Information Security Strategic Plan

State of Kansas
Enterprise Security Office
Information Security Strategic Plan
Chief Information Security Officer

Background

- Purpose for the development of the IT Security Strategic plan was to provide a roadmap to reduce risk and exposure to the State.
- The findings revealed in LPA Audit Report R-14-007 2014 concerning the lack of funding, lack of adequate personnel, and lack of data classification management.
- Increasing attacks against the State IT Infrastructure.
- CISO findings compared against SAN 20
- LPA Committee request for a plan on how to fix the issues and what the cost would be to do so.

Audits

- Repeated findings spanning more than five years
  - Audit findings that are repeated year after year indicate a fundamental lack of accountability with regard to State information resources.
  - Lack of qualified security personnel, reporting, and organizational structure has greatly contributed to the overall increase in Risk to state information resources
  - The decentralized approach to both IT and IT Security have made implementing enterprise class solutions to provide consistency and common standards across the enterprise extremely difficult and thereby increasing our exposure to an ever-growing number of cyber threats
  - Standardization and centralized security controls allow organizations to establish and maintain excepted security standards, which reduce overall exposure and decrease risk to the enterprise.

Audit Strategy

- What changed?
  - In December of 2013, the CISOs office sat down with LPA Auditors and asked the question "we have done the same audit year after year, with the same results, do we want to continue doing it? Or should we be asking different questions that might help determine the root cause and truly improve the situation?

  - I'm a member of a national committee that conducts evaluations on all 50 states, our findings are made available to the States and to the US Congress. What we found in 2012 was that States neither had adequate security staff nor adequate security funding, and there was and still is a lack of awareness of what sensitive data is and how to classify it to in order protect it appropriately.

Audit Kansas Trending

- Another question asked was whether or not Kansas is trending with the Nation; after the conclusion of latest round of LPA security audits it was determined that Kansas was trending with at least some States, but unfortunately this trend is not in the right direction. According to some Kansas is on a direct parallel path with South Carolina prior to their 100 million dollar plus breach.
- That trend towards a major breach is real; it might be said it is not a question of if, it is truly a question of when, if not already. The risk continues to increase; the inability in a decentralized security setting to protect our information resources is unreasonable and unmanageable.
- While certain functions of IT can be managed in a decentralized fashion, security (for the most part) cannot because of the nature of what it does. In an environment where establishing and adhering to standards, accountability and reducing risk is subject to an ever growing gap in resources, centralization and consolidation of security and security personnel is paramount.

Strategic Plan

- The plan presented answers two questions; how and how much? Some no longer with the State interpreted Rep Burroughs request during an LPAC hearing in July 2014, as a plan to fix the findings of the last audit. My understanding of Rep Burroughs request was that the LPAC wanted a solution to decade old problem.
- The Kansas population was 2,893,957 in 2013, the cost per Kansas resident to fund the Information Security Office is about $8.50 per person to protect their data for year one. One breach could cost the state in just identity protection alone about $28,939,570.00 per year for several years.
- Over the last three years, I have consulted with industry, government and other security experts, reached out to both KU and KSU CISOs and began to develop an IT Security Strategic plan.
- Normally, this plan would dovetail with an IT Strategic Plan, however, there hasn't been one in several years. While the IT Strategic Plan is in the development stage, the Security Strategic Plan represents the best that it can be at this time.

Strategic Plan continued

- KSU & KU CISO's and I began to look at audit findings, and what we have done in the past to fix similar problems. Combined, myself, the KSU and KU CISOs have over 50 years of experience with IT and IT Security. This plan addresses the action needed to correct not only the audit findings, but to provide a roadmap and strategy for success of the State of Kansas IT Security program over the next 5 years.
- Citizens, residents and businesses of Kansas look to the State to protect the information they have provided to the State, it is our responsibility to ensure that we maintain the Public Trust. One of the guiding principals in the development of the plan was to make sure we provided for Public trust. Information Security for government is the enabler of technology and business.

Strategic Plan Fix

- The plan calls for the consolidation of security technology and security personnel. It calls for the complete funding of security, so that agencies no longer need to make the hard choice to sacrifice security as the result of reduced agency funding. Likewise the consolidation of security technology and personnel removes the burden of determining what adequate security resources they may need.
- The plan calls for the development of the KISO, (Kansas Information Security Office) which is stand-alone from OITS. The new KISO would report to State Security Council (regularly) and to Legislative, Judicial and ITEC CITO's, as required or requested. This would be both through formal and informal methods.

