PUGET SOUND ENERGY

2023 Distributed Solar and Storage Resources RFP:

Exhibit K. Vendor Questionnaire

The Santa Fe Group
Standardized Information Gathering (SIG) Questionnaire
Version 6.0
Released: October 2010

http://www.sharedassessments.org
sharedassessments@santa-fe-group.com

Instructions
One of the many benefits of the Shared Assessments Program is that its tools help service providers reduce the number of audits and questionnaires they must undergo. Service providers instructed to complete only the "SIG Lite" questions should go directly to the "SIG Lite" tab. This tab may also be helpful in selecting the most appropriate areas of the SIG for a given type of service provided. For additional depth of evaluation, use the "SIG Lite" tab with the full SIG. Please note: Because customers may request varying amounts of information based on the scope or criticality of the services provided, completing the entire SIG allows service providers to supply consistent responses to all customers. There are two parts to this questionnaire: - SIG Lite - Detail tabs (A through L and P).

Index:	% Comp

Please follow the instructions below to complete the SIG Lite or full SIG.

Full SIG

1) Complete the "Business Information" tab.
2) Compile all documentation requested on the "Documentation" tab.
3) Answer all questions on the "SIG Lite" tab and tabs A through L and P by selecting "Yes," "No" or "N/A" from the drop-down menu.
4) Use the "Additional Information" field to provide any pertinent information. (An explanation is required for "N/A" responses.)
5) Answer questions on the "Additional Questions" tab (tab M) only if additional questions have been inserted there.

SIG Lite Only

1) Complete the "Business Information" tab.
2) Compile all documentation requested on the "Documentation" tab.
3) Answer all of the questions on the "SIG Lite" tab by selecting "Yes," "No" or "N/A" from the drop-down menu.
4) Use the "Additional Information" field to provide any pertinent information. (An explanation is required for "N/A" responses.)
5) Answer questions on the "Additional Questions" tab (tab M) only if additional questions have been inserted.

SIG Management Tool (SMT)

A macros-enabled spreadsheet is included with the SIG to help with processing service provider responses and managing the transfer of responses from previous versions of the SIG. If a master SIG is created, the SMT allows for comparisons of all responses in the master SIG to the SIG offered by a service provider. The SMT will also transfer responses and the "Additional Information" field from previous versions of the SIG. For a full list of functions, please refer to the SMT Release Notes.

Response Cell Background Color Coding (All tabs)	**Resp**
Response Required (cells with a blue background are editable)	
Yes Response	**Yes**
No Response	**No**
N/A Response	**N/A**
Top of table (no response required)	

Business Information

20 Total Questions to be Answered **0% Percent Complete**

Question/Request	Response
Responder Name	
Responder Job Title	
Responder Contact Information	
Date of Response	
Company Profile	
Name of the holding or parent company	
Company/business name	
Publicly or privately held company	
If public, what is the name of the Exchange	
If public, what is the trading symbol	
Type of legal entity and state of incorporation	
How long has the company been in business	
Are there any material claims or judgments against the company	
If yes, describe the impact it may have on the services in scope of this document	
Computer Equipment Details (relative to scope of services provided)	
Production site physical address	
Backup site physical address	
Any additional locations where Scoped Systems and Data is stored	
If so, provide locations (address, city, state, country).	
Provide details in the following areas:	
- Operating systems	
- Workstations (# of devices)	
- Servers (# of devices)	
- List Applications in scope	
- Number of employees by function (e.g., development, systems operations, information security)	
Scope Question	
Please provide the below responses to establish the scope of the SIG	

Business Information

20 Total Questions to be Answered **0% Percent Complete**

Name and description of service (relative to scope of this questionnaire)	
Type of service provided:	
- Shared (provided to multiple clients)	
- Dedicated (provided to one client)	
- Other (explain)	

Documentation

Document Request	Question Ref	Type of information provided (e.g., document, summary, table of contents)
* Information Security Policies and Procedures. This should include the following (if not, provide the individual documents as necessary): a) Hiring policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network/LAN access. c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Non-disclosure agreement document e) Information Security Incident Report policy and procedures, including all contract information f) Copy of Visitor Policy and procedures g) Security Log Review Policies and Procedures		
* Copy of internal or external information security audit report		
Information technology and security organization charts (including where information security resides in the organization and the composition of any information security steering committees). Note - Actual names of employees is not required.		
* Physical Security policy and procedures (building and/or restricted access)		
* Third-party security reviews/assessments/penetration tests		
Legal clauses and confidentiality templates for third parties		
Topics covered in the security training program		
* Security incident handling and reporting process		
Network configuration diagrams for internal and external networks defined in scope. Note - Sanitized versions of the network diagram are acceptable.		
* System and network configuration standards		
* System backup policy and procedures		
* Offsite storage policy and procedures		
* Vulnerability and threat management scan policy and procedures		
* Application security policy		
* Change control policy/procedures		
* Problem management policy/procedures		
Certification of proprietary encryption algorithms		
* Internal vulnerability assessments of systems, applications, and networks		

Documentation

Document Request	Question Ref	Type of information provided (e.g., document, summary, table of contents)
* System development and lifecycle (SDLC) process document		
* Business continuity plan (BCP) and / or Disaster recovery plan		
* Most recent BCP/DR test dates and results		
Most recent SAS70 / SSAE16 audit report		
Privacy policies (internal, external, web)		

*If your organization's policy prohibits the distribution of any of these documents, please provide the document title, the table of contents, the executive summary, revision history, and evidence of approval.

A. Risk Assessment and Treatment

14 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
A.1	**Is there a risk assessment program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program? If so, does it include:**			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.1	A risk assessment, conducted within the last 12 months?			A.2 IT & Infrastructure Risk Assessment Life Cycle	14.1.2	Business Continuity And Risk Assessment		
A.1.2	Risk Governance?			A.1 IT & Infrastructure Risk Governance and Context	N/A			
A.1.3	Range of assets to include: people, processes, data and technology?			A.1 IT & Infrastructure Risk Governance and Context	N/A			
A.1.4	Range of threats to include: malicious, natural, accidental, business changes (transaction volume)?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.5	Risk scoping?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.6	Risk context?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.7	Risk training plan?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.8	Risk evaluation criteria?			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.9	Risk scenarios? If so:			A.1 IT & Infrastructure Risk Governance and Context	4.1	Assessing Security Risks		
A.1.9.1	Have scenarios been created for a variety of events with a range of possible threats that could impact the range of assets?				N/A			
A.1.9.2	Do the scenarios include threat types impacting all assets resulting in business impact?				N/A			
A.1.10	Ownership, action plan, response plan, management update?							
A.2	**Are controls identified for each risk classified as: preventive, detective, corrective, predictive (technical or administrative controls)?**							

B. Security Policy

48 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
B.1	**Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? If so, does the policy contain:**				5.1.1	Information Security Policy Document		
B.1.1	Risk assessment?				5.1.1.c	Information Security Policy Document		
B.1.2	Risk management?				5.1.1.c	Information Security Policy Document		
B.1.3	Security awareness training/education?				5.1.1.d.2	Information Security Policy Document		
B.1.4	Business continuity?				5.1.1.d.3	Information Security Policy Document		
B.1.5	Consequences for non-compliance with corporate policies?				5.1.1.d	Information Security Policy Document		
B.1.6	Responsibilities for information security management?				5.1.1.e	Information Security Policy Document		
B.1.7	Acceptable use?				7.1.3	Acceptable use of assets		
B.1.8	Access control?				N/A			
B.1.9	Application security?				N/A			
B.1.10	Change control?				N/A			
B.1.11	Clean desk?				N/A			
B.1.12	Computer and communication systems access and use?				N/A			
B.1.13	Data handling?				N/A			
B.1.14	Desktop computing?				N/A			
B.1.15	Disaster recovery?				N/A			
B.1.16	Email?				N/A			
B.1.17	Constituent accountability?				N/A			
B.1.18	Encryption?				N/A			
B.1.19	Exception process?				N/A			
B.1.20	Information classification?				N/A			
B.1.21	Internet/Intranet access and use?				N/A			
B.1.22	Mobile computing?				N/A			
B.1.23	Network security?				N/A			
B.1.24	Operating system security?				N/A			
B.1.25	Personnel security and termination?				N/A			
B.1.26	Physical access?				N/A			
B.1.27	Policy maintenance?				N/A			
B.1.28	Remote access?				N/A			
B.1.29	Security incident and privacy event management?				N/A			
B.1.30	Secure disposal?				N/A			
B.1.31	Social media, social networking?							
B.1.32	Vulnerability management?				N/A			
B.1.33	Have the policies been reviewed in the last 12 months? If so, did the review include:			B.2 Information Security Policy Maintenance	5.1.2	Review of Information Security Policy		
B.1.33.1	Feedback from interested parties?				5.1.2.a	Review of Information Security Policy		
B.1.33.2	Results of independent reviews?				5.1.2.b	Review of Information Security Policy		
B.1.33.3	Policy compliance?				5.1.2.e	Review of Information Security Policy		
B.1.33.4	Changes that could affect the approach to managing information security?				5.1.2.f	Review of Information Security Policy		
B.1.33.5	Reported information security incidents?				5.1.2.h	Review of Information Security Policy		
B.1.33.6	Recommendations provided by relevant authorities?				5.1.2.i	Review of Information Security Policy		
B.1.33.7	Records management?			B.2 Information Security Policy Maintenance	5.1.2	Review of Information Security Policy		

B. Security Policy

48 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
B.1.34	Is there a process to approve exceptions to the policy?				N/A			
B.1.34.1	Does security own the approval process?				N/A			
B.1.35	Is the information security policy communicated to constituents? If so, is it communicated to:				5.1.1	Information Security Policy Document		
B.1.35.1	Full time employees?				N/A			
B.1.35.2	Part time employees?				N/A			
B.1.35.3	Contractors?				N/A			
B.1.35.4	Temporary workers?				N/A			

C. Organizational Security

56 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
C.1	**Is there an information security function responsible for security initiatives within the organization? If so, does it include:**				6.1.1	Management commitment to information security		
C.1.1	Creation, review and approve of information security policies?				6.1.1.b	Management commitment to information security		
C.1.2	Review the effectiveness of information security policy implementation?				6.1.1.c	Management commitment to information security		
C.1.3	Manage assignment of specific roles and responsibilities for information security?				6.1.1.f	Management commitment to information security		
C.1.4	Develop and maintain an overall strategic security plan?				6.1.1	Management commitment to information security		
C.1.5	Consistent implementation of information security across different parts of the organization?				6.1.2	Information security co-ordination		
C.1.6	Review and monitor information security / privacy incidents or events?				5.1.2.h	Review Of The Information Security Policy		
C.1.7	Monitor significant changes in the exposure of information assets?				6.1.3.b	Allocation of information security responsibilities		
C.1.8	Contacts with information security special interest groups, specialist security forums, or professional associations?				6.1.7	Contact with special interest groups		
C.1.9	Identify and document instances of non-compliance with security policies?				15.2.1	Compliance with security policies and standards		
C.1.10	Identify key Information Technology roles?				N/A			
C.2	**Do external parties have access to Scoped Systems and Data or processing facilities? If so, is:**				6.2	External parties		
C.2.1	Access prohibited prior to a risk assessment being conducted?				6.2.1	Identification of risks related to external parties		
C.2.2	A risk assessment performed on third parties?				N/A			
C.2.3	A controls assessment performed on third parties?				6.2.1	Identification of risks related to external parties		
C.2.4	Agreements in place when customers access Scoped Systems and Data?				6.2.2	Addressing security when dealing with customers		
C.2.5	Does management require the use of confidentiality or non-disclosure agreements for all third parties? If so, do they contain:				6.1.5	Confidentiality agreements		
C.2.5.1	Ownership of information, trade secrets and intellectual property?				6.1.5.e	Confidentiality agreements		
C.2.5.2	The permitted use of confidential information, and granting of rights to the signatory to use information?				6.1.5.f	Confidentiality agreements		
C.2.5.3	Process for notification and reporting of unauthorized disclosure or confidential information breaches?				6.1.5.h	Confidentiality agreements		
C.2.5.4	Expected actions to be taken in case of a breach of this agreement?				6.1.5.j	Confidentiality agreements		
C.2.6	Are there contracts with third party service providers who have access to Scoped Systems and Data ? If so do the contracts include:			C.2 Dependent Service Provider Agreements	6.2.3	Addressing security in third party agreements		
C.2.6.1	Non-Disclosure agreement?				6.2.1	Identification of risks related to external parties		
C.2.6.2	Confidentiality Agreement?				6.2.3.b.7	Addressing security in third party agreements		
C.2.6.3	Media handling?				6.2.3.b.7	Addressing security in third party agreements		
C.2.6.4	Requirement of an awareness program to communicate security standards and expectations?				6.2.3.d	Addressing security in third party agreements		
C.2.6.5	Responsibilities regarding hardware and software installation and maintenance?				6.2.3.f	Addressing security in third party agreements		
C.2.6.6	Clear reporting structure and agreed reporting formats?				6.2.3.g	Addressing security in third party agreements		
C.2.6.7	Clear and specified process of change management?				6.2.3.h	Addressing security in third party agreements		
C.2.6.8	Notification of change?				6.2.3.h	Addressing security in third party agreements		

