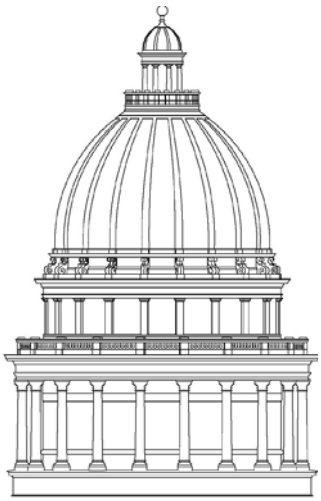
REPORT TO THE

UTAH LEGISLATURE

Number 2011-10



A Performance Audit of IT Security at Universities and Quasi-Government Agencies

September 2011

Office of the
LEGISLATIVE AUDITOR GENERAL
State of Utah

STATE OF UTAH
Office of the Legislative Auditor General

315 HOUSE BUILDING • PO BOX 145315 • SALT LAKE CITY, UT 84114-5315
(801) 538-1033 • FAX (801) 538-1063

JOHN M. SCHAFF, CIA
AUDITOR GENERAL

September 13, 2011

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report, **A Performance Audit of IT Security at Universities and Quasi-Government Agencies** (Report #2011-10). A digest is found on the blue pages located at the front of the report. The objectives and scope of the audit are explained in the Introduction.

We will be happy to meet with appropriate legislative committees, individual legislators, and other state officials to discuss any item contained in the report in order to facilitate the implementation of the recommendations.

Sincerely,

John M. Schaff

John M. Schaff, CIA
Auditor General

JMS/lm

Digest of A Performance Audit of IT Security at Universities and Quasi-Government Agencies

Chapter I: Introduction

Organizations must balance IT security management needs within their organizational structures. Quasi-government agencies and higher education institutions generate and store different amounts and types of sensitive information that need protection. Because of the balancing within their structures, the ability to protect informational assets is different for each entity's staff and financial resources availability. IT security programs need to align security requirements with staff abilities, financial resources, and other business operations.

To protect agencies, discussions about specific organizations' programs and abilities were not included in this report. Disclosure of IT security details could potentially assist an attacker in penetrating an organization's system. Organizations are rightfully protective of any IT security information they disclosed, and we have taken precautions to not disclose the sensitive details of entities' systems. Therefore, this report addresses general IT security structures that any organization may find helpful rather than identifying elements that may be lacking in specific organizations.

Chapter II: Higher Education Proactively Monitors IT Security

Higher Education Assessments Seem Comprehensive. The higher education system is undergoing its third round of IT security assessments. The assessments are performed by technical specialists from the Utah Education Network and various higher education institutions. The assessments are well documented and appear to be comprehensive. The following characteristics were observed from prior reports and on-site observation of the assessment process:

- Tasks tested key components of IT security programs
- Methodologies were consistent among institutions
- Team members used a variety of techniques to assess configurations

The assessment team appeared to follow best practices regarding the scope and various tests that were selected. Institutions now cover a portion of the costs of these assessments and have more input on

their scope. This round of assessments has greater institutional buy-in and appears to be more collaborative than prior assessments done under the direction of State Board of Regents' staff.

Most Institutions Are Implementing Recommendations. Follow-up assessments show that most institutions have addressed prior findings. However, two institutions have not implemented recommendations about specific findings in prior assessments. Implementation problems appear to be related to the absence of a full-time Information Security Officer or ISO (responsible for implementing IT security solutions) because both institutions were lacking full-time ISOs. A third institution showed positive results after they hired ISO, and their assessment this year validated the results. Therefore, institutions without a full-time ISO need to make this position a priority.

Chapter III: Key IT Security Features Needed at Quasi-Government Agencies

Agencies Should Adopt Basic IT Security Features and Consider Testing Their IT Solutions. While quasi-government agencies have implemented some IT security measures, additional steps can be taken to document and strengthen agency practices. The following shortfalls were identified in some of the reviewed agencies:

- Some small agencies were lacking policies or existing policies were incomplete.
- Most agencies did not provide employees with appropriate training on IT security issues.
- Some small agency IT continuity plans seemed inadequate because they did not:
    - Adopt incident handling procedures for different scenarios
    - Consider non-data assets in continuity plans
    - Ensure continued access to systems administered by vendors.
- Technical solutions on critical systems were not tested to ensure proper configuration.

