



Risk Management Survey

The following survey measures the risk to your administrative controls within your unit, department or organization.

Please answer all questions to the best of your ability.

Administrative Control Survey			
Practice	Is this practice used by your organization?		
Security Awareness and Training			
You and/or your staff understand their security roles and responsibilities. This is documented and verified.	Yes	No	Don't know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Yes	No	Don't know
Security awareness, training, and periodic reminders are provided for all personnel. You and or your staff understanding is documented and conformance is periodically verified.	Yes	No	Don't know
Security Strategy			
Business strategies routinely incorporate security considerations.	Yes	No	Don't know
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes	No	Don't know
Security strategies, goals, and objectives are documented and are routinely			

reviewed, updated, and communicated to the organization.	Yes	No	Don't know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No	Don't know
Security roles and responsibilities are defined for all staff in the organization.	Yes	No	Don't know
The organization's hiring and termination practices for staff take information security issues into account.	Yes	No	Don't know
The organization manages information security risks, including <ul style="list-style-type: none"> • assessing risks to information security • taking steps to mitigate information security risks 	Yes	No	Don't know
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	Yes	No	Don't know
Security Policies and Regulations			
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes	No	Don't know
There is a documented process for management of security policies, including <ul style="list-style-type: none"> • creation • administration (including periodic reviews and updates) • communication 	Yes	No	Don't know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes	No	Don't know
The organization uniformly enforces its security policies.	Yes	No	Don't know
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including <ul style="list-style-type: none"> • protecting information belonging to other organizations • understanding the security policies and procedures of external 	Yes	No	Don't know

<p>organizations</p> <ul style="list-style-type: none"> ending access to information by terminated external personnel 			
The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.	Yes	No	Don't know
Contingency Planning/Disaster Recovery			
An analysis of operations, applications, and data criticality has been performed.	Yes	No	Don't know
<p>The organization has documented, reviewed, and tested</p> <ul style="list-style-type: none"> business continuity or emergency operation plans disaster recovery plan(s) contingency plan(s) for responding to emergencies 	Yes	No	Don't know
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Yes	No	Don't know
<p>All staff are</p> <ul style="list-style-type: none"> aware of the contingency, disaster recovery, and business continuity plans understand and are able to carry out their responsibilities 	Yes	No	Don't know
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes	No	Don't know
There are documented policies and procedures for managing visitors.	Yes	No	Don't know
There are documented policies and procedures for physical control of hardware and software.	Yes	No	Don't know
Authentication and Authorization			
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	No	Don't know
Incident Management			
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes	No	Don't know

Incident management procedures are periodically tested, verified, and updated.	Yes	No	Don't know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No	Don't know
General Staff Practices			
<p>Staff members follow good security practice, such as</p> <ul style="list-style-type: none"> • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents 	Yes	No	Don't know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	No	Don't know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	No	Don't know
Information Management			
Staff understand their roles or responsibility in maintaining the privacy of records and information in their department	Yes	No	Don't know
Staff have received training in privacy of records and this training is documented, periodically updated and verified.	Yes	No	Don't know
The Local and University Custodian of Records is known to all staff in office	Yes	No	Don't know
Procedures for inspection and amendment of the records exist and staff is knowledgeable in policy and procedures for inspection.	Yes	No	Don't know
Information regarding the records is available in an alternative language or communication method to requestor.	Yes	No	Don't know

Staff knows where to locate information on record management, including policy and procedure?	Yes	No	Don't know
All staff know the requirements on retention and destruction of records.	Yes	No	Don't know