C. Organizational Security

56 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
C.2.6.9	A process to address any identified issues?				6.2.3.h	Addressing security in third party agreements		
C.2.6.10	Access control policy?				6.2.3.i	Addressing security in third party agreements		
C.2.6.11	Breach notification?				6.2.3.j	Addressing security in third party agreements		
C.2.6.12	Description of the product or service to be provided?				6.2.3.k	Addressing security in third party agreements		
C.2.6.13	Description of the information to be made available along with its security classification?				6.2.3.k	Addressing security in third party agreements		
C.2.6.14	SLAs?				6.2.3 l & m	Addressing security in third party agreements		
C.2.6.15	Audit reporting?				6.2.3.m	Addressing security in third party agreements		
C.2.6.16	Ongoing monitoring?				6.2.3.n	Addressing security in third party agreements		
C.2.6.17	A process to regularly monitor to ensure compliance with security standards?				6.2.3.n	Addressing security in third party agreements		
C.2.6.18	Onsite review?				6.2.3.o	Addressing security in third party agreements		
C.2.6.19	Right to audit?				6.2.3.o	Addressing security in third party agreements		
C.2.6.20	Right to inspect?				6.2.3.o	Addressing security in third party agreements		
C.2.6.21	Problem reporting and escalation procedures?				6.2.3.p	Addressing security in third party agreements		
C.2.6.22	Business resumption responsibilities?				6.2.3.q	Addressing security in third party agreements		
C.2.6.23	Indemnification/liability?				6.2.3.r	Addressing security in third party agreements		
C.2.6.24	Privacy requirements?				6.2.3.s	Addressing security in third party agreements		
C.2.6.25	Dispute resolution?				6.2.3.s	Addressing security in third party agreements		
C.2.6.26	Choice of venue?				6.2.3.s	Addressing security in third party agreements		
C.2.6.27	Data ownership?				6.2.3.t	Addressing security in third party agreements		
C.2.6.28	Ownership of intellectual property?				6.2.3.t	Addressing security in third party agreements		
C.2.6.29	Involvement of the third party with subcontractors?				6.2.3.u	Addressing security in third party agreements		
C.2.6.30	Security controls these subcontractors need to implement?				6.2.3.u	Addressing security in third party agreements		
C.2.6.31	Termination/exit clause?				6.2.3.v	Addressing security in third party agreements		
C.2.6.32	Contingency plan in case either party wishes to terminate the relationship before the end of the agreements?				6.2.3.v.1	Addressing security in third party agreements		
C.2.6.33	Renegotiation of agreements if the security requirements of the organization change?				6.2.3.v.2	Addressing security in third party agreements		
C.2.6.34	Current documentation of asset lists, licenses, agreements or rights relating to them?				6.2.3.v.3	Addressing security in third party agreements		

D. Asset Management

35 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
D.1	**Is there an asset management policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?**				7.1	Responsibility For Assets		
D.1.1	Is there an Inventory system for hardware and software assets? If so, does it include:			D.1 Asset Accounting and Inventory	7.1.1	Inventory Of Assets		
D.1.1.1	Asset control tag?				N/A			
D.1.1.2	Operating system?				N/A			
D.1.1.3	Physical location?				N/A			
D.1.1.4	Serial number?				N/A			
D.1.1.5	Business function supported?				N/A			
D.1.1.6	Environment (dev, test, etc.)?				N/A			
D.1.1.7	IP address?				N/A			
D.1.2	Is there a detailed description of software licenses (number of seats, concurrent users, etc.) ?			D.1 Asset Accounting and Inventory	N/A			
D.1.3	Is ownership assigned for information assets? If so, is the owner responsible to:				7.1.2	Ownership Of Assets		
D.1.3.1	Appropriately classify information and assets?				7.1.2.b	Ownership Of Assets		
D.1.3.2	Review and approve access to those information assets?				7.1.2.b	Ownership Of Assets		
D.1.3.3	Establish, document and implement rules for the acceptable use of information and assets?				7.1.3	Acceptable Use Of Assets		
D.2	**Are information assets classified?**				7.2.1	Classification Guidelines		
D.2.1	Is there an information asset classification policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				7.2.1	Classification Guidelines		
D.2.2	Is there a procedure for handling of information assets? If so, does it include:			G.13 Physical Media Tracking	7.2.2	Information Labeling And Handling		
D.2.2.1	Data ownership?				7.1.2	Ownership Of Assets		
D.2.2.2	Data access controls including authorization?				7.1.2.b, 10.7.3.b	Ownership Of Assets, Information Handling		
D.2.2.3	Data labeling?				7.2.2, 10.7.3.a	Information Labeling And Handling		
D.2.2.4	Data on removable media?				10.7.1	Management Of Removable Media		
D.2.2.5	Data in transit?			G.14 Security of Media in Transit	7.2.2	Information Labeling And Handling		
D.2.2.6	Data encryption?				12.3.1	Policy On The Use Of Cryptographic Controls		
D.2.2.7	Data in storage?				10.7.3.f	Information Handling Procedures		
D.2.2.8	Data reclassification?				7.1.2.b	Ownership Of Assets		
D.2.2.9	Data retention?				N/A			
D.2.2.10	Data destruction?				7.2.2, 10.7.2	Information Labeling And Handling, Disposal Of Media		
D.2.2.11	Data disposal?				10.7.2.b	Disposal Of Media		
D.2.2.12	Reviewed at least annually?				7.2.1	Classification Guidelines		
D.2.2.13	Data handling based on classification?			G.13 Physical Media Tracking	7.2.2	Information Labeling And Handling		
D.2.2.14	Physical media destruction?				10.7.2	Disposal Of Media		
D.2.2.15	Reuse of physical media (tapes, disk drives, etc.)?				9.2.6	Secure Disposal Or Re-Use Of Equipment		
D.3	**Is there insurance coverage for business interruptions or general services interruption? If so, are there:**				14.1.1.d	Including Information Security In The Business Continuity Management Process		
D.3.1	Limitations based on the cause of the interruption?				14.1.1.d	Including Information Security In The Business Continuity Management Process		

D. Asset Management

35 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
D.3.2	Insurance coverage for products and services provided to clients?				14.1.1.d	Including Information Security In The Business Continuity Management Process		

E. Human Resource Security

37 Total Questions to be Answered 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
E.1	**Are security roles and responsibilities of constituents defined and documented in accordance with the organization's information security policy?**			B.1 Information Security Policy Content	8.1.1	Roles and responsibilities		
E.2	**Is a background screening performed prior to allowing constituent access to Scoped Systems and Data? If so, does it include:**			E.2 Background Investigation Policy Content	8.1.2	Screening		
E.2.1	Criminal?				8.1.2.e	Screening		
E.2.2	Credit?				8.1.2.e	Screening		
E.2.3	Academic?				8.1.2.c	Screening		
E.2.4	Reference?				8.1.2.a	Screening		
E.2.5	Resume or curriculum vitae?				8.1.2.b	Screening		
E.2.6	Drug Screening?				N/A			
E.3	**Are new hires required to sign any agreements upon hire? If so, does it include:**				8.1.3	Terms and conditions of employment		
E.3.1	Acceptable Use?			B.3. Employee Acknowledgment of Acceptable	7.1.3	Acceptable use of assets		
E.3.2	Code of Conduct / Ethics?				8.1.3	Terms and conditions of employment		
E.3.3	Non-Disclosure Agreement?				8.1.3.a	Terms and conditions of employment		
E.3.4	Confidentiality Agreement?			C.1 Employee Acceptance of Confidentiality	8.1.3.a	Terms and conditions of employment		
E.3.5	Are constituents required to sign annual acknowledgements? If so, do they include:				N/A			
E.3.5.1	Acceptable Use?			B.3. Employee Acknowledgment of Acceptable	N/A			
E.3.5.2	Code of Conduct / Ethics?				N/A			
E.3.5.3	Non-Disclosure Agreement?				N/A			
E.3.5.4	Confidentiality Agreement?				N/A			
E.4	**Is there a security awareness training program? If so, does it include:**			E.1 Security Awareness Training Attendance	8.2.2	Information security awareness, education, and training		
E.4.1	Security policies, procedures and processes?				8.2.2	Information security awareness, education, and training		
E.4.2	Scored test to evaluate successful completion?				N/A			
E.4.3	New Hire and annual participation?				N/A			
E.4.4	Is security training commensurate with levels of responsibilities and access?				8.2.2	Information security awareness, education, and training		
E.4.5	Do constituents responsible for information security undergo additional training?				8.2.2	Information security awareness, education, and training		
E.4.6	Do information security personnel have professional security certifications?				6.1.7	Contact with special interest groups		
E.5	**Is there a disciplinary process for non-compliance with information security policies?**				8.2.3	Disciplinary process		
E.6	**Is there a constituent termination or change of status process?**				8.3.1	Termination responsibilities		
E.6.1	Is there a documented termination or change of status policy or process that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				8.3.1	Termination responsibilities		
E.6.2	Does HR notify security / access administration of constituent termination for access rights removal? If so, is notification provided:			H.2 Revoke System Access	8.3.3	Removal of access rights		
E.6.2.1	On the actual date?				N/A			

E. Human Resource Security

37 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
E.6.2.2	Two to seven days after termination?				N/A			
E.6.2.3	Greater than seven days after termination?				N/A			
E.6.3	Does HR notify security / access administration of a constituent change of status for access rights removal? If so, is notification provided:			H.2 Revoke System Access	8.3.3	Removal of access rights		
E.6.3.1	On the actual date of the change of status?				N/A			
E.6.3.2	Two to seven days after the change of status?				N/A			
E.6.3.3	Greater than seven days after the change of status?				N/A			
E.6.4	Are constituents required to return assets (laptop, desktop, PDA, cell phones, access cards, tokens, smart cards, keys, proprietary documentation) upon:				8.3.2	Return of assets		
E.6.4.1	Termination?				8.3.2	Return of assets		
E.6.4.2	Change of Status?				8.3.2	Return of assets		

F. Physical and Environmental Security

129 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Enter Address of the site this tab refers to:	

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
F.1	**Is there a physical security program?**				5.1.1	Information Security Policy Document		
F.1.1	Is there a documented physical security policy approved by management, communicated to constituents and an owner assigned to maintain and review the policy?			B.1 Information Security Policy Content	5.1.1	Information Security Policy Document		
F.1.2	Are reasonable physical security and environmental controls present in the building/data center that contains Scoped Systems and Data? If so, does it include:			F.2 Physical Security Controls – Scoped Systems and Data	9.1.3	Securing offices, rooms, and facilities		
F.1.2.1	Signage to identify the operations of the facility (data center)?							
F.1.2.2	Other tenants using the building?			F.2 Physical Security Controls – Scoped Systems and Data	N/A			
F.1.2.3	Access restricted and logs kept of all access?				9.1.1.g	Physical security perimeter		
F.1.2.4	Electronic system (key card, token, fob, biometric reader etc.) to control access?				9.1.1	Physical security perimeter		
F.1.2.5	Cipher locks (electronic or mechanical) to control access within or to the facility? If yes, is there a process to:			F.2 Physical Security Controls – Scoped Systems and Data	9.1.2	Physical entry controls		
F.1.2.5.1	Change the code(s) at least every 90 days?				N/A			
F.1.2.5.2	Change the code(s) when an authorized individual is terminated or transferred to another role?				8.3.3	Removal of access rights		
F.1.2.6	Security guards that provide onsite security services?				9.1.1.f	Physical security perimeter		
F.1.2.7	Perimeter physical barrier (such as fence or walls)?							
F.1.2.8	Entry and exit doors alarmed (forced entry, propped open) and/or monitored by security guards?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.f	Physical security perimeter		
F.1.2.9	A mechanism to prevent tailgating / piggybacking?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.2	Physical entry controls		
F.1.2.10	External lighting?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.f	Physical security perimeter		
F.1.2.11	Lighting on all doors?				9.1.1.b	Physical security perimeter		
F.1.2.12	Exterior doors with external hinge pins?				N/A			
F.1.2.13	Emergency doors which only permit egress?				9.1.1.e	Physical security perimeter		
F.1.2.14	Windows with contact or break alarms on all windows?				9.1.1.f	Physical security perimeter		
F.1.2.15	CCTV with video stored at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	N/A			
F.1.2.16	Walls which extend from actual floor to actual ceiling?				9.1.1.f	Physical security perimeter		
F.1.2.17	Fluid or water sensor?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.2	Physical entry controls		
F.1.2.18	Air conditioning and humidity controls?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.2	Physical entry controls		
F.1.2.19	Heat detection?				N/A			
F.1.2.20	Smoke detection?				8.3.3	Removal of access rights		
F.1.2.21	Fire suppression?			F.1 Environmental Controls – Computing Hardware	9.2.1.d	Equipment sitting and protection		
F.1.2.22	Multiple power feeds?							
F.1.2.23	Multiple communication feeds?							
F.1.2.24	Physical access control procedures? If yes, is there:				9.1.1.a	Physical security perimeter		
F.1.2.24.1	Segregation of duties for issuing and approving access to the facility (keys, badge, etc.)?				11.1.1.h	Access control policy		
F.1.2.24.2	Access reviews at least every six months?				9.1.1	Physical security perimeter		

F. Physical and Environmental Security

129 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Enter Address of the site this tab refers to:	

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
F.1.2.24.3	Collection of access equipment (badges, keys, change pin numbers, etc.) when a constituent is terminated or changes status and no longer require access?			H.6 Revoke Physical Access	9.1.2.e	Physical entry controls		
F.1.2.24.4	A process to report lost or stolen access cards / keys?				9.1.2	Physical entry controls		
F.1.3	Are visitors permitted in the facility? If so, are they required to:				9.1.2	Physical entry controls		
F.1.3.1	Sign in and out?				9.1.2.a	Physical entry controls		
F.1.3.2	Provide a government issued ID?				9.1.2	Physical entry controls		
F.1.3.3	Be escorted through secure areas?				9.1.2.c	Physical entry controls		
F.1.3.4	Wear badge distinguishing them from employees?							
F.1.3.5	Subject to right to search while at the facility?							
F.1.3.6	Are visitor logs maintained for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.2.a	Physical entry controls		
F.1.4	Is there a loading dock at the facility? If yes, is there:				9.1.6	Public access, delivery, and loading areas		
F.1.4.1	Any other tenants using the loading dock?				9.1.6.f	Public access, delivery, and loading areas		
F.1.4.2	A security guards at each point of entry?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.6.a	Public access, delivery, and loading areas		
F.1.4.3	Smoke detector?							
F.1.4.4	Fire alarm?							
F.1.4.5	Fire suppression?							
F.1.4.6	CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.1.4.7	Restricted access and logs kept of all access?				9.1.2	Physical entry controls		
F.1.5	Is there a battery/UPS room? If yes, does it contain:			F.1 Environmental Controls – Computing Hardware	9.2.2	Supporting utilities		
F.1.5.1	Hydrogen sensors?				9.2.1.d	Equipment sitting and protection		
F.1.5.2	Monitored fire alarm?				9.2.1.d	Equipment sitting and protection		
F.1.5.3	Fire suppression system?			F.1 Environmental Controls – Computing Hardware	9.1.4.c	Protecting against external and environmental threats		
F.1.5.4	CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.1.5.5	Restricted access and logs kept of all access?				9.1.2	Physical entry controls		
F.1.5.6	Are visitors permitted in the battery/UPS room?				9.1.2	Physical entry controls		
F.1.5.7	Does UPS support N+1?							
F.1.6	Is there a generator or generator area? If yes, is there:			F.1 Environmental Controls – Computing Hardware	9.2.2	Supporting utilities		
F.1.6.1	A fuel supply readily available to ensure uninterrupted service?				9.2.2	Supporting utilities		
F.1.6.2	Adequate capacity to supply power for at least 48 hours?				9.2.2	Supporting utilities		
F.1.6.3	Restricted access and logs kept of all access?				9.1.1.a	Physical security perimeter		
F.1.6.4	CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.1.7	Is there a mailroom that handles Scoped Data? If so, is access:				10.1.1	Documented operating procedures		
F.1.7.1	Restricted access and logs kept of all access?							
F.1.7.2	CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.1.8	Is there a media library to store Scoped Data? If so, is access:				N/A			