Half of the reviewed agencies outsourced their IT services, so there was no internal IT staff to recommend these security controls to management. This audit report is intended to raise awareness of these issues. In addition, one Utah association said it will work to train its members on the necessity of IT security controls.

REPORT TO THE

UTAH LEGISLATURE

Report No. 2011-10

A Performance Audit of IT Security at Universities and Quasi-Government Agencies

September 2011

Audit Performed By:

Audit Manager	Tim Osterstock
Audit Supervisor	Tim Bereece
Audit Staff	David Gibson

Table of Contents

Chapter I
Introduction

Government entities process and store large data sets that must be safeguarded against unintended access and use. Entities must decide how to best manage the risk associated with information technology (IT) assets. This report examines how well some Utah entities safeguard this information from possible inappropriate access and identifies best practices used to secure IT systems. The audit reviewed highly sensitive plans and information pertaining to agencies' security measures that will not be disclosed or discussed in this report. With this restriction, we reviewed quasi-government agencies and higher education institutions IT security programs. We focused on management's capabilities to develop and implement core IT security program elements rather than discussing the configuration of technical controls.

This report provides an overview of IT security practices rather than disclosing specific agency practices.

An audit of higher education institutions in Arizona found multiple types of vulnerabilities in their IT security systems. The audit team provided summary of findings to the Arizona Legislature. Concerns whether similar problems exist in Utah's higher education system prompted this audit request. The scope was expanded to include quasi-government agencies that are not under the purview of the Department of Technology Services.

IT Security Management Must Be Balanced with Other Needs

Quasi-government agencies and higher education institutions provide a variety of public services. Many of these services generate or obtain sensitive information that must be protected. The ability to protect information is different for each entity. Security programs' budgets often result from a compromise between the desired security level and the entities' operational needs and financial abilities.

Well-established IT security programs should have a program manager within the organization who oversees IT security issues. Program managers need to ensure that adequate personnel, funds, and technical support are available to fulfill policy objectives. Compliance measures should also be implemented to ensure that policies are

IT security programs should specify who oversees security activities and what resources and plans are necessary.

followed. These components, as well as others, are the resources that make up an IT security program.

Entities Must Protect Various Information Assets

Since higher education institutions collect several types of sensitive information, they have a corresponding responsibility to protect each different type of information. Quasi-government agencies typically manage simpler sets of information; however, resource constraints can pose the problem of providing adequate protection.

Higher education institutions provide numerous data-generating services that must be adequately protected. Some of the IT assets protected by institutions are:

- Student records
- Financial transactions
- Patient medical history

Adequate protection levels for these assets are ultimately decided by each institution, depending on the level of risk that can be tolerated. However, specific requirements are placed on them by federal law or industry standards, such as the following:

The scope of informational assets protected by higher education institutions is much greater than that of most quasi-government agencies.

- Family Educational Rights and Privacy Act (FERPA)
- Payment Card Industry (PCI) data security standards
- Health Insurance Portability and Accountability Act (HIPAA)

Thus, the scope of IT security at higher education institutions can be broad. Combining the broad scope with the size of some institutions makes the task of providing IT security challenging.

Quasi-Government Agencies' IT Security Needs Differ from Those of Higher Education Institutions. Quasi-government agencies typically have a much simpler list of data resources to protect than higher education institutions. The most common quasi-government agencies we looked at were special service districts. Such districts provide a diverse set of services to the public, including basic utilities, health care treatment, and fire protection. Each of these services may have special information assets that must be protected, such as supervisory control and data acquisition (SCADA) devices that

monitor drinking wells or payment systems that allow customers to make online payments. While these agencies can be relatively small, they still have IT assets that need to be secured. Despite their differences, a major challenge for both higher education institutions and quasi-government agencies is prioritizing their IT security efforts within their resource constraints.

Agency Resources Dictate Approaches to Security

Information assets are never totally secure, so the risk to IT assets must be managed to appropriate levels. Agency management must balance competing interests when implementing a security plan. IT investment and expenditures represent a relatively small portion of agency expenditures. As a result, agencies take various approaches to protecting assets, including:

- Contracting for IT services
- Not accepting credit or debit cards
- Partnering with larger organizations

One of the fundamental assumptions of IT security is that risk is always present. Possible disruptions to an IT system can come from multiple sources such as employee fraud, hardware failure, facility destruction, malicious hackers, and others. Since risks can never be fully eliminated, management's job is to manage risks to an acceptable level. One of the challenges in mitigating risk is that only a finite amount of resources are available to implement security solutions.

