the product aligns with Client Organisation requirements e.g. l technologies, roadmaps
Component structure/tiering	**Not applicable**	The product could be to be partially deployed for a customer who only wanted some
Total for Strategic Fit		

	MoSCoW	**Description**
Delivery Time	**Must**	The development / delivery aligns with the project timeline
Product meets UK and US specific requirements	**Must**	As per market research these products are operational for various customers for diffe

Application support training	**Must**	The cost of introducing the new technology to application support does require additi through training
IT support training	**Must**	The cost of introducing the new technology to server infrastructure, DBA, networks s staff and can be managed through training
Quality and availability of Vendor staff	**Should**	Confidence in development capability, number and frequency of on site meetings, rev
Change Management Process	**Should**	Evidence the vendor manages change requests effectively
Development costs	**Nice to have**	The cost of the initial development phase is within Client Organisation
Total for Development		

	MoSCoW	**Description**
Deployment time	**Must**	The time from purchase to being operational aligns with project plans
Deployment cost/seat	**Must**	Infrastructure will be provided by Client Organisation and product will be deployed b
Training and User documentation	**Must**	The cost and time taken to train staff to be competent with the product is acceptable
Operational cost/seat	**Should**	Ongoing operational costs of licenses/support are acceptable compared to other vend
Support call turnaround	**Should**	Evidence from the vendor to demonstrate the turnaround to resolution of support iss
Data migration	**Not applicable**	The cost \ duration of any migration to the product is acceptable
Total for Deployment		

	MoSCoW	**Description**
New environment support	**Must**	If on premise solution, What would be dedicated infrastrcute to host the application (received)
Ease of enhancement	**Could**	Ease of change to the application to increase in functionality, or bolt on other compon vendors are acceptable
Implementation	**Must**	Implementation with professional services included
SLA	**Must**	Vendor response time for Change Request are acceptable
Frequency	**Must**	New releases from the supplier are manageable (i.e. not too frequent/infrequent)
N-1	**Should**	Product old version(s) are supported for an acceptable period
Total for Change		

	MoSCoW	**Description**
Multi client support/adaptability	**Must**	The product can be easily configured for potential new clients
Training and User documentation	**Must**	The product is provided with appropriate documentation and training materials
24 x 7 operation support	**Could**	The product supports a 24x7 operation for contact centre, web presence, minimal dow
Fit for purpose	**Not applicable**	The product performance both on the WAN and via Citrix is appropriate to perform th use within a contact centre environment NOTE : Application / Software will be accessed via URL
Total for Operations		

	MoSCoW	**Description**
Audit Management	**Must**	Ability to provide complete audit lifecycle management including annual and detailed electronic workpapers, material requests, audit notes, time & expense entry, findings reports.
Continuous Controls Testing	**Must**	Ability to Automate ongoing workflow-based control testing activities.
Exception Management	**Must**	Ability to Submit, analyse, and dynamically approve exception requests against any pr standards, and controls. Ability to automate process routing and expiration reviews.
Incident Management	**Must**	Ability to manage centrally, variety of incident types through analysis, investigation, a audit history.