F. Physical and Environmental Security

129 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Enter Address of the site this tab refers to:	

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
F.1.8.1	Restricted and logs kept of all access?				9.1.1.a	Physical security perimeter		
F.1.8.2	CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.1.9	Is there a separate room for telecom equipment? If so, is access:				N/A			
F.1.9.1	Monitored with CCTV and the video stored for 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.1.9.2	Restricted and logs kept of all access?				9.2.3.f.1	Cabling security		
F.2	**Do the Scoped Systems and Data reside in a data center? If yes, are the following controls in place:**			F.1 Environmental Controls – Computing Hardware	N/A			
F.2.1	Is the data center shared with other tenants?				9.1.1.g	Physical security perimeter		
F.2.2	Fluid or water sensor?			F.1 Environmental Controls – Computing Hardware	9.2.1.d	Equipment sitting and protection		
F.2.3	Air conditioning?							
F.2.4	heat detection?							
F.2.5	smoke detection?							
F.2.6	fire suppression?							
F.2.7	Vibration alarm / sensor?				9.2.1.d	Equipment sitting and protection		
F.2.8	Monitored fire alarm?				9.2.1.d	Equipment sitting and protection		
F.2.9	Fire suppression e.g., dry, chemical, wet?			F.1 Environmental Controls – Computing Hardware	9.1.4.c	Protecting against external and environmental threats		
F.2.10	Multiple power feeds?				9.2.2	Supporting utilities		
F.2.11	Multiple communication feeds?				9.2.2	Supporting utilities		
F.2.12	Are there generator(s)?			F.1 Environmental Controls – Computing Hardware	9.2.2	Supporting utilities		
F.2.13	Is access to the data center restricted and logs kept of all access?				9.1.1.a	Physical security perimeter		
F.2.14	Badge readers at points of entry?							
F.2.14.0.1	Locked doors requiring a key or PIN at points of entry?							
F.2.14.1	Access request procedures?			H.7 Physical Access Authorization	9.1.2	Physical entry controls		
F.2.14.1.1	Segregation of duties for issuing and approving access?				11.1.1.h	Access control policy		
F.2.14.2	Access reviews conducted at least every six months?				9.1.1	Physical security perimeter		
F.2.14.3	Is there a mechanism to thwart tailgating / piggybacking into the data center?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.2	Physical entry controls		
F.2.14.4	Are there security guards at points of entry?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.c	Physical security perimeter		
F.2.14.5	Do the security guards monitor security systems and alarms?				9.1.1.c	Physical security perimeter		
F.2.14.6	Are visitors permitted in the data center?				9.1.2	Physical entry controls		
F.2.14.6.1	Are they required to sign in and out of the data center?				9.1.2.a	Physical entry controls		
F.2.14.6.2	Are they escorted within the data center?				9.1.2.c	Physical entry controls		
F.2.14.7	Are all entry and exit points to the data center alarmed?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.f	Physical security perimeter		
F.2.14.8	Are there alarm motion sensors monitoring the data center?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.f	Physical security perimeter		
F.2.14.9	Are there alarm contact sensors on the data center doors?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.f	Physical security perimeter		
F.2.14.10	Are there prop alarms on data center doors?				9.1.6	Public access, delivery, and loading areas		

F. Physical and Environmental Security

129 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Enter Address of the site this tab refers to:	

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
F.2.14.11	Do emergency doors only permit egress?				9.1.1.e	Physical security perimeter		
F.2.14.12	Is access to the Data center monitored with CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.2.14.13	Walls extending from true floor to true ceiling?			F.2 Physical Security Controls – Scoped Systems and Data	9.2.1.d	Equipment sitting and protection		
F.2.14.14	Windows or glass walls along the perimeter?				9.1.1.b	Physical security perimeter		
F.2.15	Does the Scoped Systems and Data reside in a caged environment within a data center? If so, are these controls present:				N/A			
F.2.15.1	Locks requiring a key or PIN used at points of entry?				9.1.2	Physical entry controls		
F.2.15.2	A process for requesting access?				9.1.1.a	Physical security perimeter		
F.2.15.2.1	Segregation of duties for granting and storage of access devices (badges, keys, etc.)?				11.1.1.h	Access control policy		
F.2.15.3	A list maintained of personnel with cards / keys to the caged environment?				9.1.2	Physical entry controls		
F.2.15.4	A process to report lost access cards / keys?				9.1.2	Physical entry controls		
F.2.15.5	A process to review access to the cage at least every six months?				9.1.1	Physical security perimeter		
F.2.15.6	A process to collect access equipment (badges, keys, change pin numbers, etc.) when a constituent is terminated or changes status and no longer requires access?			H.6 Revoke Physical Access	9.1.2.e	Physical entry controls		
F.2.15.7	Are visitors permitted in the caged environment? If so, are they:				9.1.2	Physical entry controls		
F.2.15.7.1	Required to sign in and out?				9.1.2.a	Physical entry controls		
F.2.15.7.2	Escorted?				9.1.2.c	Physical entry controls		
F.2.15.8	Monitored with CCTV and the video stored for at least 90 days?			F.2 Physical Security Controls – Scoped Systems and Data	9.1.1.e	Physical security perimeter		
F.2.16	Does the Scoped Systems and Data reside in a locked cabinet? If so, is there:				N/A			
F.2.16.1	Shared cabinets?				9.1.1.g	Physical security perimeter		
F.2.16.2	Restricted access and logs kept of all access?				9.1.1.a	Physical security perimeter		
F.2.16.3	Access request procedures?				9.1.1.a	Physical security perimeter		
F.2.16.4	Segregation of duties for issuing, approving access and storing devices (badges, keys, etc.)?				11.1.1.h	Access control policy		
F.2.16.5	Segregation of duties for issuing and approving access?				11.1.1.h	Access control policy		
F.2.16.6	A list of personnel with cards / keys to the cabinet?				9.1.2	Physical entry controls		
F.2.16.7	A process to report lost access cards / keys?				9.1.2	Physical entry controls		
F.2.16.8	Collection access equipment (badges, keys, change pin numbers, etc.) when a constituent is terminated or changes status and no longer requires access?				9.1.2.e	Physical entry controls		
F.2.16.9	Cabinets monitored with CCTV and the video stored for at least 90 days?				9.1.1.e	Physical security perimeter		
F.2.17	Is there a policy on using locking screensavers on unattended system displays or locks on consoles within the data center?				11.3.2.a, 11.3.3	Unattended user equipment, Clear desk and clear screen policy		
F.2.18	Is there a procedure for equipment removal from the data center?				9.2.7	Removal of property		
F.2.19	Is there a preventive maintenance or current maintenance contracts for:				N/A			
F.2.19.1	UPS system?				9.2.4	Equipment maintenance		
F.2.19.2	Security system?				9.2.4	Equipment maintenance		
F.2.19.3	Generator?				9.2.4	Equipment maintenance		
F.2.19.4	Batteries?				9.2.4	Equipment maintenance		
F.2.19.5	Monitored fire alarm?				9.2.4	Equipment maintenance		
F.2.19.6	Fire suppression systems?				9.2.4	Equipment maintenance		
F.2.19.7	HVAC?				9.2.4	Equipment maintenance		

F. Physical and Environmental Security

129 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Enter Address of the site this tab refers to:	

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
F.2.20	Are the following tested:				N/A			
F.2.20.1	UPS system - annually?				N/A			
F.2.20.2	Security alarm system - annually?				N/A			
F.2.20.3	Fire alarms - annually?				N/A			
F.2.20.4	Fire suppression system - annually?				N/A			
F.2.20.5	Generators - monthly?				N/A			
F.2.20.6	Generators full load tested - monthly?				N/A			

G. Communications and Operations Management

258 Total Questions to be Answered | 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.1	**Are Management approved operating procedures utilized? If so, are they:**				10.1.1	Documented Operating Procedure		
G.1.1	Documented, maintained, and made available to all users?				10.1.1	Documented Operating Procedure		
G.2	**Is there an operational change management / change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? If so, does it include:**			G.21 Change Control	10.1.2	Change Management		
G.2.1	Documentation of changes?				10.1.2.a	Change Management		
G.2.2	Request, review and approval of proposed changes?				10.1.2.a, 10.1.2.d	Change Management		
G.2.3	Pre-implementation testing?				10.1.2.b	Change Management		
G.2.4	Post-implementation testing?				10.1.2.b	Change Management		
G.2.5	Review for potential security impact?				10.1.2.c	Change Management		
G.2.6	Review for potential operational impact?				10.1.2.c	Change Management		
G.2.7	Communication of changes to all relevant constituents?				10.1.2.e	Change Management		
G.2.8	Rollback procedures?				10.1.2.f	Change Management		
G.2.9	Maintenance of change control logs?				10.1.2	Change Management		
G.2.10	Code reviewed by information security prior to the implementation of internally developed applications and / or application updates?				12.5.1	Change Control Procedures		
G.2.11	Is Information security's approval required prior to implementation changes?				N/A			
G.2.12	Are the following changes to the production environment subject to the change control process:				10.1.2	Change Management		
G.2.12.1	Network?				N/A			
G.2.12.2	Systems?				10.1.2	Change Management		
G.2.12.3	Application updates?				10.1.2	Change Management		
G.2.12.4	Code changes?				10.1.2	Change Management		
G.2.13	Is there a segregation of duties between those requesting, approving and implementing a change?				10.1.3	Segregation Of Duties		
G.3	**Is application development performed? If so, is:**				12.5	Security In Development And Support Processes		
G.3.1	Development, test, and staging environment separate from the production environment? If so how are they separated:				N/A			
G.3.1.0.1	Logically?				N/A			
G.3.1.0.2	Physically?				N/A			
G.3.1.0.3	No segregation?				N/A			
G.4	**Do third party vendors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc)? If so, is there:**				N/A			
G.4.1	Security review prior to engaging their services (logical, physical, other controls)?				10.2.1	Service Delivery		
G.4.2	Security review at least annually, on an ongoing basis?				10.2.2	Monitoring And Review Of Third Party Services		
G.4.3	Risk assessments or review?				6.2.1	Identification Of Risks Related To External Parties		
G.4.4	Confidentiality and/or Non Disclosure Agreement requirements?				6.2.3.b.7	Addressing Security In Third Party Agreements		
G.4.5	Requirement to notify of changes that might affect services rendered?				10.2.3	Managing Changes To Third Party Services		
G.5	**Are system resources reviewed to ensure adequate capacity is maintained?**				10.3.1	Capacity Management		
G.6	**Are criteria for accepting new information systems, upgrades, and new versions established? If so, do they include:**				10.3.2	System acceptance		
G.6.1	Performance and computer capacity requirements?				10.3.2.a	System acceptance		
G.6.2	Error recovery and restart procedures?				10.3.2.b	System acceptance		

G. Communications and Operations Management

258 Total Questions to be Answered | 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.6.3	Preparation and testing of operating procedures?				10.3.2.c	System acceptance		
G.6.4	Agreed set of security controls?				10.3.2.d	System acceptance		
G.6.5	Effective manual procedures?				10.3.2.e	System acceptance		
G.6.6	Business continuity arrangements?				10.3.2.f	System acceptance		
G.6.7	Evidence that new system will not adversely affect existing systems, particularly at peak processing times, such as month end?				10.3.2.g	System acceptance		
G.6.8	Evidence of the effect on the overall security of the organization?				10.3.2.h	System acceptance		
G.7	**Is there an anti-virus / malware policy or program (workstations, servers, mobile devices) that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?**				10.4.1.e	Controls Against Malicious Code		
G.7.1	What is the interval between the availability of a new signature update and its deployment:				10.4.1.d	Controls Against Malicious Code		
G.7.1.1	Hourly?				N/A			
G.7.1.2	Daily?				N/A			
G.7.1.3	Weekly?				N/A			
G.7.1.4	Monthly?				N/A			
G.8	**Are system backups of Scoped Systems and Data performed?**				10.5.1	Information Back-Up		
G.8.1	Is there a policy or process for the backup of production data? If so, does it include a requirement to:				10.5.1	Information Back-Up		
G.8.1.1	Store backups to avoid any damage from a disaster at the main site?				10.5.1.d	Information Back-Up		
G.8.1.2	Test backup media and restoration procedures at least annually?				10.5.1.f	Information Back-Up		
G.8.2	Is backup media stored offsite? If so, is there:				10.5.1.d	Information Back-Up		
G.8.2.0.1	Secure transport?				10.8.3	Physical Media In Transit		
G.8.2.0.2	Tracking shipments?				10.8.2.a & 10.8.2.b	Exchange Agreements		
G.8.2.0.3	Verification of receipt?				10.8.2.a & 10.8.2.b	Exchange Agreements		
G.9	**Are there external network connections (Internet, extranet, etc.)? If so, is there:**				N/A			
G.9.1	Security and hardening standards for network devices (baseline configuration, patching, passwords, access control)?				10.6.1.e	Network Controls		
G.9.1.1	Regular review and/or monitoring of network devices for continued compliance to security requirements?				15.2.2	Technical Compliance Checking		
G.9.2	Is every connection to an external network terminated at a firewall?			G.17 Network Security – Firewall(s)	11.4.5	Segregation In Networks		
G.9.3	Are network devices configured to prevent communications from unapproved networks?			G.17 Network Security – Firewall(s)	11.4.5	Segregation In Networks		
G.9.4	Do network devices deny all access by default?				11.1.1.B	Access Control Policy		
G.9.5	Is there a process to request, approve, log, and review access to networks across network devices?				11.4.1.b	Policy On Use Of Network Services		
G.9.6	Is network traffic logged to support forensics?			G.4 Network Logging	10.6.1.d	Network Controls		
G.9.6.1	Do logs contain: failed login attempts, disabling of audit logs, changes, timestamps, IP info, etc?			G.4 Network Logging	10.6.1.d	Network Controls		
G.9.6.2	In the event of a network device audit log failure, does the network device generate an alert and prevent further connections?				10.10.5	Fault Logging		
G.9.6.3	Is the overwriting of audit logs disabled?				10.10.3.b	Protection Of Log Information		
G.9.6.4	Are the logs from network devices aggregated to a central server?				10.10.3	Protection Of Log Information		
G.9.7	Are security patches reviewed and applied to network devices?				12.6.1.d	Control Of Technical Vulnerabilities		
G.9.8	Is there an approval process prior to installing a network device?				10.1.2.d	Change Management		
G.9.9	Is there an approval process for the ports allowed through the network devices?			G.18 Network Security – Authorized Network Traffic	10.6.2.c	Security Of Network Services		