Since agency IT resources are limited, agencies should consider the return on investment for security measures.

Managers of IT security systems must evaluate whether the IT security controls they implement are cost effective by balancing security demands, control costs, and procedures. Part of this process includes evaluating the return on investment for security systems. For example, spending a dollar to protect an informational asset worth a dollar would not provide a return on investment. Therefore, management must be careful not implement elaborate controls that outweigh the value of the asset being protected.

According to higher education reports and discussions with quasi-government agency staff, agencies spend up to approximately ten percent of their operating budget on IT needs. Since some agencies have relatively small operations, which can result in significant

limitations for IT security. For example, one quasi-government agency spent $65,000 in fiscal year 2010 on IT services, including their contractor and equipment. This agency's total IT budget would only cover a portion of the costs for a single security professional at other organizations. Another reviewed agency is under greater financial constraints, illustrating that some small agencies must be resourceful when deciding on security solutions.

During our review, we found one agency that made the conscious decision to not accept debit and credit card payments. Agency staff said they did not want to incur the risks associated with processing this information. The agency felt the best decision was not to take custody of nonessential information and incur the security costs. In these circumstances, cost avoidance appears to be a prudent risk management decision that others could consider.

Specific Conditions Were Omitted to Protect Agencies

Given the critical nature of and need to protect IT security plans, some information and conditions at universities and quasi-government agencies will not be discussed in this report. Instead, this report focuses on presenting some best practices that entities can rely on to protect their information assets and processing resources.

The entities we worked with during this audit were rightfully protective of the security information they shared with us during the audit. Disclosure of security control details in this report could enable a potential attacker to more easily breach an entities IT security. Therefore, we have not disclosed the sensitive details of entities' systems. Where needed, we discussed issues with agency management as items were identified. Higher education institutions have been participating in system-wide assessments of their IT security systems. However, some institutions can do a better job of implementing prior recommendations. Overall, quasi-government agencies have implemented some elements of an IT security program but some agencies are missing key planning and training elements.

IT Security Controls Are The Focus of This Report

In 1995, the National Institute for Standards and Technology (NIST) published an introductory handbook on computer security. In the handbook, they discuss three groups of security controls: managerial, operational, and technical. Management controls include policies and risk assessments that outline an organization's plan to address security risks. Operational controls include employee-driven activities such as awareness training, business continuity plans, and physical security. Technical controls include encryption, firewall configurations, and identification and authentication settings that computer systems execute.

Recommendations in this report are based on best practices published by NIST.

The focus of our report is on the management and operational controls that we felt should be addressed and warranted discussion in this report. Specific negative conditions at a particular entity will not be discussed to protect the agency from becoming a potential target. Discussion of technical controls has also been omitted because each entity's system is unique, and disclosure of the particular technical solution being utilized by an agency increases that entity's vulnerability to an attack on its IT system.

Audit Scope and Objectives

Audits in other states, particularly Arizona, have found serious weaknesses in IT security programs in government agencies and educational institutions. We were asked to test the vulnerability of the IT security controls in place at quasi-government agencies and universities. The scale of security efforts at quasi-government agencies and universities required different approaches to evaluating each group.

In Chapter II, we discuss the IT security assessments taking place at higher education institutions. A higher education assessment team had already performed two assessments of each institution's security program and was conducting their third assessment during our audit. As a result, we focused on evaluating the adequacy of these assessments and the institutions' implementation of assessment recommendations.

Our audit focused on higher education's assessment process and quasi-government institutions' security programs.

In Chapter III, we discuss IT security at quasi-government agencies. We performed a documentation review of management and operational controls. Our objective was to determine whether each agency had adequate policies and other security features in place that showed that management has been implementing an adequate security system.

Chapter II
Higher Education Proactively Monitors IT Security

Beginning in 2007, higher education took the initiative to evaluate its institutions' IT security systems. A series of assessments has provided a comprehensive review that covers several elements, and the methodology the assessment team uses appears to be consistent across institutions and with other assessments. Most institutions have implemented the recommendations from these assessments. However, we believe that all institutions should further ensure their IT security progress with an assigned Information Security Officer empowered to drive improvements in each institution's IT security.