The Fix and Cost

- People are a number one concern. It does no good to have technology deployed if you don't have the bodies to respond and fix the situations. No amount of software or hardware can reduce the risk to an acceptable level for the State. Only trained, qualified security professional have the necessary skill sets to do so.
- Consolidation of personnel that report directly to the CISO, and the CISOs office reports risk directly to the Secretaries, or the appropriate senior executive. Security personnel must report independently of the CIO and IT Infrastructure as noted in LPA audit findings.

Kansas Information Security Office (KISO) Formation

- KISO to provide all security personnel, enterprise technology solutions to State government.
- KISO will support, develop and manage identity access management for all systems.
- KISO will maintain and manage through a Managed Security Service, all firewalls, intrusion detection systems and other security controls as meet agency requirements.
- KISO will provide to agencies, boards, and commissions a "trained" security professional to perform the functions of Information Security Officer.

KISO Secure Kansas

- KISO will provide as needed, or required, limited support for municipalities and counties of the State.
- KISO will provide assistance and support to educational institutions in the State to protect the information of Kansas students grades K-12.
- KISO will continue to develop a comprehensive relationship between the Regents and the State.
  - In 2013 as the Chair of the Security Council, I directed the development of a sub-committee to rewrite the State Security Policy to not only better serve the State, but to also serve the regents. With the assistance of the CISO from KSU, KU and others, the security council delivered to the State a revised Security Plan that both the Regents and the State have agreed to use. This marks the first time that both regents and State will operate off the same Security Policy.
  - It will be the goal of the KISO to continue to develop various security programs and embrace the goal of mutual support and mutual growth of both the Regents and State security programs.

Dec 11, 2014 Financial Services Sector

- On December 9, Hackers breached payment solutions provider CHARGE Anywhere: Undetected since 2009. Electronic payment solutions provider CHARGE Anywhere stated December 9 that attackers had gained access to its network as early as November 2009 using a previously unknown and undetected piece of malware and were able to capture payment card data from some communications that did not have encryption. The company discovered the compromise September 22 and an investigation found that network traffic capture occurred between August 17 and September 24.
- What is important to note is that the attackers were in the network undetected for over 5 years. "The investigation revealed that an unauthorized person initially gained access to the network and installed sophisticated malware that was then used to create the ability to capture segments of outbound network traffic," the company said. "Much of the outbound traffic was encrypted. However, the format and method of connection for certain outbound messages enabled the unauthorized person to capture and ultimately then gain access to plain text payment card transaction authorization requests." This type of attack would seem to indicate lack of adequate trained person, lack of monitoring, lack of personnel to respond to the situation. Very similar to our situation here in the State today.

Dec 11, 2014 DHS Open Source Report

- On any given day we look at these threats as well as hundreds of others that are similar in nature. And since there is no centralized security, no way to enforce security standards at the end of the day we realize how lucky we were not to have been hit. And we go on to do it again the following day, 7 days a week. But for how long before we are just one of the victims or a causality of the Cyber-Wars

  - December 10, Red October cyber spy op goes mobile via spear-phishing. Researchers with Blue Coat and Kaspersky Lab identified and analyzed a cyber-espionage campaign that appears similar to the RedOctober campaign dubbed Cloud Atlas or Inception Framework that has been targeting the Android, iOS, and BlackBerry devices of specific users in the government, finance, energy, military, and engineering sectors in several countries via spearphishing. The malware appears to primarily be designed to record phone conversations and can also track locations, monitor text messages, and read contact lists.
  - December 10, Trihedral fixes vulnerability in SCADA monitoring and control software. Trihedral Engineering Ltd., released software updates for its VTScada (VTS) supervisory control and data acquisition (SCADA) software to close a vulnerability that could be used by an unauthenticated attacker to crash VTS servers. The software is used in industries including the energy, chemical, manufacturing, agriculture, transportation, and communications sectors.
  - December 10, Flash Player 16.0.0.235 fixes remote code execution bug exploited in the wild. Adobe released patches for six vulnerabilities in its Flash Player software, including a vulnerability reported by a researcher that could allow arbitrary code to be executed on affected systems. The arbitrary code execution vulnerability has been observed being exploited in the wild and all users were advised to update their versions of Flash Player as soon as possible.
  - December 10, SQLinjection, other vulnerabilities found in InfiniteWP admin panel. A researcher with Slik identified and reported several vulnerabilities in the InfiniteWP administration application for WordPress Web sites, including SQL injection vulnerabilities that could be used by an unauthenticated attacker to gain control of WordPress sites.
  - December 10, Flaw in AirWatch by VMware leaks info in multi-tenant environments. VMware released an update for its AirWatch enterprise mobile management and security platform December 10 that closes vulnerabilities that could allow a user that manages a deployment in a multi-tenant environment to view the statistics and organizational information of another tenant.