G. Communications and Operations Management

258 Total Questions to be Answered 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.9.10	Are critical network segments isolated?			G.17 Network Security – Firewall(s)	11.4.5	Segregation In Networks		
G.9.11	Is there a process to prevent unauthorized devices from physically connecting to the internal network?				11.4.3	Equipment Identification In Networks		
G.9.12	Are internal systems required to pass through a content filtering proxy prior to accessing the Internet?				11.4.7	Network Routing Control		
G.9.13	Is there an approval process to allow extranet connections?				11.4.1.b	Policy On Use Of Network Services		
G.9.14	Are insecure protocols (telnet) used to access network devices?			G.2 Network Management – Encrypted Authentication Credentials	11.4.1.d	Policy on use of network services		
G.9.15	Is access to diagnostic or maintenance ports on network devices restricted?			G.3 Externally Facing Open Administrative Ports	11.4.4	Remote Diagnostic And Configuration Port Protection		
G.9.16	Is there a separate network segment or endpoints for remote access?				11.7.1	Mobile Computing And Communications		
G.9.17	Are firewall rules and network access control lists regularly reviewed?							
G.9.18	Is there a DMZ environment within the network that transmits, processes or stores Scoped Systems and Data? If so, is it:				N/A			
G.9.18.1	Limited to only those servers that require access from the Internet?				11.4.5	Segregation In Networks		
G.9.18.2	Separated with DMZ segments for devices that initiate outbound traffic to the Internet?				11.4.5	Segregation In Networks		
G.9.19	Is Intrusion Detection/Prevention System employed in all network zones? If so, does it include:			G.19 Network Security – IDS/IPS Attributes	10.10.3	Protection Of Log Information		
G.9.19.1	Configuration to generate alerts when incidents and values exceed predetermined thresholds?				10.10.2.c.4	Monitoring System Use		
G.9.19.2	Regularly updated signatures based on new threats?			G.1 Network Security – IDS/IPS Signature Updates	10.4.1.d	Controls Against Malicious Code		
G.9.19.3	System monitoring 24x7x365?				10.6.1.d	Network Controls		
G.9.19.4	Event feeds into the Incident Management process?				N/A			
G.9.20	Is approval required prior to connecting any outbound or inbound modem lines, cable modem lines, DSL phone lines or wireless access points to a desktop or other access point directly connected to the company-managed network?				11.4.1.b	Policy On Use Of Network Services		
G.9.21	Are modems used? If so are they all set to auto-answer and required to use an authentication or encryption device?				11.4.2	User Authentication For External Connections		
G.10	**Is wireless networking technology used? Is so, is there:**			G.15 Unapproved Wireless Networks	10.6.1.c	Network Controls		
G.10.1	Approved and fully implemented wireless networking policy?				10.8.1.e	Information Exchange Policies And Procedures		
G.10.2	Two active network connections allowed at the same time (split-tunneling)?				N/A			
G.10.3	Wireless connections authenticated using multi-factor authentication?				11.4.2	User Authentication For External Connections		
G.10.4	Encrypted using strong encryption (WPA2 or higher)?			G.16 Wireless Networks Encryption	10.6.1	Network Controls		
G.10.5	Wireless access points SNMP community strings changed?				11.4.4	Remote Diagnostic And Configuration Port Protection		
G.10.6	Quarterly scans for rogue wireless access points?				N/A			
G.11	**Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy? If so, is:**				10.7.1	Management Of Removable Media		
G.11.1	Data encrypted while stored?				10.8.1.g	Information Exchange Policies And Procedures		

G. Communications and Operations Management

258 Total Questions to be Answered | 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.11.2	Sensitive data encrypted?				12.3.1.c	Policy On The Use Of Cryptographic Controls		
G.11.3	Is all media containing Scoped Systems and Data disposed of securely to prevent recovery?? If so, is it:				10.7.2	Disposal Of Media		
G.11.3.1	Logged to maintain an audit trail?				10.7.2.e	Disposal Of Media		
G.11.3.2	Made unrecoverable (wiped or overwritten) prior to asset reuse?				9.2.6	Secure disposal or re-use of equipment		
G.11.3.3	Inventoried at least quarterly?							
G.12	**Is Scoped Data sent or received electronically or via physical media? If so, is there:**				10.8.3	Physical Media In Transit		
G.12.1	Encryption in transit while outside the network?				10.8.1.g	Information Exchange Policies And Procedures		
G.12.2	Encryption in transit within the network?				N/A			
G.12.3	Protection against malicious code?				10.8.1	Information Exchange Policies And Procedures		
G.12.4	Confidentiality / integrity of data following any transmissions?				10.8.1	Information Exchange Policies And Procedures		
G.12.5	Review and approval process for transmissions?				N/A			
G.12.6	Transport containers to protect against physical damage?				10.8.3.b	Physical Media In Transit		
G.12.7	Locked or have tamper evident transport containers?				10.8.3.c	Physical Media In Transit		
G.12.8	Physical media tracking?				10.8.2.c	Exchange Agreements		
G.12.9	Protection when transmitted through email?				10.8.1	Information Exchange Policies And Procedures		
G.12.10	Encryption when sent through email?				10.8.1.g	Information Exchange Policies And Procedures		
G.12.11	Are content filtering scans performed on incoming/outgoing email to enforce email policy?				10.4.1.d.2	Controls Against Malicious Code		
G.13	**Do systems and network devices utilize a common time synchronization service?**				10.10.6	Clock Synchronization		
G.14	**Are UNIX or Linux operating systems used for transmitting, processing or storing Scoped Data? If so, is there:**				N/A			
G.14.1	UNIX hardening standards?			I.3 Secure System Hardening Standards	10.6.1.e	Network Controls		
G.14.1.1	Periodic monitoring for continued compliance to build standards and security requirements?				15.2.2	Technical Compliance Checking		
G.14.2	Are users required to 'su' or 'sudo' into root?				11.5.2	User Identification And Authentication		
G.14.3	Does remote SU/root access require multi-factor authentication?				11.7.1	Mobile Computing And Communications		
G.14.4	Are remote access tools that do not require authentication (e.g., rhost, shost, etc.) allowed?				11.4.2	User Authentication For External Connections		
G.14.5	Is access to modify startup and shutdown scripts restricted to root-level users?				11.5.4	Use Of System Utilities		
G.14.6	Are all unnecessary/unused services turned off?				11.5.4.h	Use Of System Utilities		
G.14.7	Are logs regularly reviewed using a specific methodology to uncover potential incidents?				10.10.2	Monitoring System Use		
G.14.8	Do operating system event logs contain sufficient detail to support incident investigation including failed login attempts?			G.7 Administrative Activity Logging, G.8 Log-on Activity Logging	10.10.1	Audit Logging		
G.14.9	Are operating system logs retained for a minimum of one year?			G.9 Log Retention	10.10.3	Protection Of Log Information		
G.14.10	In the event of an operating system audit log failure, does the system generate an alert?				10.10.5	Fault Logging		
G.14.11	Are audit logs stored on alternate systems?				10.10.3	Protection Of Log Information		
G.14.12	Are audit logs protected against modification, deletion, and/or inappropriate access?				10.10.3	Protection Of Log Information		
G.14.13	Minimum password length at least eight characters?			H.1 Password Controls	11.3.1.d	Password Use		

G. Communications and Operations Management

258 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.14.14	Complex passwords required?			H.1 Password Controls	11.3.1.d	Password Use		
G.14.15	Minimum password expiration at least 90 days?				11.3.1.c	Password Use		
G.14.16	Password history at least 12 before reuse?				11.5.3.f	Password Management System		
G.14.17	Initial password required to be changed at first logon?			H.1 Password Controls	11.3.1.f	Password use		
G.14.18	Passwords encrypted in transit?				11.5.1.i	Secure Log-On Procedures		
G.14.19	Passwords encrypted or hashed in storage?				11.5.3.i	Password Management System		
G.14.20	Passwords displayed when entered into a system?				11.5.1.g	Secure Log-On Procedures		
G.14.21	User accounts associated to a unique individual?				11.5.2	User Identification And Authentication		
G.14.22	Does the system lock an account when three to five invalid login attempts are made?				11.5.1.e	Secure Log-On Procedures		
G.15	**Are Windows systems used to transmit, process or store Scoped Data? If so, are there:**				N/A			
G.15.1	Windows hardening standards?			I.3 Secure System Hardening Standards	10.6.1.e	Network Controls		
G.15.1.1	Standard builds/security compliance checks?				15.2.2	Technical Compliance Checking		
G.15.2	Current patches?			I.4 System Patching	12.6.1.d	Control Of Technical Vulnerabilities		
G.15.3	Unnecessary/unused services turned off?				11.5.4.h	Use Of System Utilities		
G.15.4	Regular log reviews using a specific methodology to uncover potential incidents?				10.10.2	Monitoring System Use		
G.15.5	Sufficient information in the logs to evaluate incidents?			G.7 Administrative Activity Logging, G.8 Log-on Activity Logging	10.10.1	Audit Logging		
G.15.6	Logs retained for a minimum of one year?			G.9 Log Retention	10.10.3	Protection Of Log Information		
G.15.7	System generated alerts in the event of an audit log failure?				10.10.5	Fault Logging		
G.15.8	Audit logs stored on alternate systems?				10.10.3	Protection Of Log Information		
G.15.9	Audit logs protected against modification, deletion, and/or inappropriate access?				10.10.3	Protection Of Log Information		
G.15.10	Minimum password length at least eight characters?			H.1 Password Controls	11.3.1.d	Password Use		
G.15.11	Complex passwords required?			H.1 Password Controls	11.3.1.d	Password Use		
G.15.12	Minimum password expiration at least every 90 days?				11.3.1.c	Password Use		
G.15.13	Password history of 12 before reuse?				11.5.3.f	Password Management System		
G.15.14	Initial password required to be changed at first logon?			H.1 Password Controls	11.3.1.f	Password use		
G.15.15	Can a PIN or secret question be a stand-alone method of authentication?				11.3.1.d	Password Use		
G.15.16	Passwords encrypted in transit?				11.5.1.i	Secure Log-On Procedures		
G.15.17	Passwords encrypted or hashed in storage?				11.5.3.i	Password Management System		
G.15.18	Passwords displayed when entered into a system?				11.5.1.g	Secure Log-On Procedures		
G.15.19	User accounts associated to a unique individual?				11.5.2	User Identification And Authentication		
G.15.20	Does the system lock an account when three to five invalid login attempts are made?				11.5.1.e	Secure Log-On Procedures		
G.16	**Is a mainframe used to transmit, process or store Scoped Systems and Data? If so, are:**				N/A			
G.16.1	Mainframe security controls documented?				10.6.1.e	Network Controls		
G.16.1.1	Reviews performed to validate compliance with documented standards?				15.2.1	Compliance With Security Policies And Standards		
G.16.2	Transmission encrypted?				10.8.1.g	Information Exchange Policies And Procedures		

G. Communications and Operations Management

258 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.16.3	Authentication required for access to any transaction or database system?				11.6.1	Information Access Restriction		
G.16.4	Job scheduling systems secured to control the submission of production jobs?				11.5.4	Use Of System Utilities		
G.16.5	Storage management personnel (tape operators) given privileged access to mainframe systems?				11.5.4	Use Of System Utilities		
G.16.6	ESM (RACF) and inherent security configuration settings configured to support the access control standards and requirements?				10.6.1.e	Network Controls		
G.16.7	Regular review of logs using a specific methodology to uncover potential incidents?				10.10.2	Monitoring System Use		
G.16.8	System generated alerts in the event of an audit log failure?			G.7 Administrative Activity Logging, G.8 Log-on Activity Logging	10.10.1	Audit Logging		
G.16.9	Logs retained for a minimum of one year?			G.9 Log Retention	10.10.3	Protection Of Log Information		
G.16.10	Audit logs adequately protected against modification, deletion, and/or inappropriate access?				10.10.3	Protection Of Log Information		
G.16.11	Minimum password length at least eight characters?			H.1 Password Controls	11.3.1.d	Password Use		
G.16.12	Complex passwords required?			H.1 Password Controls	11.3.1.d	Password Use		
G.16.13	Minimum password expiration at least 90 days?				11.3.1.c	Password Use		
G.16.14	Password history of 12 before reuse?				11.5.3.f	Password Management System		
G.16.15	Password minimum age?				N/A			
G.16.16	Initial password required to be changed at first logon?			H.1 Password Controls	11.3.1.f	Password use		
G.16.17	Can a PIN or secret question be a stand alone method of authentication?				11.3.1.d	Password Use		
G.16.18	Passwords encrypted in transit?				11.5.1.i	Secure Log-On Procedures		
G.16.19	Passwords encrypted or hashed in storage?				11.5.3.i	Password Management System		
G.16.20	Passwords displayed when entered into a system?				11.5.1.g	Secure Log-On Procedures		
G.16.21	User accounts associated to a unique individual?				11.5.2	User Identification And Authentication		
G.16.22	Does the system lock an account when three to five invalid login attempts are made?				11.5.1.e	Secure Log-On Procedures		
G.16.23	Administrator intervention required to unlock an account?				11.5.1.e.2	Secure Log-On Procedures		
G.17	**Is an AS400 used to transmit, process or store Scoped Systems and Data? If so, are:**				N/A			
G.17.1	Security controls documented?				10.6.1.e	Network Controls		
G.17.1.1	Systems periodically monitored to ensure continued compliance with the documented standards?				15.2.2	Technical Compliance Checking		
G.17.2	Group profile assignments based on constituent role?				11.1.1.f	Access Control Policy		
G.17.3	Group profile assignments approved?				11.1.1.i	Access Control Policy		
G.17.4	User profiles created with the principle of least privilege?				11.1.1.B	Access Control Policy		
G.17.5	Logs regularly reviewed using a specific methodology to uncover potential incidents?				10.10.2	Monitoring System Use		
G.17.6	Sufficient information in the logs to evaluate incidents?			G.7 Administrative Activity Logging, G.8 Log-on Activity Logging	10.10.1	Audit Logging		
G.17.7	Logs retained for a minimum of one year?			G.9 Log Retention	10.10.3	Protection Of Log Information		
G.17.8	System generated alerts in the event of an audit log failure?				10.10.5	Fault Logging		
G.17.9	Audit logs protected against modification, deletion, and/or inappropriate access?				10.10.3	Protection Of Log Information		
G.17.10	Minimum password length at least eight characters:			H.1 Password Controls	11.3.1.d	Password Use		
G.17.11	Complex passwords required?			H.1 Password Controls	11.3.1.d	Password Use		
G.17.12	Minimum password expiration at least 90 days?				11.3.1.c	Password Use		