Institutions' IT security systems have undergone three assessments since 2007. A team consisting of higher education IT security professionals from the Utah Education Network (UEN), Utah State University, Weber State University, and Salt Lake Community College performed these assessments. Since higher education has employees who possess the technical expertise to perform the necessary tests, the assessments were completed at a reasonable cost to the Utah State Board of Regents and the individual institutions.

Higher education's IT security experts have conducted three rounds of IT security assessments.

Higher Education Assessments Are Comprehensive

The periodic assessments performed by the higher education IT security team consistently covered a number of security elements. The team's methodology is based on various nationally recognized techniques. Our observations and review found that the current practices by higher education are a key component to ensure institutions identify potential vulnerabilities in their systems.

The security team's review is quite involved. Before the assessment team arrives at a school, they perform scans of the school's systems to help determine potential areas that may need further investigation. Once on the school's campus, each team member tests the specific system vulnerabilities they were assigned. The team is on-site for four to five days, attempting to penetrate various systems, evaluating

The assessment team provides reports that outline concerns and provide supporting data to identify systems weaknesses.

physical security, and meeting with campus staff regarding system configurations. On the last day, the team provides a brief overview of their findings, meeting with key IT personnel, including the Chief Information Officer, Information Security Officer, and other technical staff. Within the next month, the team produces a detailed final report that includes information specific to each institution's security needs and issues.

Assessments Improve With Each New Round

The higher education assessments covered several core elements of the reviewed institution's IT security programs. Assessments were consistently performed at each institution reviewed. Over time, the assessments have been refocused and now do a better job of focusing on the issues that present the greatest risk to institutions. The scope of these assessments appears to be increasing the effectiveness as institutions cover a larger portion of the costs and have more input on scoping decisions.

Assessments review the implementation of core IT security practices.

The three assessments have reviewed many of the key IT security program features discussed in the National Institute for Standards and Technology's handbook, An Introduction to Computer Security. The key assessment components include:

- Security Policies
- Security Awareness and Training
- Physical Security
- Incident Handling
- Identification and Authentication
- Logical Access Controls
- Cryptography

The higher education assessment team has covered all of these key components at some point during their assessments. As such, we feel that the assessments are comprehensive in scope. Each round of assessments was well documented by the team, following a task list that defined each of the assessment's objectives. To achieve these objectives and catalog their findings' significance, the team has used the rating scale shown in Figure 2.1 to maintain consistency for each evaluated area.

Figure 2.1 Identified Vulnerabilities Were Rated From Acceptable to Help Institutions Prioritize Corrective Actions. Each test area is evaluated and given the status of the vulnerability. Definitions of each status were included in the 2011 reports.

The team determined the severity of issues identified at each institution.

Status Results	
Acceptable	All tests performed for this test showed that no significant vulnerability existed at the time of the assessment within the scope of the task.
Warning	During the assessment task, vulnerabilities may have been identified. The vulnerabilities discovered either do not pose significant risk, or are protected through some technological means.
Vulnerable	Tests performed showed that a vulnerability existed which has the potential of exposing the organization to information leakage. Specific exploits during the time of the assessment were unsuccessful in accessing the data.
Highly Vulnerable	Test performed during the assessment showed a vulnerability which was successfully exploited which lead to information leakage or privileged access to systems or services.
Critical	Test performed during the assessment showed a vulnerability which was successfully exploited and lead to the exposure of critical and/or sensitive information.

The team's findings are documented in reports that go to each individual institution. While the reports focused on reporting negative conditions, our observations at three institutions during this assessment showed consistency in the team's activities.

As will be discussed later in this chapter, the institutions have implemented most of the recommendations in the assessment reports. Therefore, as the assessment program progresses, each newer assessment becomes more focused on the areas of greatest risk. Initially, assessments were broad and included a variety of tasks. Recent assessment activities have become more limited and focused on scanning for vulnerabilities and attempting to penetrate security measures.

The 2011 round of assessments was more collaborative since institutions began covering some costs.

For the 2011 round of assessments, the institutions rather than the Board of Regents began covering the assessment costs beyond the donated time of UEN and institutions employees. Since the institutions are paying for a share of the IT assessments, institutions seem to have a more positive outlook. Institution staff and the assessment team are now collaboratively working together to

determine the status of IT security at the schools. Institution staff reports that the current round of assessments has been more collaborative than prior assessments.

