

**Internal Audit
Request for Information**

X-Ref to Survey Questions	Item Description	Documentation is:
1.1.1	Risk Assessment & Information Security Policy	
2.1.1	Organizational Chart	
3.1.1	Hardware Inventory List	
3.1.2	Software Inventory List	
3.2.2	Information Asset Classification and Data Protection Policy	
3.2.7	Procedure / Software used to sanitize media	
4.1.2	Information Technology (IT) job descriptions	
4.2.1	IT Training Plan / Materials	
5.x.x	Physical & Environmental Security documentation	
6.1.1	Patch Management policy / strategy / procedures for O/S, Applications, Antivirus, etc.	
6.4.1	Backup Procedures	
6.4.2	- Offsite Rotation Log	
6.4.3	- Backup Logs	
6.5.2	Network diagram	
6.5.3	Product used to perform vulnerability scans	
7.1.1	Logical Access Policies and Procedures	
7.1.x	System User List	
7.3.x	Password Parameters	
9.1.x	Business Continuity Plan	
10.1.1	College/Department Record Retention Requirements	
10.2.3	Results of Recent Software License Review	

Please proceed to the Survey Tab.

Email Address:
iawebsurvey@ia.ohio-state.edu

Mailing Address:
Department of Internal Audit
Attn: IS Audit
2080 Blankenship Hall
901 Woody Hayes Drive
Columbus, Ohio 43210

**Information Security Review
OSU Department of Internal Audit
FY06**

Please read instructions and contact information on the "Instructions" Sheet.
Please return completed survey to Internal Audit (iawebsurvey@ia.ohio-state.edu).
Press Tab to move from field to field.

0.0.0	General Information	Cell display limited to 50 characters.	Comments (Optional)
0.0.1	College / VP Area org. number (5 digits)		
0.0.2	Department org. number (5 digits)		
0.0.3	Your name		
0.0.4	Title		
0.0.5	Email address		
0.0.6	Phone number		
0.0.7	Total number of users		
0.0.8	Total IT staff		
0.0.9	Total department budget		
0.0.10	Total IT budget		
0.0.11	List Operating systems supported / managed by your department. (e.g. Windows 2000 server, Linux, HPUX, etc.)		
0.0.12	List important applications supported / managed by your department. (e.g. email, databases, financial applications, etc.)		
0.0.13	List IP Range / Domain Name used by your department.		
0.0.14	Is your IT function critical to your daily operation?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
0.0.15	Is your IT function critical to other departments' daily operation?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
0.0.16	Does your IT department have responsibility for managing all IT assets within the department, e.g., servers, clients, printers, research project computer assets?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
0.0.17	Does your department store / process any FERPA related data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
0.0.18	Does your department store / process any HIPAA related data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
0.0.19	Does your department store / process any GLBA related data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
0.0.20	Does your department store / process any credit card data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	

1.0.0	Security Governance		
1.1.0	Security Policy - An Information Security Policy sets your organization's requirements, direction and management support for information security.		
1.1.1	Does your department have a documented and senior management approved information security policy?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
1.1.2	Is senior management involved in information security governance strategy (e.g. policy development, risk management, monitoring)?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
1.1.3	Has the Office of the CIO's Security Group reviewed the organization's information security governance strategy?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	

2.0.0	Security Organization		
2.1.0	Security Infrastructure - An Information Security Infrastructure is a crucial element of an overall security plan, which if effectively deployed, ensures that Information Security is implemented and managed within your company.		
2.1.1	Does your department have a documented information security infrastructure (e.g. org. chart, job descriptions)?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.1.2	Does a director (or equivalent) have responsibility for information security?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.1.3	Is expertise on Information Security available internally, and where not, is external advice sought when required?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	

2.2.0	Third Party Access		
2.2.0	Third Party Access - The security of your department's information, if accessed by third parties, must be ensured.		
2.2.1	Does a third party's (e.g. joint venture, guest) access to information require approval by an appropriate senior manager or data owner?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.2.2	If access is allowed, are the associated risks assessed and the appropriate security measures put in place?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.2.3	Do third party contracts address information security matters, such as liabilities, data protection, privacy, intellectual property and copyright?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.2.4	Are security requirements, including responsibilities, addressed in the written contract between your organization and the third party?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	

2.3.0	Outsourcing		
2.3.0	Outsourcing - The security of information needs to be maintained when the responsibility for information processing has been outsourced to another organization, e.g. use of a Credit Card Processor.		
2.3.1	Does an outsourcing party's (e.g. contractors, vendors) access to information require approval by an appropriate senior manager or data owner?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.3.2	If access is allowed, are the associated risks assessed and the appropriate security measures put in place?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.3.3	Do outsourcing contracts address information security matters, such as liabilities, data protection, privacy, intellectual property and copyright?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
2.3.4	Are security requirements, including responsibilities, addressed in the written contract between your organization and the outsourcing party?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	

3.0.0	Asset Classification & Control		
3.1.0	Accountability - The maintenance of assets can be greatly enhanced through the use of an inventory control system.		
3.1.1	Does your department maintain a documented inventory of software assets?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.1.2	Does your department maintain a documented inventory of hardware assets?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	