G. Communications and Operations Management

258 Total Questions to be Answered 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.17.13	Password history of 12 before reuse?				11.5.3.f	Password Management System		
G.17.14	Initial password required to be changed at first logon?			H.1 Password Controls	11.3.1.f	Password use		
G.17.15	Can a PIN or secret question be a stand alone method of authentication?				11.3.1.d	Password Use		
G.17.16	Passwords encrypted in transit?				11.5.1.i	Secure Log-On Procedures		
G.17.17	Passwords encrypted or hashed in storage?				11.5.3.i	Password Management System		
G.17.18	Passwords displayed when entered into a system?				11.5.1.g	Secure Log-On Procedures		
G.17.19	User accounts associated to a unique individual?				11.5.2	User Identification And Authentication		
G.17.20	Does the system lock an account when three to five invalid login attempts are made?				11.5.1.e	Secure Log-On Procedures		
G.17.21	Users required to log off when the session is finished?				11.3.2.b	Unattended User Equipment		
G.18	**Is an Open VMS (VAX or Alpha) system used to transmit, process or store Scoped Systems and Data? If so, are:**				N/A			
G.18.1	Administrative privilege restricted to those responsible for VMS administration?				11.2.2.b	Privilege Management		
G.18.2	Logs regularly reviewed using a specific methodology to uncover potential incidents?				10.10.2	Monitoring System Use		
G.18.3	Sufficient information to investigate incidents including (failed login attempts)?			G.7 Administrative Activity Logging, G.8 Log-on Activity Logging	10.10.1	Audit Logging		
G.18.4	Logs retained for a minimum of one year?			G.9 Log Retention	10.10.3	Protection Of Log Information		
G.18.5	System generated alerts in the event of an audit log failure?				10.10.5	Fault Logging		
G.18.6	Are audit logs protected against modification, deletion, and/or inappropriate access?				10.10.3	Protection Of Log Information		
G.18.7	Minimum password length at least eight characters?			H.1 Password Controls	11.3.1.d	Password Use		
G.18.8	Complex passwords required?			H.1 Password Controls	11.3.1.d	Password Use		
G.18.9	Minimum password expiration at least every 90 days?				11.3.1.c	Password Use		
G.18.10	Password history of 12 before reuse?				11.5.3.f	Password Management System		
G.18.11	Initial password required to be changed at first logon?			H.1 Password Controls	11.3.1.f	Password use		
G.18.12	Can a PIN or secret question be a stand alone method of authentication?				11.3.1.d	Password Use		
G.18.13	Passwords encrypted in transit?				11.5.1.i	Secure Log-On Procedures		
G.18.14	Passwords encrypted or hashed in storage?				11.5.3.i	Password Management System		
G.18.15	Passwords displayed when entered into a system?				11.5.1.g	Secure Log-On Procedures		
G.18.16	User accounts associated to a unique individual?				11.5.2	User Identification And Authentication		
G.18.17	Does the system lock an account when three to five invalid login attempts are made?				11.5.1.e	Secure Log-On Procedures		
G.19	**Are Web services provided? If so, are:**				N/A			
G.19.1	Electronic commerce web sites or applications used to transmit, process or store Scoped Systems and Data?				10.9.1	Electronic Commerce		
G.19.1.1	Cryptographic controls used for the electronic commerce application (SSL)?			G.11 Website – Client Encryption	10.9.1	Electronic Commerce		
G.19.1.2	Users required to authenticate to the application?				10.9.1.a	Electronic Commerce		
G.19.1.3	Transaction details stored in the DMZ?				10.9.2.e	On-Line Transactions		
G.19.2	Is Windows IIS for these Web services used? If so, is:				N/A			
G.19.2.1	Anonymous access to FTP disabled?				10.8.2	Exchange Agreements		
G.19.2.2	Membership to the IIS Administrators group restricted to those with web administration roles and responsibilities?				11.2.2.b	Privilege Management		
G.19.2.3	Dedicated virtual directory structure used for each website?				10.8.1	Information Exchange Policies And Procedures		
G.19.2.4	Unused services turned off on IIS servers?				11.5.4.h	Use Of System Utilities		

G. Communications and Operations Management

258 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
G.19.2.5	Services running on standard ports?				N/A			
G.19.2.6	Logging configured to support incident investigation?				10.10.1	Audit Logging		
G.19.2.7	Sample applications and scripts removed?				11.5.4.h	Use Of System Utilities		
G.19.2.8	Least privilege used when setting IIS content permissions?				11.2.1.c	User Registration		
G.19.2.9	Content folder on the same drive as the operating system?				N/A			
G.19.3	Is Apache used for these Web services? If so, is:				N/A			
G.19.3.1	Logging configured to support incident investigation?				10.10.1	Audit Logging		
G.19.3.2	Anonymous access to FTP disabled?				10.8.2	Exchange Agreements		
G.19.3.3	Membership to the Apache group restricted to those with web administration roles and responsibilities?				11.2.2.b	Privilege Management		
G.19.3.4	Dedicated virtual directory structure used for each website?				N/A			
G.19.3.5	Configuration options restricted to authorized users?				10.8.5.g	Business Information Systems		
G.19.3.6	Services run on standard ports?				N/A			
G.19.3.7	Sample applications and scripts removed?				11.5.4.h	Use Of System Utilities		
G.19.3.8	Least privilege used when setting permissions?				11.2.1.c	User Registration		
G.20	**Are desktop computers used to transmit, process or store Scoped Systems and Data. If so, is:**				N/A			
G.20.1	Segregation of duties for granting access and approving access?				11.1.1.h	Access Control Policy		
G.20.2	Segregation of duties for approving and implementing access requests?				10.1.3	Segregation Of Duties		
G.20.3	User able to use removable media (floppy disk, recordable CD, USB drive) without detection?							
G.20.4	User of a system also responsible for reviewing its security audit logs?				10.1.3	Segregation Of Duties		
G.20.5	Segregation of duties to prevent the user of a system from modifying or deleting its security audit logs?				10.1.3	Segregation Of Duties		
G.20.6	Standard operating environment required?				10.6.1.e	Network Controls		
G.20.7	Content filtering proxy used prior to accessing the Internet?				11.4.7	Network Routing Control		
G.20.8	Security approval required prior to implementing non-standard operating equipment?				15.1.5	Prevention Of Misuse Of Information Processing Facilities		
G.20.9	Security approval required prior to implementing freeware or shareware applications?				15.1.5	Prevention Of Misuse Of Information Processing Facilities		
G.20.10	Non-company managed PCs used to connect to the company network without detection?				N/A			
G.20.11	Installation of software on company-owned equipment (workstations, mobile devices) restricted to administrators?				10.8.5.g	Business Information Systems		
G.20.12	Users permitted to execute mobile code?				10.4.2	Controls Against Mobile Code		
G.20.13	Mobile devices used?				11.7.1	Mobile Computing And Communications		
G.20.14	Encryption used to secure mobile computing devices?				11.7.1	Mobile Computing And Communications		

H. Access Control

57 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
H.1	**Are electronic systems used to transmit, process or store Scoped Systems and Data?**				N/A			
H.1.1	Is there an access control policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?			B.1 Information Security Policy Content	11.1.1	Access Control Policy		
H.1.2	Does access control on applications, operating systems, databases, and network devices ensure users have least privilege?				11.1.1.c	Access Control Policy		
H.2	**Are unique user IDs used for access?**				11.2.1.a	User Registration		
H.2.1	Can a user ID contain personal information (SSN, access level, admin of the user)?				N/A			
H.2.2	Is an inactive user ID deleted or disabled within 90 days?			H.4 Inactive Accounts	N/A			
H.2.3	Can a user ID be shared?				11.2.1.a	User Registration		
H.2.4	Is there a process to grant and approve access to systems transmitting, processing or storing Scoped Systems and Data?				11.2.1	User Registration		
H.2.4.1	Does access to electronic systems include a formal request and management approval?			H.3 Logical Access Authorization	N/A			
H.2.4.2	Are approved requests for granting access logged, archived and maintained?				11.2.1.g	User Registration		
H.2.5	Is system access limited by:				11.2.1.c	User Registration		
H.2.5.1	Time of day?				11.5.6	Limitation Of Connection Time		
H.2.5.2	Physical location?				N/A			
H.2.5.3	Network subnet?				N/A			
H.2.6	Are user access rights reviewed at least quarterly?				11.2.4.a	Review Of User Access Rights		
H.2.7	Are access rights reviewed when a constituent changes roles?				11.2.4.b	Review Of User Access Rights		
H.2.8	Are reviews of privileged systems conducted to ensure unauthorized privileges have not been obtained?				11.2.4.d	Review Of User Access Rights		
H.2.9	Are privileged user access rights reviewed at least quarterly?				11.2.4.c	Review Of User Access Rights		
H.2.10	Are changes to privileged user access rights logged?				11.2.4.e	Review Of User Access Rights		
H.2.11	Are there logon banners for all electronic systems access?			L.1 Presence of Log-on Banners	11.5.1.b	Secure Log-On Procedures		
H.2.12	Upon logon failure, does the error message describe the cause of the failure to the user (Invalid password, invalid user ID, etc.)?				11.5.1.c	Secure Log-On Procedures		
H.2.13	Upon successful logon, does a message indicate the last time of successful logon?				11.5.1.g	Secure Log-On Procedures		
H.2.14	Is multi-factor authentication deployed for “high-risk” environments?				11.5.2	User Identification And Authentication		
H.2.15	Do all users have a unique user ID when accessing applications?				11.5.2	User Identification And Authentication		
H.2.16	Is the use of system utilities restricted to authorized users only?				11.5.4	Use Of System Utilities		
H.2.17	Do inactive workstation lock within 15 minutes?			H.5 Controls for Unattended Systems	11.5.5	Session Time-Out		
H.2.18	Do inactive sessions timeout within 15 minutes?			H.5 Controls for Unattended Systems	11.5.5	Session Time-Out		
H.3	**Is application development performed? If so, are developers permitted to:**				11.6	Application and information access control		
H.3.1	Access production environments, including read only access?				12.4.3.c	Access Control To Program Source Code		
H.3.2	Access systems and applications based on established profiles that define responsibilities or job functions?				11.1.1	Access Control Policy		
H.3.3	Request or obtain access outside an established role (emergency access)?				11.2.2.b	Privilege Management		
H.3.4	Are system, vendor, or service accounts disallowed for normal operations and monitored for usage?							

H. Access Control

57 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
H.4	**Are passwords required to access systems transmitting, processing or storing Scoped Systems and Data?**				11.2.3	User Password Management		
H.4.1	Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management and communicated to appropriate constituents? If so, does it include:				11.2.3	User Password Management		
H.4.1.1	Keep passwords confidential?							
H.4.1.2	Not keep a record of passwords (paper, software file or handheld device)?							
H.4.1.3	Change passwords when there is an indication of possible system or password compromise?							
H.4.1.4	Change passwords at regular intervals?							
H.4.1.5	Change temporary passwords at first logon?							
H.4.1.6	Not include passwords in automated logon processes? (stored in a macro or function key)?							
H.4.1.7	Terminate or secure active sessions when finished?							
H.4.1.8	Logoff terminals, PC or servers when the session is finished?							
H.4.1.9	Lock (using key lock or equivalent control) when systems are unattended?							
H.4.1.10	Prohibit users from sharing passwords?							
H.4.2	Are strong passwords required on systems transmitting, processing storing Scoped Systems and Data?				11.5.2	User Identification And Authentication		
H.4.3	Are password files and application system data stored in different file systems?				11.5.3.h	Password Management System		
H.4.4	Are user ID and passwords communicated/distributed via separate media (e-mail and phone)?				N/A			
H.4.5	Are new constituents issued random initial single use passwords?				11.2.3.b	User Password Management		
H.4.6	Do temporary passwords expire within 10 days?							
H.4.7	Is a user's identity verified prior to resetting a password?				N/A			
H.4.8	Are vendor default passwords removed, disabled or changed prior to placing the device or system into production?				11.2.3.h	User Password Management		
H.4.9	Is password reset authority restricted to authorized persons and/or an automated password reset tool?							
H.5	**Is remote access permitted?**				11.7	Mobile Computing And Teleworking		
H.5.1	Is there a remote access policy for systems transmitting, processing and storing Scoped Systems and Data that has been approved by management and communicated to appropriate constituents?				11.7.1	Mobile Computing And Communications		
H.5.2	Is split tunneling or bridged internet connections allowed by policy and/or technical control?				N/A			
H.5.3	Is only company owned equipment permitted to connect remotely?				N/A			
H.5.4	Is remote desktop technology (Citrix) used to access the network remotely?				11.7.1	Mobile Computing And Communications		
H.5.5	Are remote users prevented from copying data to remote devices?				N/A			
H.5.6	Are encrypted communications required for all remote connections?							
H.5.7	Is multi-factor authentication required for remote access?			H.8 Two-Factor Authentication for Remote Access	11.7.1	Mobile Computing And Communications		