Other Assessments Follow Similar Methodologies

The assessments conducted by the higher education assessment team employ nationally recognized best practice techniques similar to those used in other assessments. The National Institute of Science and Technology (NIST) has identified several techniques to incorporate in IT security assessments. Similar techniques were used by the Legislative Auditor General's Office in Arizona during their assessment of Arizona's higher education institutions. Utah's higher education assessment team's approach is consistent with those used and recommended by others.

The assessment team relied on a variety of techniques to test and verify institutions' IT security systems.

IT security assessments involve a variety of tasks that determine whether a system provides adequate levels of protection. In NIST's Technical Guide to Information Security Testing and Assessment, several techniques are listed that enable an assessment team to layer evidence of adequate controls. Figure 2.2 identifies types of techniques that are included in the guide. Assessment technicians must possess the specific skills necessary to administer each test.

Figure 2.2 IT Security Assessment Techniques Recommended by NIST. Several techniques can be implemented during assessments. Each technique requires specific skills to perform the necessary tasks.

Type	Techniques
Reviews	Documentation Review Log Review Rule Set Review System Configuration Review Network Sniffing File Integrity Checking
Target Identification and Analysis	Network Discovery Network Port and Service Identification Vulnerability Scanning Wireless Scanning
Target Vulnerability Validation	Password Cracking Penetration Testing Social Engineering

Our review of the reports and assessment objectives found that the assessment team was relying on these various techniques.

The Office of the Auditor General in Arizona also relied on similar assessment techniques when they evaluated Arizona's higher education institutions. Their scope focused primarily on web-application development, information security officers, and IT security programs, applying all three techniques in their audit. The team reviewed documentation regarding each institution's security organization to ensure they were appropriately designed. Target identification was conducted through network scans which identified the actual number of significant web-based applications. Then vulnerability validation was performed by penetration testing sampled applications.

Utah's higher education assessment team has used these techniques as they evaluated each institution's IT security infrastructure. As stated earlier, initial assessments were vast in scope, but over time, each round of assessments has become more focused. We believe that the assessments being performed by higher education are appropriate given the technical expertise, methodologies, and frequency of the reviews taking place.

Security Personnel Are Key to Implementing Recommendations

Most schools have implemented the recommendations that were included in their assessment reports. However, the 2008-2009 assessments identified a lack of implementation at two institutions that received recommendations in 2007. These two institutions also received findings about lacking full-time Information Security Officers (ISO). A third institution that also lacked a full-time ISO made major improvements that were noted by the assessment team during one of the assessments we attended. Considering the improvements at the third institution, institutions that lack ISOs should expedite their plans to find the necessary resources to fill this critical position.

From 2007 to 2008, most institutions implemented recommendations from the assessment team's reports. If no continuing problems were identified, a section regarding prior assessment recommendations was omitted from the reports.

In 2008, the team raised concerns about two schools that did not implement earlier recommendations.

However, two institutions did have these sections in their reports because the assessment team felt that some recommendations had not been addressed. Therefore, the team felt warranted in including a section addressing the continuing problem to raise awareness on the lack of implementation.

The team also raised concerns about these institutions' lack of a full-time ISO. According to State Board of Regents rule, the ISO should "report directly to a senior institutional administrator" and is "responsible for the coordination, review and approval of procedures used to provide the requisite security for Private Sensitive Information or Critical IT Resources." We believe that the lack of a staff member dedicated to IT security issues is related to the non-implemented recommendations and continuing unresolved issues.

The same two schools did not have a full-time ISO to mange campus IT security operations.

The impact of hiring an ISO was apparent during this recent round of assessments. A third institution that lacked an ISO in 2008 found the resources to create an ISO position. Their new ISO addressed concerns identified in the 2008 assessment, and the assessment team noticed significant changes. A theme during the assessment team's exit conference this institution was the vast improvement since 2008. The institution's Chief Information Officer credited their new ISO position as the catalyst for the improvement.

One institution is still seeking the resources to hire a full-time ISO. The institution's IT group reports having a plan to hire someone in the near future. Given the positive results at one institution, this institution's plan to fund this position seems a positive step in improving their IT security program. While a single individual may not be adequate to make all necessary changes, they should be adequate to assess what technical expertise would be required to implement satisfactory solutions.

Recommendation

1. We recommend that institutions ensure they have a full-time Information Security Officer dedicated to addressing IT security issues.