Indicators and Metrics	**Must**	Ability to automate quantitative-to-qualitative conversion of point-in-time KPI, KRI da provide robust charting and notification functionality supporting objective-based dec
Issue / Findings Management	**Must**	Ability to record, correlate, track, and centrally manage role-based findings/issues an
Risk & Compliance Management	**Must**	Provides vast library of harmonized regulatory assessment questions Ability to provide dynamic assessments for any tangible or intangible assets with auto findings generation and scoring ensuring prioritized remediation.
Risk Management	**Must**	Ability to establish common taxonomies and to consolidate siloed risks into a centrali streamlining risk and remediation activities.
Regulatory Change Management	**Must**	Ability to automate legislative awareness through sourced integration. Ability to provide internal notifications and correlation of externally sourced informa
Cyber Incident and Breach Response	**Must**	Provides central catalog for organizational and IT assets, establishing business contex and implement processes designed to escalate, investigate, and resolve declared incid
Risk Quantification	**Must**	Quantify an organization's financial risk exposure to cybersecurity events.
Enterprise policy Management (IT)	**Must**	Provide easily accessible library of policies with automated lifecycle management inc and redline functionality. Includes exception management and policy attestation cam
Enterprise Risk Management (IT)	**Must**	Support top-down, bottom-up, and hybrid approaches to objective-based risk manage Dynamically created risk assessments provide distributed input from stakeholders w further validate the enterprise risk posture. Ability to provide quantitative scenario analysis capabilities.
Regulatory and Corporate Compliance	**Must**	Ability to document external obligations and regulatory change management. Ability to manually assess and report on the performance of controls at the business l Ability to perform data protection impact assessments and tracking regulatory and da data protection authorities. Ability to define and manage separate compliance projects, assess and report on the Enterprise asset levels including technical infrastructure, and the ability to automate continuously.
Poll Vulnerability Scanner	**Must**	Ability to identify and track vulnerabilities to build aggregate risk view.
Business Continuity	**Should**	Ability to perform business impact analysis (BIA) and to maintain test continuity plan process, asset, and control relationships. Ability to provide incident and crisis management automated creation and communic
Vendor Risk Management	**Could**	Ability to take charge of our ecosystem with interactive, portal-based, vendor risk ma boarding, assessments, contracts, and ongoing service-level performance. Ability to integrate with industry- leading rating firms to provide additional validatio
Business Resiliency	**Should**	Ability to provide Resiliency Management to enable organization to report and manag notifications, and activate BCM or IT DR plans. Ability to provide issue management
Build Your Own	**Nice to have**	Provides the ability to create an application from scratch for Customer specific use ca Ability to provide on demand applications to enable us to take advantage of the platfo processes that are manually completed today.
PCI Management	**Must**	Ability to streamline the PCI compliance process, Ability to automate assessments. Ability to conduct continuous, automated assessments and to gain visibility to manag

Third Party Governance	**Should**	Third Party Governance provides the capability to track the performance of engageme It provides the ability to document and track service level agreement metrics, utilize a promote consistency in assigning SLA metrics to similar engagements.
Financial Controls Management	**Not applicable**	End-to-end management of Internal Controls over Financial Reporting (ICFR) from ac executive certification processes.
Enterprise and Operational Risk Management (IT)	**Must**	Ability to have Top-Down Risk Assessment allows organizations to catalogue their ris up risk register records in higher level risk statements, catalog controls and establish controls to named individuals and by business hierarchy. It also allows to catalogue Risk Register is designed to provide bare-boned risk and internal control managemen Bottom-Up Risk Assessment allows organizations to build and execute risk assessmen targeting business hierarchy and/or business assets. Key Indicator Management is an introductory package to catalog and monitor Key Ris management program. Loss Event Management is an introductory package to catalog and track loss events as program. Operational Risk Management combines the core elements of risk and internal contro found in Risk Register and Risk Questionnaire and adds risk assessment techniques ty including, Process Risk and Control Self-Assessments (pRCSA), Risk and Control Self A Self Assessments (CSA). It also extends the scope of Operational Risk Management to Products and Services and adds core ORM capabilities around loss event capture and and Key Control Indicator management and monitoring.

ISO 27001 Controls GRC Automation Requirements

Domain	Control List ISO 27002: 2013	Control Title	Control Description	Automation I is required to modules Yes
Information Security Policy	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	
Information Security Policy	A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	
Organisation of Information Security	A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	
Organisation of Information Security	A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	
Organisation of Information Security	A.6.1.3	Contact with authorities.	Appropriate contacts with relevant authorities shall be maintained.	
Organisation of Information Security	A.6.1.4	Contact with special interest groups.	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	

Organisation of Information Security	A.6.1.5	Information security in project management.	Information security shall be addressed in project management, regardless of the type of the project.	
Organisation of Information Security	A.6.2.1	Mobile device policy.	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	
Organisation of Information Security	A6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	
HR Security	A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	
HR Security	A.7.1.2	Terms and conditions of employment.	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	
HR Security	A.7.2.1	Management responsibilities.	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	
HR Security	A.7.2.2	Information security awareness, education and training.	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	
HR Security	A.7.2.3	Disciplinary process.	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	
HR Security	A.7.3.1	Termination and change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	
Asset Management	A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	
Asset Management	A.8.1.2	Ownership of assets.	Assets maintained in the inventory shall be owned.	
Asset Management	A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	
Asset Management	A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	
Asset Management	A.8.2.1	Classification of information.	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	
Asset Management	A.8.2.2	Labelling of information.	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	