I. Information Systems Acquisition Development & Maintenance

76 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
I.1	**Are business information systems used to transmit, process or store Scoped Systems and Data? If so, are:**				12.1.1	Security Requirements Analysis And Specification		
I.1.1	Security requirements documented?				12.1.1	Security Requirements Analysis And Specification		
I.1.2	Information security reviews conducted and approved for the use or installation of open source software (Linux, Apache, etc.)?				12.1.1	Security Requirements Analysis And Specification		
I.2	**Is application development performed? If so, does it provide:**				12.5	Security In Development And Support Processes		
I.2.1	Independent security evaluation or certification?				N/A			
I.2.2	Formal application methodology (OWASP)?				N/A			
I.2.3	An authenticated and maintained state for every data transaction?				11.5.6	Limitation Of Connection Time		
I.2.4	A means for secure session management?				11.5.6	Limitation Of Connection Time		
I.2.5	Comprehensive secure error handling?				12.2.2	Control Of Internal Processing		
I.2.6	Audit log failures and generate an alert?				10.10.5	Fault Logging		
I.2.7	Is there a formal Software Development Life Cycle (SDLC) process? If so, does it include:				12.5	Security In Development And Support Processes		
I.2.7.1	Peer code review, integration testing, and acceptance testing?				12.5.1	Change Control Procedures		
I.2.7.2	Separate source code repositories for production and non-production?				12.4.3.a	Access Control To Program Source Code		
I.2.8	Do IT support personnel have access to program source libraries?				12.4.3.c	Access Control To Program Source Code		
I.2.9	Is all access to program source libraries logged?				12.4.3.f	Access Control To Program Source Code		
I.2.10	Are change control procedures required for all changes to the production environment?				12.4.3.g	Access Control To Program Source Code		
I.2.11	Do applications provide granular and comprehensive logging?				10.10.1	Audit Logging		
I.2.12	Are application sessions set to time out within 15 minutes or less?				11.5.5	Session Time-Out		
I.2.13	Is application development Third party / outsourced developers onshore?				12.5.5	Outsourced Software Development		
I.2.14	Is application development Third party / outsourced developers offshore?				12.5.5	Outsourced Software Development		
I.2.15	Are there access controls to protect source code and test data?				12.4.3	Access Control To Program Source Code		
I.2.16	Does the version management system provide segregation of code, data and environments?				N/A			
I.2.17	Do changes to applications or application code go through a risk assessment including application testing?				12.5.1	Change Control Procedures		
I.2.18	Is Scoped Systems and Data ever used in the test, development, or QA environments? If so, is:				12.4.2	Protection Of System Test Data		
I.2.18.1	Authorization required when production data is copied to the test environment?				12.4.2.b	Protection Of System Test Data		
I.2.18.2	Test data destroyed following the testing phase?				12.4.2.c	Protection Of System Test Data		
I.2.18.3	Test data masked or obfuscated during the testing phase?				12.4.2	Protection Of System Test Data		
I.2.18.4	Copying to the test environment logged?				12.4.2.d	Protection Of System Test Data		
I.2.19	Are access control procedures the same for both the test and production environment?				12.4.2.a	Protection Of System Test Data		
I.2.20	Prior to implementation, do applications go through a risk assessment and approval by security?				12.5.1	Change Control Procedures		
I.2.21	Is Internet facing software and infrastructure tested prior to implementation? If so, does the testing include:				6.1.8	Independent Review Of Information Security		
I.2.21.1	Issue tracking and resolution?				6.1.8	Independent Review Of Information Security		

I. Information Systems Acquisition Development & Maintenance

76 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
I.2.21.2	Metrics on software defects and release incidents?				6.1.8	Independent Review Of Information Security		
I.2.22	Is there a documented change management / change control process? If so, does it include:				12.5.1	Change Control Procedures		
I.2.22.1	Testing prior to deployment?				12.4.1.c	Control Of Operational Software		
I.2.22.2	Management approval prior to deployment?				12.5.1.e	Change Control Procedures		
I.2.22.3	Establishment of restart points?				12.4.1.e	Control Of Operational Software		
I.2.22.4	Management approval for changes?				12.5.1.e	Change Control Procedures		
I.2.22.5	Requirements for the transfer of software from development to production?				10.4.2.a	Controls Against Mobile Code		
I.2.22.6	Review of code changes by information security?			I.2 Secure Systems Development Life Cycle (SDLC) code reviews	12.4.1.c	Control Of Operational Software		
I.2.22.7	Stakeholder communication and/or approvals?				12.5.1.a	Change Control Procedures		
I.2.22.8	A list of individuals authorized to approve changes?				12.5.1.b	Change Control Procedures		
I.2.22.9	An impact assessment to review of all affected systems and applications?				12.5.1.d	Change Control Procedures		
I.2.22.10	Documentation for all system changes?				12.5.1.g	Change Control Procedures		
I.2.22.11	Version control for all software?				12.5.1.h	Change Control Procedures		
I.2.22.12	Logging of all change requests?				12.5.1.i	Change Control Procedures		
I.2.22.13	Changes only take place during specified and agreed upon times (green zone)?				12.5.1.k	Change Control Procedures		
I.2.22.14	Modifications and changes to software are strictly controlled?				12.5.1	Change Control Procedures		
I.2.23	Are audit logs maintained and reviewed for all program library updates?				12.4.1.f	Control Of Operational Software		
I.2.24	Are compilers, editors or other development tools present in the production environment?				10.1.4.c	Separation Of Development, Test, And Operational Facilities		
I.3	**Are systems and applications patched? If so, does the process include:**			I.4 System Patching	12.6.1	Control Of Technical Vulnerabilities		
I.3.1	Testing of patches, service packs, and hot fixes prior to installation?				12.6.1.g	Control Of Technical Vulnerabilities		
I.3.2	Evaluation and prioritize vulnerabilities?				12.6.1.g	Control Of Technical Vulnerabilities		
I.3.3	Logging?				12.6.1.h	Control Of Technical Vulnerabilities		
I.3.4	Priority patching of high-risk systems first?				12.6.1.j	Control Of Technical Vulnerabilities		
I.3.5	Are third party alert services used to keep up to date with the latest vulnerabilities?				12.6.1.b	Control Of Technical Vulnerabilities		
I.4	**Is a web site supported, hosted or maintained that has access to Scoped Systems and Data? If so, are these controls in place:**				N/A			
I.4.1	Regular penetration tests executed against web-based applications?			I.1 Application Vulnerability Assessments/Ethical Hacking	15.2.2	Technical Compliance Checking		
I.4.2	Physical separation of server components (web, application, database)?				11.6.1	Information Access Restriction		
I.4.3	Web applications configured to follow best practices or security guidelines (OWASP)?				N/A			
I.4.4	Data input into applications validated for accuracy?				12.2.1	Input Data Validation		
I.4.5	Do validation checks include cross site scripting and SQL injections?				12.2.1	Input Data Validation		
I.5	**Are vulnerability tests (internal/external) performed on all applications at least annually? If so, are there:**			I.1 Application Vulnerability Assessments/Ethical Hacking	15.2.2	Technical Compliance Checking		

I. Information Systems Acquisition Development & Maintenance

76 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
I.5.1	Results tracked, remediated and reported to management?				15.2.1.a	Compliance With Security Policies And Standards		
I.5.2	Processes to manage threat and vulnerability assessment tools and the data they collect?				15.3.2	Protection Of Information Systems Audit Tools		
I.6	**Are encryption tools managed and maintained for Scoped Data? If so, is there:**				N/A			
I.6.1	An encryption policy?				12.3.1	Policy On The Use Of Cryptographic Controls		
I.6.2	Encryption in storage / at rest?				10.8.1.g	Information Exchange Policies And Procedures		
I.6.3	Is encrypted Scoped Data ever visible in clear text by anyone including systems administrators?							
I.6.4	Centralized key management system?				12.3.2	Key Management		
I.6.5	Encryption keys encrypted at rest and when transmitted?				N/A			
I.6.6	Segregation of duties between key management duties and normal operational duties?				10.1.3	Segregation Of Duties		
I.6.7	Key/certificate sharing between production and non-production?				10.1.4.f	Separation Of Development, Test, And Operational Facilities		
I.6.8	Default certificates provided by vendors replaced with proprietary certificates?				11.2.3.h	User Password Management		
I.6.9	Segregation of access to both parts of a symmetric key?				12.3.2.A	Key Management		
I.6.10	Asymmetric encryption key length a minimum of 256 bit?				N/A			

J. Incident Event and Communications Management

32 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
J.1	**Is there an Incident Management program?**				N/A			
J.1.1	Is there a documented policy for incident management that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?			J.1 Information Security Incident Management Policy and Procedures Content	13.1.1	Reporting Information Security Events		
J.1.2	Is there a formal Incident Response Plan. If so, does it include:				13.1.1	Reporting Information Security Events		
J.1.2.1	Reporting procedure for an information security event?				13.1.1	Reporting Information Security Events		
J.1.2.2	Escalation procedure?				13.1.1	Reporting Information Security Events		
J.1.2.3	An Incident / Event Response team with defined roles and response related qualifications available 24x7x365?				13.1.1	Reporting Information Security Events		
J.1.2.4	Procedures to collect and maintain a chain of custody for evidence during incident investigation?				13.2.3	Collection Of Evidence		
J.1.2.5	Feedback process to ensure those reporting information security events are notified of the results after the issue has been dealt with and closed?				13.1.1.a	Reporting Information Security Events		
J.1.2.6	Event reporting mechanism to support the reporting action, and to list all necessary actions in case of an information security event?				13.1.1.b	Reporting Information Security Events		
J.1.2.7	Actions to be taken in the event of an information security event?				13.1.1.c	Reporting Information Security Events		
J.1.2.8	Formal disciplinary process for dealing with those who commit a security breach?				13.1.1.d	Reporting Information Security Events		
J.1.2.9	Process for assessing and executing client and third party notification requirements (legal, regulatory, and contractual)?				13.1.1	Reporting Information Security Events		
J.1.2.10	Postmortem to include root cause analysis and remediation plan, provided to leadership?				13.1.2	Reporting Security Weaknesses		
J.1.2.11	Is there an identification of incident process? If so, does it include:				N/A			
J.1.2.11.1	Unauthorized physical access?				13.1.1	Reporting Information Security Events		
J.1.2.11.2	Information system failure or loss of service?				13.2.1.a.1	Responsibilities And Procedures		
J.1.2.11.3	Malware activity (anti-virus, worms, Trojans)?				13.2.1.a.2	Responsibilities And Procedures		
J.1.2.11.4	Denial of service?				13.2.1.a.3	Responsibilities And Procedures		
J.1.2.11.5	Errors resulting from incomplete or inaccurate business data?				13.2.1.a.4	Responsibilities And Procedures		
J.1.2.11.6	Breach or loss of confidentiality?				13.2.1.a.5	Responsibilities And Procedures		
J.1.2.11.7	System exploit?				13.2.1.a.6	Responsibilities And Procedures		
J.1.2.11.8	Unauthorized logical access or use of system resources?				13.2.1.a.6	Responsibilities And Procedures		
J.1.2.11.9	Containment?				13.2.1.b.2	Responsibilities And Procedures		
J.1.2.11.10	Remediation?				13.2.1.b.3	Responsibilities And Procedures		
J.1.2.11.11	Notification of stakeholders?				13.2.1.b.4	Responsibilities And Procedures		
J.1.2.11.12	Tracking?				13.2.1.c	Responsibilities And Procedures		
J.1.2.11.13	Repair?				13.2.1.d	Responsibilities And Procedures		
J.1.2.11.14	Recovery?				13.2.1.d	Responsibilities And Procedures		
J.1.2.11.15	Feedback and lessons learned?				13.2.2	Learning From Information Security Incidents		

J. Incident Event and Communications Management

32 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
J.1.2.11.16	Unique, specific, applicable data breach notification requirements, including timing of notification (HIPAA/HITECH, state breach laws, client contracts)?							
J.1.2.11.17	Annual testing of the procedures?				13.2.2	Learning From Information Security Incidents		
J.1.3	Are the following considered Information Security events:				N/A			
J.1.3.1	Loss of service (equipment or facility)?				13.1.1.A	Reporting Information Security Events		
J.1.3.2	System malfunction or overload?				13.1.1.B	Reporting Information Security Events		
J.1.3.3	Human error?				13.1.1.C	Reporting Information Security Events		
J.1.3.4	Non-compliance with policy or guidelines?				13.1.1.D	Reporting Information Security Events		
J.1.3.5	Breach of physical security arrangement?				13.1.1.E	Reporting Information Security Events		
J.1.3.6	Uncontrolled system change?				13.1.1.F	Reporting Information Security Events		
J.1.3.7	Malfunction of software or hardware?				13.1.1.G	Reporting Information Security Events		
J.1.3.8	Access violation?				13.1.1.H	Reporting Information Security Events		
J.1.3.9	Physical asset loss or theft?				N/A			