Chapter III
Key IT Security Features Needed at Quasi-Government Agencies

Quasi-government agencies have implemented some information technology (IT) security program controls; however, additional steps can be taken to strategically strengthen agency security. Agencies often lacked key security features, such as written policies, IT security awareness instruction, and adequate business continuity plans. Agencies, as a whole, also appear to be lacking assurances that adequate controls are in place to protect their most sensitive information assets. This report provides recommendations that agencies can take to document and strengthen their IT security programs.

IT security best practices were identified in publications by NIST and the SANS Institute.

Several resources are available to help agencies develop a security program that better meets agency needs. The National Institute for Standards and Technology (NIST), within the U.S. Department of Commerce, as well as the System Administration, Networking, and Security Institute (SANS) have publications that provide guidance on developing better IT security programs. In addition, small agencies like special service districts can get assistance from the Utah Association of Special Districts. The association has over 380 special district members and provides management services as needed, including the creation of agency policies. The Association has voiced its desire to help these districts address IT security needs.

Agencies Should Adopt Basic IT Security Features

All agencies we reviewed have implemented some IT security features to protect their systems and data; however, we believe some agencies are missing key features that strategically implement specific technical controls and educate employees about security risks. The absence of these features could leave agencies open to unnecessary risk. Key features that could be improved in the reviewed agencies and should be incorporated in other small agencies to improve IT security programs include:

- IT security policies
- IT security awareness instruction
- IT continuity plans

These key features can be found in NIST's special publication called "An Introduction to Computer Security: The NIST Handbook." The handbook provides an overview of IT security and separates controls into three categories: managerial, operational, and technical. These controls help agencies develop a more structured approach to designing and implementing their IT security programs. As mentioned in Chapter I, we will not discuss the specific technical solutions each agency has implemented. Specific technical solutions should be determined by management after consideration of various factors.

Agencies Need IT Security Policies

Agency staff members typically were not aware that they needed written policies. As an example, some smaller reviewed agencies did not document their IT security practices in their policies. One agency under review improved its practices and began drafting policies as it realized its security shortfalls. This audit report, as well as the Utah Association of Special Districts, can help raise awareness regarding the need for policies as well as point to resources to help management with the drafting process.

Some smaller agencies' policies were missing or incomplete.

As part of our review of quasi-government agency policies, we focused on four smaller agencies with fewer than 50 employees. Unlike the larger agencies which had comprehensive polices, these agencies were either lacking or working on enhancing their policies. Of the four smaller agencies we reviewed:

- Two agencies did not have any policies when the audit began.
- One had policies for their outward-facing network but lacked internal network policies.
- Another agency had a significant number of appropriate policies and was in the process of drafting additional polices.

IT security policies are essential since they outline key objectives.

While policies were not in place at some smaller agencies, we did find that they all still had some security measures in place. Without policies, it is difficult to determine what actions have been taken to address security risks. In addition, policies are essential to ensure

operations are carried out consistently and cover all of critical areas identified during risk assessment activities. Therefore, the lack of policies raises concerns whether IT security controls have been thoughtfully implemented.

During the audit, the two agencies that were lacking policies drafted and adopted written IT policies for their agencies. One of the agencies shared some specific improvements that they made to their IT security program. For example, the agency had an existing practice of periodically backing up their data and storing it on site. However, the agency realized that there was risk associated with storing all data at a single location. As a result, their new policy requires off-site storage of these backups to mitigate this risk.

Staff members at agencies without policies were not aware that they needed policies. These small agencies outsourced their IT services, leaving no IT professionals in-house to promote IT security. We are hopeful that best practices discussed in this report will be read by these smaller quasi-government agencies. In addition, associations, such as the Utah Association of Special Districts, can help promote these IT best practices as they help small districts adopt good management practices, including model policies and procedures.

All quasi-government agencies need to adopt appropriate IT security policies. These policies should include a program policy that provides the overarching objectives of the IT program. The program policy can be supplemented with additional issue or system-specific policies as needed by the agency. Several resources exist to help agencies develop a working set of IT security policies. The SANS Institute, a research and education organization, provides several resources to help agency management get started. As an example, the SANS Security Policy Project provides policy templates at no cost. In addition, NIST publishes several special publications that can help agencies draft policies that meet their needs.

The SANS Security Policy Project provides guidance on drafting policies.