Asset Management	A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	
Asset Management	A.8.3.1	management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	
Asset Management	A.8.3.2	Disposal of media.	Media shall be disposed of securely when no longer required, using formal procedures.	
Asset Management	A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	
Access Control	A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	
Access Control	A.9.1.2	Access to networks and network services.	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	
Access Control	A.9.2.1	User registration and de-registration.	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	
Access Control	A.9.2.2	User Access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	
Access Control	A.9.2.3	Management of Privileged access rights.	The allocation and use of privileged access rights shall be restricted and controlled.	
Access Control	A.9.2.4	Management of secret Authentication information of users.	The allocation of secret authentication information shall be controlled through a formal management process.	
Access Control	A.9.2.5	Review of User access rights	Asset owners shall review users' access rights at regular intervals.	
Access Control	A.9.2.6	Removal or adjustment of user access tights.	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	
Access Control	A9.3.1	Use of secret authentication information.	Users shall be required to follow the organization's practices in the use of secret authentication information.	
Access Control	A.9.4.1	Information access restriction.	Access to information and application system functions shall be restricted in accordance with the access control policy.	
Access Control	A.9.4.2	Secure log on procedures.	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	
Access Control	A.9.4.3	Password management system.	Password management systems shall be interactive and shall ensure quality passwords.	
Access Control	A.9.4.4	Use of privileged utility programs.	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	

Access Control	A.9.4.5	Access control to program source code.	Access to program source code shall be restricted.	
Cryptography	A.10.1.1	Policy on the use of cryptographic controls.	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	
Cryptography	A.10.1.2	Key management.	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	
Physical and Enviornmental Security	A.11.1.1	Physical security perimeter.	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	
Physical and Enviornmental Security	A.11.1.2	Physical entry controls.	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	
Physical and Enviornmental Security	A.11.1.3	Securing offices rooms and facilities.	Physical security for offices, rooms and facilities shall be designed and applied.	
Physical and Enviornmental Security	A.11.1.4	Protecting against external and environmental threats.	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	
Physical and Enviornmental Security	A.11.1.5	Working in secure areas.	Procedures for working in secure areas shall be designed and applied.	
Physical and Enviornmental Security	A.11.1.6	Delivery and loading areas.	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	
Physical and Enviornmental Security	A.11.2.1	Equipment siting and protection.	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	
Physical and Enviornmental Security	A.11.2.2	Supporting utilities.	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	
Physical and Enviornmental Security	A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	
Physical and Enviornmental Security	A.11.2.4	Equipment maintenance.	Equipment shall be correctly maintained to ensure its continued availability and integrity.	
Physical and Enviornmental Security	A.11.2.5	Removal of assets.	Equipment, information or software shall not be taken off-site without prior authorization.	
Physical and Enviornmental Security	A.11.2.6	Security of equipment and assets off premises.	Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.	
Physical and Enviornmental Security	A.11.2.7	Secure disposal or reuse of equipment's.	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	
Physical and Enviornmental Security	A.11.2.8	Unattended user equipment.	Users shall ensure that unattended equipment has appropriate protection.	

Physical and Enviornmental Security	A.11.2.9	Clear desk and clear screen policy.	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	
Operations Security	A.12.1.1	Documented operating procedures.	Operating procedures shall be documented and made available to all users who need them.	
Operations Security	A.12.1.2	change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	
Operations Security	A.12.1.3	Capacity Management.	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	
Operations Security	A.12.1.4	Separation of development, testing and operational environments.	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	
Operations Security	A.12.2.1	Controls against Malware.	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	
Operations Security	A.12.3.1	Information backup.	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	
Operations Security	A.12.4.1	Event logging.	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	
Operations Security	A.12.4.2	Protection of log information.	Logging facilities and log information shall be protected against tampering and unauthorized access.	
Operations Security	A.12.4.3	Administrator and operator logs.	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	
Operations Security	A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	
Operations Security	A.12.5.1	Installation of software on operational systems.	Procedures shall be implemented to control the installation of software on operational systems.	
Operations Security	A.12.6.1	Management of technical vulnerabilities.	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	
Operations Security	A.12.6.2	Restrictions on software installations.	Rules governing the installation of software by users shall be established and implemented.	
Operations Security	A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	
Communications Security	A.13.1.1	Network Controls.	Networks shall be managed and controlled to protect information in systems and applications.	