3.2.0	Information Classification		
3.2.0	Information Classification - Information assets have varying degrees of sensitivity and criticality. By classifying information assets, the appropriate level of protection can be specified.		
3.2.1	Does your department classify information assets based on risk, sensitivity, and compliance?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.2.2	Does your department have a documented Information Asset Classification and Data Protection policy?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.2.3	Does your department tell staff how they should handle information assets with regard to its storage, transportation, and destruction?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.2.4	Is sensitive data encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.2.5	Are staff required to lock away or secure sensitive documents when not in use?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.2.6	Are sensitive paper documents properly disposed (e.g. shredded)?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	
3.2.7	Are computer storage media properly cleaned or sanitized prior to transfer or disposal in accordance with minimum requirements defined in DOD 5220.22-M?	<input type="checkbox"/> Yes <input type="checkbox"/> Partially <input type="checkbox"/> No <input type="checkbox"/> N/A	

4.0.0	Personnel Security				
4.1.0	Staffing - Security responsibilities should be addressed in the recruitment process and should be monitored during employment.				
4.1.1	Are formal background investigations performed for sensitive positions?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.1.2	Are staff made aware of their security responsibilities (e.g. via job descriptions, Info. Sec. policy)?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.1.3	Are job applicants' claims of previous experience, qualifications and identity, and character references verified?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.1.4	Are employees and contract staff required to sign confidentiality or non-disclosure agreements?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.1.5	Are employees who violate the security policy subject to a disciplinary process?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

4.2.0	User Training - User training is crucial to ensuring that staff are adequately equipped to support the security policy in the course of their normal work.				
4.2.1	Is a formal, documented information security training plan in place?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.2.2	Do all staff receive basic information security training at induction (e.g. system use, confidentiality, malicious software, use of passwords)?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.2.3	Is information security training provided periodically (e.g. monthly, yearly)?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4.2.4	Do staff with specific responsibilities (e.g. IT Manager) receive additional training?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

5.0.0	Physical & Environmental Security				
5.1.0	Secure Area - It is important that measures are taken to prevent unauthorized access, damage and interference to business premises and information processing facilities.				
5.1.1	Does your organization take steps to prevent unauthorized access to your premises?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.1.2	Are secure areas (e.g. computer rooms), or office areas where sensitive information is stored, protected by access controls?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.1.3	Are unmanned external doors and accessible windows protected through additional controls?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

5.2.0	Equipment Security - Equipment should be protected against security threats and environmental hazards.				
5.2.1	Does your department take steps to prevent loss, damage or compromise of equipment and interruption to business activities?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.2.2	Is important equipment, e.g. servers, located in secure areas?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.2.3	Is equipment protected from power failure, e.g. use of a UPS?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.2.4	Is guidance provided with regard to the use of company material off site (e.g. use of a laptop)?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

5.3.0	Housekeeping - General controls are required to prevent compromise or theft of information.				
5.3.1	Does your organization implement general measures to protect the department's information?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.3.2	Are paper and computer media locked away when not in use?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5.3.3	Is automatic computer screen locking functionality enabled that lock the screen when a computer is left unattended for a period of time?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

6.0.0	Communication & Operations Mgmt				
6.1.0	Change Management - Describes methods, approaches, and policies which organizations can use to make systems changes in a controlled way and to assure that configuration are standardized, documented, and maintained.				
6.1.1	Does your department have documented change management policy / procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.1.2	Are all changes to systems justified, approved, and managed? (e.g. installing a new piece of software.)	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.1.3	Are patches tested on non-production systems before they are implemented?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.1.4	Are high priority security patches implemented within 24 hours of identification / notification?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

6.2.0	System Planning & Monitoring - The risk of system failures should be minimized by system planning and monitoring.				
6.2.1	Is capacity on systems monitored, and future capacity projected?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.2.2	Are logs used for system monitoring?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

6.3.0	Anti-Virus - Are precautions taken against the introduction of malicious software such as viruses and worms?				
6.3.1	Does your department have a documented anti virus policy?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.3.2	Is anti-virus software operating on all servers, PCs and mobile computers?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.3.3	Are anti-virus updates applied within 24 hours of release?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

6.4.0	Backup - The integrity and availability of information and communication systems is enhanced through the deployment of techniques such as information back-up.				
6.4.1	Are backup and recovery procedures documented and in place?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.4.2	Is backup data stored off-site in a secure University or approved vendor facility?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.4.3	Are logs maintained as to who has made the backup and when?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.4.4	During transport, is backup media properly secured?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

6.5.0	Network Management - The information in networks must be safeguarded, and supporting infrastructure protected.				
6.5.1	Are network controls, where required, used to conceal the meaning of text (e.g. encryption / SSL)?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6.5.2	Have controls been implemented to protect systems connected to the internet (e.g. firewalls)?	<input type="checkbox"/> Yes	<input type="checkbox"/> Partially	<input type="checkbox"/> No	<input type="checkbox"/> N/A