Employees Should Receive IT Security Awareness Instruction

While all agencies required their employees to agree to an acceptable use policy, agencies' efforts fell short on training their employees to be aware of security issues that can put IT resources at risk. The NIST handbook recommends making users aware of their

responsibilities and teaching them appropriate practices to promote the desired IT security behavior. Whether agencies rely on free training from the State or some other resource, agencies need to ensure that employees are trained on appropriate IT security practices to protect agency assets.

Most quasi-government agencies only provide IT security awareness training during new hire training.

Currently, quasi-government agency IT security awareness training is typically a onetime event during the hiring process. As part of the process, employees review agency policies and procedures, including a section on acceptable use of office electronic equipment. At the end, the employee usually signs an acknowledgement that they have read and understand the policies. Typically, there is no structured annual training on acceptable IT equipment use or security issues. Agency management did say that, on occasion, employees are exposed to some IT security issues during another training event, but no formal training with the sole focus of IT security awareness is provided.

Untrained users present a significant risk to agencies' IT security. According to the NIST handbook, "human actions account for a far greater degree of computer-related loss than all other sources combined." Thus, agencies should invest in providing employees the instruction they need to protect information assets. The NIST handbook distinguishes two types of employees that need different types of instruction: awareness for basic users and training for users who maintain the IT infrastructure. The following table highlights some of the key differences between these levels of instruction.

Figure 3.1 IT Security Instruction Has Different Characteristics for Different Users. The intensity of instruction is illustrated by six characteristics in the table. Agency users require a different level of knowledge based on their level of interaction with the IT infrastructure.

	Basic User Awareness	IT Staff Training
Attribute:	"What?"	"How?"
Level:	Information	Knowledge
Objective:	Recognition	Skill
Teaching Method:	Media	Practical Instruction
Test Measure:	True/False, Multiple Choice	Problem Solving
Impact Timeframe:	Short-Term	Intermediate

* Source: *An Introduction to Computer Security: The NIST Handbook,* page147, figure 13.1.

Since nearly all employees interact with IT systems, users need to be made aware of security threats they can introduce to the IT system. As seen in Figure 3.1, the instruction these users require is relatively simple, but needs to be repeated regularly due to its short-term impact.

Awareness training typically has a short-term impact, which requires concepts to be presented regularly.

Three of the six agencies we reviewed have contracted out their IT services, minimizing their need for intensive IT staff training. However, those agencies with in-house services need to ensure they provide more than just awareness training. IT staff members need knowledge-based training to increase and build their security control abilities.

For all agencies throughout the state, the Department of Technology Services has compiled an online awareness program. We recommend that agencies without formal IT security awareness instruction use this or some other instruction for their employees. The Department of Technology Services training informs employees about common threats. The subjects covered in the 2011 training are listed below.

- Why is Cyber Security a Problem?
- Choosing and Protecting Passwords
- Reducing SPAM
- Avoid Social Engineering and Phishing Attacks
- Defending Cell Phones & Smart Phones
- Protecting Your Privacy and the Privacy of Others
- Data Disclosure

The Department of Technology Services provides free training that can be accessed via the Internet.

These topics are designed to familiarize employees with common threats. Although this training will not guarantee the absence of security incidents, educated employees should help reduce the likelihood of such incidents. Since the Department of Technology Services provides this training free of charge, all agencies should be able to incorporate IT security awareness instruction into their training curricula. Agencies can access this training by registering for a free Utah-ID at https://login.utah.gov/login/. Once a login is obtained, the training can be accessed at www.training.security.utah.gov/sota.

Comprehensive Continuity Plans Should Be Prepared

The essence of IT continuity planning is to be prepared for the unknown. While specific losses may not have occurred yet, it is best practice for agencies to have a plan in place that addresses several potential interruptions to operations. We reviewed the NIST handbook and identified the following four issues that were often lacking in IT continuity plans:

Most agencies' continuity plans are limited in the number of threats, assets, and scenarios they cover.

- Incident-handling procedures that are limited in scope
- IT continuity plans that are limited to only protecting data
- Access to vendor-administered systems

Each of these topics has a common theme: organizations need to do more than just addressing the basics. This audit report identifies several instances where smaller quasi-government agencies were lacking these components of adequate IT continuity plans. Larger agencies have done a good job developing a plan that allows them to continue their operations relatively quickly if an interruption takes place. Agencies should review aspects of their business continuity plans and make changes if needed.