Communications Security	A.13.1.2	Security of network services.	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	
Communications Security	A.13.1.3	Segregation in networks.	Groups of information services, users and information systems shall be segregated on networks.	
Communications Security	A.13.2.1	Information transfer policies and procedures.	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	
Communications Security	A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	
Communications Security	A.13.2.3	Electronic messaging.	Information involved in electronic messaging shall be appropriately protected.	
System Aqusition, Development and Maintainance	A.13.2.4	Confidentiality and non disclosure agreements.	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	
System Aqusition, Development and Maintainance	A.14.1.1	Security requirements of information systems	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	
System Aqusition, Development and Maintainance	A.14.1.2	Securing application services on public networks.	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	
System Aqusition, Development and Maintainance	A.14.1.3	Protecting application services transactions.	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	
System Aqusition, Development and Maintainance	A.14.2.1	Secure development policy.	Rules for the development of software and systems shall be established and applied to developments within the organization.	
System Aqusition, Development and Maintainance	A.14.2.2	System change control procedures.	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	
System Aqusition, Development and Maintainance	A.14.2.3	Technical review of applications after operating platform changes.	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	
System Aqusition, Development and Maintainance	A.14.2.4	Restriction on changes to software packages.	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	
System Aqusition, Development and Maintainance	A.14.2.5	Secure system engineering principles.	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	

System Aqusition, Development and Maintainance	A.14.2.6	Secure development environment.	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	
System Aqusition, Development and Maintainance	A.14.2.7	Outsourced development.	The organization shall supervise and monitor the activity of outsourced system development.	
System Aqusition, Development and Maintainance	A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	
System Aqusition, Development and Maintainance	A.14.2.9	System acceptance testing.	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	
System Aqusition, Development and Maintainance	A.14.3.1	Protection of test data.	Test data shall be selected carefully, protected and controlled.	
Supplier Relationships	A.15.1.1	Information security policy for supplier relationships.	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	
Supplier Relationships	A.15.1.2	Addressing security within supplier agreements.	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	
Supplier Relationships	A.15.1.3	Information and communication technology supply chains	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	
Supplier Relationships	A.15.2.1	Monitoring and review of supplier services.	Organizations shall regularly monitor, review and audit supplier service delivery.	
Supplier Relationships	A.15.2.2	Managing changes to supplier services.	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	
Information Security Incident Management	A.16.1.1	Responsibilities and Procedures.	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	
Information Security Incident Management	A.16.1.2	Reporting information security events.	Information security events shall be reported through appropriate management channels as quickly as possible.	
Information Security Incident Management	A.16.1.3	Reporting information security weaknesses.	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	
Information Security Incident Management	A.16.1.4	Assessment of and decision on information security events.	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	

Information Security Incident Management	A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	
Information Security Incident Management	A.16.1.6	Learning from information security incidents.	Knowle e gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	
Information Security Incident Management	A.16.1.7	Collection of evidence.	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	
Information Security Aspects of Business Continuity	A.17.1.1	Planning information security continuity.	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	
Information Security Aspects of Business Continuity	A.17.1.2	Implementing information security continuity.	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	
Information Security Aspects of Business Continuity	A.17.1.3	Verify, review and evaluate information security continuity.	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	
Information Security Aspects of Business Continuity	A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	
Compliance	A.18.1.1	Identification of applicable legislation and contractual requirements.	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	
Compliance	A.18.1.2	Intellectual property rights.	Appropriate procedures shall be implemented to ensure compliance related to intellectual property rights and use of proprietary software products.	
Compliance	A.18.1.3	Protection of records.	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	
Compliance	A.18.1.4	Privacy and protection of personally identifiable information.	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	
Compliance	A.18.1.5	Regulation of cryptographic controls.	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	

Compliance	A.18.2.1	Independent review of information security.	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	
Compliance	A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	
Compliance	A.18.2.3	Technical compliance review.	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	

Other Evaluation Criteria

Role	Number of Resources Required	Location
L1 Admin		
L2 Admin		
Project Manager		
Infra Support - Wintel BAU		
Infra Support - N/W		
Infra Support - MW		
Infra Support - DB		
Security Ops Support		

Market Customer Experience Evaluation KPI Parameters	Vendor X	Vendor Y
Integration & Deployment		
Ease of Deployment		
Service & Support		
Timeliness of Vendor Response		
Severity-1 SLA		
Severity-2 SLA		
Severity-3 SLA		
Quality of Technical Support		

Standard	Vendor X	Vendor Y
ISO27001		
ISO20000		
ISO22301		
SOX		
HIPAA		
ISAE 3402		
NY DFS		
Current Forrester Position		
Current Gartner Position		