K. Business Continuity and Disaster Recovery

58 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
K.1	**Is there a documented policy for business continuity and disaster recovery that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?**			B.1 Information Security Policy Content	N/A			
K.1.1	Has a third party evaluated the BC/DR Program within the past 12 months?				N/A			
K.1.2	Is there a BC/DR Program that has been approved by management, communicated to appropriate constituents and an owner or group to maintain and review the plan? If so ,does it include:				5.1.1.d.3	Information security policy document		
K.1.2.1	Annual management review of the BC program for adequacy of resources (people, technology, facilities, and funding)?				N/A			
K.1.2.2	Virtual or physical command center where management can meet, organize, and conduct emergency operations in a secure setting?				N/A			
K.1.2.3	The product or service in scope have an assured business continuity capability?				14.1.4	Business Continuity Planning Framework		
K.1.2.4	Conditions for activating the plan, and the associated roles and responsibilities?				14.1.4.a	Business Continuity Planning Framework		
K.1.2.5	Maintenance schedule to revise and test the plan?				14.1.4.f	Business Continuity Planning Framework		
K.1.2.6	Awareness and education activities?				14.1.4.g	Business Continuity Planning Framework		
K.1.2.7	Roles and responsibilities for those who invoke and execute the plan?				14.1.4.h	Business Continuity Planning Framework		
K.1.2.8	Change management to ensure changes are replicated to contingency environments?				N/A			
K.1.2.9	Identification of applications, equipment, facilities, personnel, supplies and vital records necessary for recovery?				14.1.1.b	Including Information Security In The Business Continuity Management Process		
K.1.2.10	Updates from the inventory of IT and telecom assets?				14.1.1.b	Including Information Security In The Business Continuity Management Process		
K.1.2.11	Alternate and diverse means of communications in the event standard communication channels are unavailable?				14.1.3.c	Developing And Implementing Continuity Plans Including Information Security		
K.1.2.12	Interaction with the media during an event?				N/A			
K.1.2.13	Resumption procedures to return to normal business operations?				14.1.4.e	Business Continuity Planning Framework		
K.1.2.14	Notification and escalation to clients?				N/A			
K.1.2.15	Dependencies upon critical service providers. If so, does it include:				14.1.3.c	Developing And Implementing Continuity Plans Including Information Security		
K.1.2.15.1	Contact information for key personnel, which is updated at least annually?				14.1.4.h	Business Continuity Planning Framework		
K.1.2.15.2	Notification and escalation?				14.1.4.b	Business Continuity Planning Framework		
K.1.2.15.3	Communication in the event of a disruption at their facility?				14.1.3.c	Developing And Implementing Continuity Plans Including Information Security		
K.1.2.15.4	Capabilities adequate to support the plan through contract requirements, SAS 70 reviews or both?				14.1.3.c	Developing And Implementing Continuity Plans Including Information Security		

K. Business Continuity and Disaster Recovery

58 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
K.1.2.15.5	Notification when their BCP is modified?				14.1.3	Developing And Implementing Continuity Plans Including Information Security		
K.1.2.16	Annual review which includes: critical functions, organizational structure and personnel changes?				N/A			
K.1.3	Is there an annual schedule of required tests? If so, does it include:				14.1.5	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.3.1	Test objectives for a technology outage, loss of facility or personnel, identification of parties involved, and the evaluation of testing results?				14.1.5.d, 14.1.5.c	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4	Are BC/DR tests conducted at least annually? If so, do they include:				N/A			
K.1.4.1	Evacuation drills?				N/A			
K.1.4.2	Notification tests?				N/A			
K.1.4.3	Tabletop exercises?				14.1.5.a	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4.4	Application recovery tests?				N/A			
K.1.4.5	Remote access tests?				N/A			
K.1.4.6	Full scale exercises?				14.1.5.f	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4.7	Business relocation test?				14.1.5.e	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4.8	Business disruptions?							
K.1.4.9	Data center failover test?				14.1.5.e	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4.10	Critical service providers included in testing?				14.1.5.e	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4.11	Recovery site tests?				14.1.5.d	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.1.4.12	Assessment of the Ability to retrieve vital records?				14.1.5.c	Testing, Maintaining And Re-Assessing Business Continuity Plans		
K.2	**Is there a Pandemic Plan? If so, does it include:**				14.1.2	Business Continuity And Risk Assessment		
K.2.1	Trigger points for activating the plan?				N/A			
K.2.2	Travel and visitor restrictions?				N/A			
K.2.3	Cleaning and disinfecting protocols?				N/A			
K.2.4	Pandemic-specific HR policies and procedures?				N/A			
K.2.5	Specific "Social Distancing" criteria / techniques (work from home)?				N/A			
K.2.6	Personal protective equipment for constituents (face masks)?				N/A			
K.2.7	Special food handling in cafeterias?				N/A			
K.2.8	Seasonal flu vaccinations for constituents?				N/A			
K.2.9	Annual review?				N/A			
K.2.10	Periodic testing of the plan?				N/A			
K.2.11	Verification of critical service provider pandemic plans?				N/A			
K.2.12	Business Impact Analysis?				14.1.2	Business Continuity And Risk Assessment		
K.3	**Is a Business Impact Analysis conducted at least annually? If so, does it include:**				14.1.2	Business Continuity And Risk Assessment		

K. Business Continuity and Disaster Recovery

58 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
K.3.1	Business Process Criticality (high, medium, low or numerical rating) that distinguishes the relative importance of each process?				14.1.1.a	Including Information Security In The Business Continuity Management Process		
K.3.2	Recovery Time Objective?				N/A			
K.3.3	Recovery Point Objective?				N/A			
K.3.4	Maximum allowable downtime?				N/A			
K.3.5	Impact to clients?				N/A			

L. Compliance

12 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
L.1	**Is there an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues?**				6.1.2	Information security co-ordination		
L.2	**Are audits performed to ensure compliance with any legal, regulatory or industry requirements?**				N/A			
L.3	**Is there a process used to manage the controls on a life cycle basis?**				N/A			
L.4	**Are there procedures to ensure compliance with legislative, regulatory, and contractual requirements on the use of material where intellectual property rights may be applied and on the use of proprietary software products?**				15.1.2	Intellectual Property Rights (Pier)		
L.5	**Is there a records retention policy covering paper and electronic records, including email, in support of applicable regulations, standards and contractual requirements?**				15.1.3	Protection Of Organizational Records		
L.6	**Are encryption tools managed and maintained?**				N/A			
L.7	**Does management regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements?**				15.2.1	Compliance With Security Policies And Standards		
L.8	**Has a review of security policies, standards, procedures, and/or guidelines been performed within the last 12 months?**				15.2.1	Compliance With Security Policies And Standards		
L.9	**Are information systems regularly checked for compliance with security implementation standards?**			L.2 Technical Compliance Checking – Vulnerability Testing and Remediation	15.2.2	Technical Compliance Checking		
L.10	**Has a network penetration test been conducted within the last 12 months?**			L.2 Technical Compliance Checking – Vulnerability Testing and Remediation	15.2.2	Technical Compliance Checking		
L.11	**Is there an independent audit function within the organization?**				15.3.1	Information Systems Audit Controls		
L.12	**Are information systems audit tools (e.g., software or data files) protected and separated from development and operational systems nor held in tape libraries or user areas?**				15.3.2	Protection Of Information Systems Audit Tools		

P. Privacy

65 Total Questions to be Answered 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
P.1	**Is there a dedicated person (or group) responsible for privacy compliance? If yes, describe. If no, explain reason.**							
P.2	**Is there a formally documented privacy policy (or policies)? If yes, describe. If no, explain reason.**							
P.2.1	Is the privacy policy (or policies) reviewed by a licensed, qualified attorney?							
P.2.2	Is the privacy policy (or policies) approved by the organization's senior management?							
P.2.3	Is the privacy policy (or policies) reviewed and revised (as needed) on a regular basis (e.g. annually)?							
P.3	**Are there regular privacy risk assessments? If yes, provide frequency and scope. If no, explain reason.**							
P.3.1	Are identified privacy risks and associated mitigation plans formally documented?							
P.3.2	Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?							
P.4	**Is there formal privacy awareness training for employees, contractors, volunteers (and other parties, as appropriate)? If yes, provide frequency and scope. If no, explain reason.**							
P.4.1	Is proof of privacy training formally documented and appropriately retained?							
P.4.2	Is privacy training updated as needed?							
P.4.3	Are employees, contractors, volunteers (and other parties, as appropriate) re-trained when privacy training is updated?							
P.5	**Is personal information about individuals transmitted to or received from non-US countries? If yes, identify the countries.**							
P.6	**Is there a process for responding to a privacy incident? If yes, describe. If no, explain reason.**							
P.6.1	Are privacy incident response plans formally documented and updated regularly?							
P.7	**Is personal information collected directly from individuals as a service to the client? If yes, describe the information collected.**							
P.7.1	Are controls in place to ensure that the collection of personal information is limited to the contract between the client and service provider?							
P.7.2	Are controls in place to ensure that the collection of personal information is fair and lawful?							
P.7.3	Are controls in place to ensure that third parties contracted by the service provider collect information fairly and lawfully?							
P.7.4	If personal information is collected directly from individuals as a service to the client, are individuals from whom personal information is collected provided with appropriate notice? If yes, describe. If no, explain reason.							
P.7.4.1	Does the notice describe the types of personal information collected?							
P.7.4.2	Does the notice describe purposes for which the information will be used?							
P.7.4.3	Does the notice describe the categories of people within the organization who will have access to the information?							
P.7.4.4	Does the notice describe categories of third parties with which the information will be shared?							
P.7.4.5	Does the notice describe the length of time that the information will be retained?							
P.7.4.6	Does the notice provide details on the access and correction rights available to the individual?							
P.7.4.7	Does the notice describe an individual's right to object to certain types of processing of their information (e.g., direct marketing)?							

P. Privacy

65 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
P.7.4.8	Does the notice describe the countries in which the information will be accessible or to which the information will be transferred?							
P.7.4.9	Does the notice provide contact information for questions or complaints?							
P.7.4.10	Is the notice provided to individuals prior to or at the time of collection?							
P.7.4.11	Is the notice provided in the local language or in the same language as other employment documents (in the case of employees) or marketing materials (in the case of customers)?							
P.7.4.12	If business practices change with respect to individual notice, are individuals provided a revised notice prior to implementation of the changes?							
P.7.5	Is the notice reviewed and updated (as needed) at least annually? If yes, describe. If no, explain reason.							
P.7.5.1	Is the notice reviewed by a licensed, qualified attorney?							
P.7.6	If personal information is collected directly from individuals as a service to the client, are individuals from whom personal information is collected provided with appropriate choice and consent options? If yes, describe. If no, explain reason.							
P.7.6.1	Is the choice and consent language included on the privacy policy?							
P.7.6.2	Does the choice and consent language cover the collection, use, and cross-border transfer of personal information?							
P.7.6.3	Are there documented processes to allow an individual to remove his/her consent to share personal information?							
P.7.6.4	Are there documented processes to facilitate the removal of consent, or consent, to/from the service provider's third party contractors?							
P.7.6.5	Are there controls to ensure that choice and consent language is followed?							
P.7.6.6	Are there any exemptions or restrictions regarding an individual's choice and/or consent to allow the service provider to share personal information?							
P.8	**Is there a document retention program that isolates protected subsets of sensitive or confidential information for special handling? If yes, identify the subsets and describe the process for isolating these subsets.**							
P.9	**If the service provider hosts and/or maintains (as a service to the client) data about an individual, does the organization provide appropriate controls to ensure the privacy of that data? If yes, describe. If no, explain reason.**							
P.9.1	Are there processes in place that enable individuals to access and update their personal information?							
P.9.2	Are there processes in place and communicated so that individuals can request and review their personal information maintained by the service provider?							
P.9.3	Are there processes in place to confirm the identity of individuals who request access prior to providing such personal information?							
P.9.4	Are there processes in place or mechanisms to allow individuals to update or correct personal information held by service provider?							
P.9.5	Are there measures in place to limit what personal information an individual has the ability to modify or correct?							
P.10	**Is personal information - provided by the client - shared with other third parties within the US only? If yes, describe.**							
P.11	**Is personal information - provided by the client - shared with other third parties outside of the US? If yes, list countries.**							

P. Privacy

65 Total Questions to be Answered **0% Percent Complete**

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text	GAPP No.	GAPP Text
P.12	**Are there appropriate contractual controls to ensure that personal information shared with other third parties is appropriately protected by the third party? If yes, describe. If no, explain reason.**							
P.12.1	Do contracts or agreements with other third parties include privacy provisions if required?							
P.12.2	Are there appropriate contractual controls to ensure that personal information shared with other third parties is limited to defined parameters for access, use and disclosure? If yes, describe. If no, explain reason.							
P.12.3	Is there a remediation plan to address other third-party misuse and/or breach of personal information? If yes, describe. If no, explain reason.							
P.13	**Are there documented controls and procedures to appropriately safeguard personal information about individuals? If yes, describe. If no, explain reason.**							
P.14	**Does the information security program address the protection of personal information separately from other information (such as proprietary business information)? If yes, describe. If no, explain reason.**							
P.15	**Does the information security function regularly communicate and collaborate with the privacy function (if the two functions are separate)? If yes, describe. If no, explain reason.**							
P.16	**Is there a process for ensuring the accuracy and currency of personal information at the direction of the client? If yes, describe. If no, explain reason.**							
P.16.1	Is there a process to inform an individual supplying his/her personal information that he/she is responsible for the accuracy of such information? If yes, describe. If no, explain reason.							
P.16.2	Is there a process to inform an individual that he/she is responsible for informing the organization of needed corrections to his/her personal information? If yes, describe. If no, explain reason.							
P.17	**Is there a process to ensure that the personal information provided by an individual is limited for the purposes described in the organization's privacy notice? If yes, describe. If no, explain reason.**							
P.18	**Are employees, contractors, volunteers (and other parties, as appropriate) regularly monitored for privacy compliance? If yes, describe. If no, explain reason.**							
P.19	**Are third-party service providers regularly monitored for privacy compliance? If yes, describe. If no, explain reason.**							
P.20	**Are appropriate sanctions applied to employees, contractors, volunteers (and other parties, as appropriate) who violate privacy policies? If yes, describe process. If no, explain reason.**							
P.21	**Is there a process for employees, contractors, volunteers (and other parties, as appropriate) to notify privacy compliance personnel of an actual or suspected privacy breach? If yes, describe. If no, explain reason.**							

Glossary

Term	Definition
Acceptable Use Policy	Part of the information security framework that defines what users are and are not allowed to do with the IT systems of the organization. It should contain a subset of the information security policy and refer users to the full security policy when relevant. It should also clearly define the sanctions applied if a user violates the policy.
Acknowledgement of Acceptable Use	A written attestation from a user of an information system indicating the user's acceptance and willingness to comply with the relevant information systems control policies.
Anti-Tailgating / Anti-Piggybacking Mechanism	Two sets of doors whereby access to the second is not granted until the individual has passed through (and closed) the first, often referred to as a "man trap." A controlled turnstile is also considered an anti-tailgating/piggybacking mechanism.
Asset Classification	The category or type assigned to an asset, which is derived from the asset classification policy. Asset classifications frequently vary from company to company.
Asset Control Tag	A unique identification number assigned to all inventoried assets.
Attribute	A property or field of a particular object.
Baseline	A benchmark by which subsequent items are measured.
Battery	An electrochemical cell (or enclosed and protected material) that can be charged electrically to provide a static potential for power or released electrical charge when needed.
Biometric Reader	A device that uses measurable biological characteristics such as fingerprints or iris patterns to assist in authenticating a person to an electronic system.
Business Continuity Plan (BCP)	A process that defines exactly how, for which applications, and for how long a business plans to continue functioning after a disruptive event. The business continuity plan is usually an overarching plan that includes both operational and technology-related tasks.
Business Impact Analysis (BIA)	This term is applicable across Technology Risk Management, in both information security and business continuity planning domains. An impact analysis results in the differentiation between critical and non-critical business functions. A function may be considered critical if there is an unacceptable impact to stakeholders from damage to the function. The perception of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.
Business Process	An end-to-end service made available to internal or external parties that usually corresponds to standard service products that the Service Provider offers to clients.
Change Initiation Request (CIR)	A document (physical or electronic) used to track change requests, including new features, enhancement requests, defects, and changed requirements. The change initiation request document must contain: - The name of the person initiating the change - The system affected by the change - A description of the change, including the file name(s) and file location(s) - The date the change will occur - An approval signature by someone other than the person initiating the change - An approval date
Climate Control System	A combination of sensors and equipment that monitors the temperature and humidity in a sensitive environment (such as a data center) and that automatically heats/cools/dehumidifies as needed to keep the atmosphere within acceptable tolerances.
Cold Site	A remote facility that provides the equipment necessary for data and process restoration.