Incident-Handling Procedures Should Address Various Incidents. Some reviewed agencies have not adequately defined their incident handling responses. NIST identified some types of incidents that might need to be addressed, including:

- Corrupted data files
- Malicious code
- Unauthorized access
- Natural disasters

Most incident-handling policies do not consider multiple threats.

Each of these incidents likely requires a different response. Three of the six reviewed agencies' do not have incident-handling processes specified in their policies. In addition, a fourth agency only had a single response specified for all types of incidents, which seems inadequate. The other two agencies have fairly comprehensive policies. Specifically, one of the agencies outlined the possible consequences of inappropriately sharing software (inappropriate use), help desk software that tracks user issues (malicious code/denial of service), as well as other features. This policy is an example of a fairly

comprehensive incident-handling solution that other agencies could emulate as their resources allow. While resources to implement automated solutions may not always be available or necessary, agencies should still consider documenting the procedures necessary to handle various incidents.

Other Agency Assets Should Be Considered in Continuity Plans. Five of six agencies have some sort of business continuity plan written in policy. Four of the five plans were limited to backing up data or retaining documentation without considering the other resources required to process the data. According to the NIST handbook, several different resources besides data need to be considered, as listed below.

- Human resources
- Processing capability
- Computer-based services
- Applications
- Physical infrastructure

Agencies should consider all assets required to process data if IT system disruptions occur.

Agencies need to ensure that each of these areas is appropriately addressed in cases of service interruption. The NIST handbook illustrates how each of these resources can limit the ability to process backup data. Agencies should review their IT continuity plans and ensure that their processing capability addresses proper use and consideration of all agency resources.

Agencies Should Ensure They Retain Access to Systems Administered by Vendors. Staff at one agency shared their experience with losing temporary access to a system after terminating service with a contracted provider. Two other agencies do not have written contracts with their providers and may be at risk for a similar experience without controls in place to ensure continued access. Staff at one agency said that a contract with their providers did not make sense because they did not want be tied to a single provider for a specific amount of time. While these arrangements may be flexible, agencies need to protect themselves from losing access to critical systems if their contracted providers leave. If a contract is not desired, the agency should ensure they retain information, such as network diagrams and account access, which would allow for uninterrupted service.

Agencies using IT vendors need to ensure they maintain informational control and access if their agreement terminates.

Agencies Need Assurance That Controls Are Adequate

Assurance activities give confidence that valid controls have been implemented and configured appropriately. Agencies have relied on assurance activities to different extents. Since testing activities can be expensive, agencies should include discussions about assurance activities when they conduct risk assessments to ensure their most sensitive assets are protected.

Agency management should consider testing their IT security solutions to ensure proper configuration.

According to the NIST handbook, "security assurance is the degree of confidence one has that the security controls operate correctly and protect the system as intended." Agencies can gain assurance that controls are operating appropriately by conducting ongoing monitoring activities and periodic audits or assessments. Assurance activities, such as vulnerability scans, which identify network resources, and penetration testing, which attempts to exploit unprotected resources, systematically test IT security systems for weaknesses.

Testing activities varied greatly among the agencies we reviewed. For example, one agency contracted for a physical security assessment because they were concerned with their current practices. Another agency, which is in process of developing their IT security program, has not performed vulnerability assessments but plans to in the future.

While potentially costly, some agencies have performed IT security assessments.

Conducting assurance testing activities can be costly for an agency. Therefore, it makes sense to closely align testing activities with risk assessment results. For example, one reviewed agency conducted a risk assessment of their systems and found minimal need to protect IT assets. Consequently, the agency has very few assurance measures. As discussed in Chapter I, agencies deal with a variety of different information assets and have different requirements to protect that data. We recommend that agencies consider validating their controls as part of their risk assessment practices when evaluating an agency's information assets.

Recommendations

1. We recommend that all quasi-government agencies adopt written IT security policies.

2. We recommend that agencies lacking formal IT security awareness training provide appropriate instruction on IT security issues.

3. We recommend that each agency review and make necessary changes to their IT continuity plans.

4. We recommend that agencies develop testing procedures to validate controls as part of their risk assessment activities for valuable assets.

This Page Left Blank Intentionally

Agency Response

This Page Left Blank Intentionally

This Page Left Blank Intentionally