Term	Definition
Communications Plan	A tool for communicating information on the considerations and implications of business continuity within the organization used to improve decision making.
Confidentiality	The protection of sensitive information from unauthorized disclosure and sensitive facilities due to physical, technical, or electronic penetration or exploitation.
Constituent	An active employee or contractor.
Contractor	A contracted professional with expertise in a particular domain or area.
Demilitarized Zone (DMZ)	A controlled network space, delimited by firewalls or other policy-enforcing devices, which is neither inside an organization's network nor directly part of the Internet. A DMZ is typically used to isolate an organization's most highly secured information assets while allowing predefined access to those assets that must provide or receive data outside of the organization. The access and services provided should be restricted to the absolute minimum required.
Disaster Recovery	The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity
Enclosed	Closed in, surrounded, or included within.
Exception	A result that deviates from the norm or expectation.
External Vulnerability Scan	A systematic review process executed from a network address outside of the Scoped Systems and Data network that uses software tools designed to search for and map systems for weaknesses in an application, computer or network. The intent is to determine if there are points of weakness in the security control system that can be exploited from outside the network.
Externally Facing	The network entry point that receives inbound traffic.
Extranet	An intranet that is partially accessible to authorized outsiders.
Facility	A structure or building, or multiple structures or buildings, in which operations are conducted for the services provided. These operations include handling, processing and storage of information, data or systems, as well as personnel that support the operations.
Fire Suppression System	A combination of sensors and equipment designed to detect the presence of heat/smoke/fire and actuate a fire retardant or fire extinguishing system.
Firewall	A set of related programs, located at a network gateway server, that protects the resources of private networks from other networks. Firewalls may be application/proxy, packet-filtering, or stateful-based. Examples of firewalls are Cisco PIX, Check Point Firewall, Juniper NetScreen and Cyberguard. (Though they contain some firewall functionality, routers are not included in this definition.)
Firewall Rule	Information added to the firewall configuration to define the organization's security policy through conditional statements that tell the firewall how to react in a particular situation.
Fluid Sensor	A mechanical device that is sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.
Gateway	A node on a network that facilitates the communication of information between two or more nodes.
General Perimeter	An area with fully enclosed walls that extend from floor to ceiling (beyond raised floors and ceilings) surrounding the secure perimeter. This may be the same floor as the secure perimeter, if shared by other tenants in the facility, or the facility itself.
Generator	A device that converts mechanical energy to electrical energy via an engine (usually fuel-powered) that provides electrical current as input to a power source.

Term	Definition
Hardware Systems	Includes servers and network devices.
Heat Detector	A mechanical device that is sensitive to temperature and transmits a signal to a measuring or control instrument.
Hot Site	A duplicate of an organization's original site, with full computer systems and near-complete backups of user data.
Immediate Perimeter	A rack or cage that houses the Scoped Systems and Data.
Incident	Events outside normal operations that disrupt normal operational processes. An incident can be a relatively minor event, such as running out of disk space on a server, or a major disruption, such as a breach of database security and the loss of private and confidential customer information.
Incident Severity	A ranking of an event's significance that uses, at a minimum, a three-point scale: minor, moderately severe, and severe. For each level of severity, IT organizations should define acceptable resolution times, escalation procedures, and reporting procedures.
Intermediate Distribution Frame IDF	A free-standing or wall-mounted rack for managing and interconnecting the telecommunications cable between end user devices and a main distribution frame (MDF).
Internal Vulnerability Scan	A systematic review process using software tools designed to search for and map systems for weaknesses in an application, computer or network, executed from a network address within the Scoped Systems and Data network. Internal vulnerability scans are used to determine whether points of weakness in the security control system exist that could be exploited by a user with access to the internal network.
Internet	A global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions.
Internet Protocol (IP)	A networking standard that allows messages to be sent back and forth over the Internet or other IP networks.
Intranet	An IP network that resides behind a firewall and is accessible only to people who are members of the same organization.
Intrusion Detection Systems (IDS)	A security inspection system for computers and networks that can allow for the inspection of systems activity and inbound/outbound network activity. The IDS key function identifies suspicious activity or patterns that may indicate a network or system attack.
Intrusion Protection System (IPS)	A more sophisticated Intrusion Detection System (IDS) that allows administrators to configure predefined actions to be taken if suspicious activity is detected.
Inventory	An itemized list of current assets.
Local Backup	A method for backing up data on the local system. For example, an attached tape or storage device.
Main Distribution Frame	A wiring rack that connects outside lines with internal lines. Main distribution frames are used to connect public or private lines entering the building to the organization's internal networks
Map of Dependencies	A diagram that illustrates how a business process relates to its supporting capabilities. ("Supporting capabilities" include: people involved in the delivery of the business process, application software, middleware software, servers, storage, networking, physical facilities, and people involved in the IT and physical infrastructure management.)

Term	Definition
Master Change Log	A document or database that contains a report of each change initiation request (CIR) (approved or rejected). The document or database must contain: - Reference to a CIR - Date submitted - Date of change - Name of affected system - Approval status (approved or rejected)
MD5	A one-way cryptographic hash algorithm that produces a unique 128-bit alphanumeric fingerprint of its input.
Mobile Code	Software code that is transferred from one computer to another and that executes automatically. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded in Microsoft Office documents.
Modem	A device that allows a computer or terminal to transmit data over an analog telephone line.
Network Address Translation (NAT)	A process of rewriting the source and/or destination addresses of IP packets as they pass through a network device.
Network Devices	Units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU).
Network Segment	A portion of a computer network that is separated from the remainder of the network by a device such as a repeater, hub, bridge, switch or router. Each segment may contain one or multiple computers or other hosts. Network segments are typically established for throughput and/or security reasons.
Network time protocol (NTP)	A protocol designed to synchronize the clocks of computers over a network.
Node	Any physical device with a unique network address.
Non-Employees	Auditors, consultants, contractors, and vendors.
Owner	An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Ownership is not an indication of property rights to the asset.
Ownership	A formally assigned responsibility for a given asset.
Personal Identification Number (PIN)	A secret shared between a user and a system that can be used to authenticate the user to the system.
Physical Media	Any portable device or substance (e.g., paper) used to store data for specific and legitimate purposes. Examples of physical media include: - Magnetic tapes and disks - Cartridges, including 9-track, DAT, and VHS - Optical disks in CD and DVD format - Microfilm/fiche - Paper (e.g., computer-generated reports and other printouts) - Static memory devices, such as USB memory sticks
Port Scan	A systematic scan of a computer's ports that identifies open doors. Used in managing networks, port scanning also can be used maliciously to find a weakened access point from which to break into computer.

Term	Definition
Post-Deployment Test Document	A document that provides evidence that the change was tested and approved in the production environment. The document must contain: - Reference to a CIR - Identified deployment resources - Deployment start date - Deployment end date - Expected results - Actual results - Approval signature - Approval date
Power Redundancy	Any type of power delivery mechanism that provides continuous power to connected systems in the event of a failure in the main delivery mechanism for electricity. Such mechanisms include multiple electric feeds, automatic failover generators, and uninterruptible power supplies.
Pre-Deployment Test Document	A document (electronic or paper) that provides evidence that the requested changes were tested prior to deployment in the production environment. A pre-deployment test document is inspected for: - Reference to a CIR - Identified testing resources - Testing start date - Testing end date - Expected test results - Actual test results
Protocol	A set of rules and formats that enable the proper exchange of information between different systems.
Publicly Accessible	In networking terms, able to accept a connection originating from the public domain, e.g., the Internet.
Raised Floor	Used in data center construction, a raised floor above the "true" floor allows air conditioning flow and wiring to pass freely under equipment. The space between the true and raised floors is accessed by removable floor tiles.
Receiver Company	The organization that has contracted with a service provider for a specific service.
Residual Risk Rating Scoring Method	A calculation of the risk that remains after security controls have been applied.
Risk Prioritization Scoring Method	A systematic approach that quantifies risk in terms of loss potential, then sequences individual risks to determine the order in which compensating controls should be implemented.
Scoped Systems and Data	Computer hardware, software and/or Non-Public Personal Information that is stored, transmitted, or processed by the service provider in scope for the engagement.
Scoping Meeting	A meeting held prior to commencement of a Shared Assessments engagement, to determine the Scoped Systems and Data to be included in a company's Standardized Information Gathering Questionnaire (SIG) and Agreed Upon Procedures (AUP) assessment.
Secure Perimeter	A space fully enclosed by walls that surround the immediate perimeter and that extend from floor to ceiling (beyond raised floors and ceilings), which is contained, and whose points of entry are secured.
Secure Socket Layer (SSL)	A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system with two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message.
Secure Workspace	An environment from where people work from their desks with the purpose of accessing, editing or inputting Scoped Systems and Data on a computer, telephone or physical media, e.g., a BPO or call center environment.

Term	Definition
Secure Workspace Perimeter	A space fully enclosed by walls that surround the Secure Workspace which is contained, and whose points of entry and exit are secured.
Security Policy	A published document or set of documents defining requirements for one or more aspects of information security.
Server	A computer that makes services, such as access to data files, programs, and peripheral devices, available to workstations on a network.
Service Provider	An organization that provides outsourced services, such as data processing, business operations, applications, systems or staffing.
Service Set Identifier (SSID)	A 32-character unique identifier attached to the header of packets sent over a wide area network to identify each packet as part of that network.
Simple Mail Transfer Protocol (SMTP)	The de facto standard for email transmissions across the Internet.
Smoke Detector	A mechanical device that is sensitive to the presence of smoke or particulate material in the air that transmits a signal to a measuring or control instrument.
Status Change	Change to employment status that is recorded by human resources, such as promotions, demotions or departmental changes.
Stewardship	The act of managing and maintaining a given asset.
Strong Password	Password length must be a minimum of seven (7) characters, must not to contain a common usage word or a word found in the English dictionary, may not contain user name, any part of a full name or access level of the user and must contain characters from at least three (3) of the following four (4) classes of characters: • Upper case letters (A, B, C, ….Z) • Lower case letters (a, b, c, ….z) • Numbers (0,1, 2, …9) • Non-alphanumeric ("special characters") such as punctuation symbols
System Owner	The business unit that retains financial ownership or decision rights for the business use of the asset.
System Steward	The primary assigned administrator responsible for maintenance and day-to-day tasks that support the business.
Third Party	All entities or persons that work on behalf of the organization but are not its employees, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates and any other person or entity that accesses Scoped Systems and Data.
Threat Impact Calculation Method	A systematic method of determining the loss potential of a particular threat, based on the value of assets affected.
Threat Probability Calculation Method	A systematic method of determining the potential for a particular threat to occur, based on the likelihood of the occurrence collected from internal staff, past records, and official security records. Threats x Vulnerability x Asset Value = Total Risk (Threats x Vulnerability x Asset Value) x Controls Gap = Residual Risk
Token	A unique identifier generated on both a host and small, user-held device that allows the user to authenticate to the host.
True Ceiling	The permanent overhead interior surface of a room, constructed of solid building materials offering resistance to and evidence of unauthorized entry.
True Floor	The permanent bottom interior surface of a room, constructed of solid building materials offering resistance to and evidence of unauthorized entry.

Term	Definition
Unapproved	Operating without consent.
Unidentified	Being or having an unknown or unnamed source.
Uninterruptible Power Supply (UPS)	A power supply consisting of a bank of batteries, which is continually charged. When power fails, the UPS becomes the source of electrical current for computer equipment until the batteries are discharged. A UPS is often connected to a generator that can provide electrical power indefinitely.
Vibration Alarm Sensor	An alarm that responds to vibrations in the surface onto which it is mounted. A normally closed switch momentarily opens when the sensor is subjected to a vibration of sufficiently large amplitude.
Virtual Private Network (VPN)	A communication tunnel running through a shared network, such as the Internet, which uses encryption and other security mechanisms to ensure the data cannot be intercepted and that the data senders and receivers are authenticated.
Volumetric Alarm Sensor	An alarm sensor designed and employed to detect an unauthorized person in a confined space when the space is normally unoccupied. Such alarms include ultrasonic, microwave, and infrared sensors.
War Walk	Also known as "war drive," using a laptop to "sniff" for wireless access points. War walking may be used to locate a public access point for personal use or as a controls assessment to identify access points that are inadequately secured and may indicate an elevated risk of breach.
Warm Site	A remote facility which replicates production data in set intervals.
Water Sensor	A mechanical device sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.
Workstation	(1) Single-user computers typically linked together to form a local area network, that can also be used as standalone systems. (2) In networking, any computer connected to a local area network, including a workstation or personal computer.