Dec 11, 2014 DHS Open Source Report

- December 10, Flash Player 16.0.0.235 fixes remote code execution bug exploited in the wild. Adobe released patches for six vulnerabilities in its Flash Player software, including a vulnerability reported by a researcher that could allow arbitrary code to be executed on affected systems. The arbitrary code execution vulnerability has been observed being exploited in the wild and all users were advised to update their versions of Flash Player as soon as possible.
- December 10, SQL injection, other vulnerabilities found in InfiniteWP admin panel. A researcher with Slik identified and reported several vulnerabilities in the InfiniteWP administration application for WordPress Web sites, including SQL injection vulnerabilities that could be used by an unauthenticated attacker to gain control of WordPress sites.
- December 10, Flaw in AirWatch by VMware leaks info in multi-tenant environments. VMware released an update for its AirWatch enterprise mobile management and security platform December 10 that closes vulnerabilities that could allow a user that manages a deployment in a multi-tenant environment to view the statistics and organizational information of another tenant.
- December 10, Recursive DNS resolvers affected by serious vulnerability. The Computer Emergency Response Team Coordination Center (CERT/CC) reported December 9 that recursive Domain Name System (DNS) resolvers are vulnerable to an issue where a malicious authoritative server can cause them to follow an infinite chain of referrals, leading to a denial of service (DoS) state.

Dec 11, 2014 DHS Open Source Report

- December 10, Third-party bundling made IBM products most vulnerable: Study. Secunia released a report on security vulnerabilities disclosed between August and October and found that vulnerabilities increased by 40 percent compared to the previous year to a total of 1,841 vulnerabilities in the 20 most vulnerable products, among other findings. The report also found that Google Chrome had the largest number of disclosed security issues, and that IBM was the most vulnerable vendor due to products being bundled with third-party software.
- December 9, Microsoft releases critical IE security update on Patch Tuesday. Microsoft released its monthly Patch Tuesday round of updates for its products December 9, which included 7 security bulletins addressing 24 vulnerabilities. Three vulnerabilities were considered critical and affected Internet Explorer, Microsoft Word and Office Web Apps, and the VBScript scripting engine.
- December 9, New version of Destover malware signed by stolen Sony certificate. Researchers at Kaspersky Lab identified a new variant of the Destover malware used in an attack on Sony Pictures Entertainment that uses a stolen, legitimate certificate from Sony. The malware is basically identical to previous versions except for the use of a certificate.
- December 9, SEO poisoning campaign ensnares several thousand websites, security expert finds. A webmaster identified and researchers from Websense and High-Tech Bridge confirmed that several thousand legitimate Web sites hosted on GoDaddy and other services had been compromised to improve the search engine optimization (SEO) ranking of other sites by inserting links into the legitimate sites. GoDaddy stated that the company was investigating the issue.

Finalizing

- No amount of funding, personnel or technology can assure that an incident does not occur.
- What can be guaranteed is that disclosures, incidents and breaches will occur, so the real question is how well we are able to respond to these events? Based on the State's lack of vigilance to this issue, the current lack of security resources and the decentralized approach to IT and IT security, these events will most certainly result in Major breaches and headline news.

Ending

- We would like to provide to all members of the legislative branch information on a couple of services that we provide that all state, county and municipalities can take advantage of.
- I would personally like to thank you for your time and allowing me to present an overview of our Security Strategic Plan.
- Questions?

STATE OF KANSAS
Information Security Strategic Plan

September 2014

Developed By:	John Byers, Chief Information Security Officer Kansas
Contributions:	Rodney Blunt, Deputy Chief Information Security Officer Kansas
	Robert Vaile, Chief Information Security Officer Kansas State University
	Rob Arnold, Chief Information Security Officer Kansas University
Reviews:	Joseph F. Martin II, CISSP, CIPP/US/G, CHSS Leadership Partner, EITL Security & Risk Management Gartner, Inc.
	State of Kansas Security Council

Table of Contents

1 EXECUTIVE SUMMARY

Information Security as a professional discipline has one basic, primary mission: protect the confidentiality, integrity, and availability of an organization's information assets. When that organization is governmental, those goals take on a much larger significance since much of that data is personal data on the citizens that live, work, and play in the State of Kansas. Information security, in this context, becomes much more of a calling than a discipline or a characteristic. It is a protection similar to the protection of a citizen's basic rights, and it must be done efficiently and professionally.

This Information Security Strategic Plan acknowledges that the information security capability of the State is insufficient to support its critical mission. Of the ten core functions of enterprise information security outlined in this plan, few of the functions are fully operational in the State. The plan proposes to build an organization comprised of individuals with the security expertise to execute the foundational security functions, based on risk management principles. Of concern is the audit findings over the last five years and the findings of the 2014 audit.

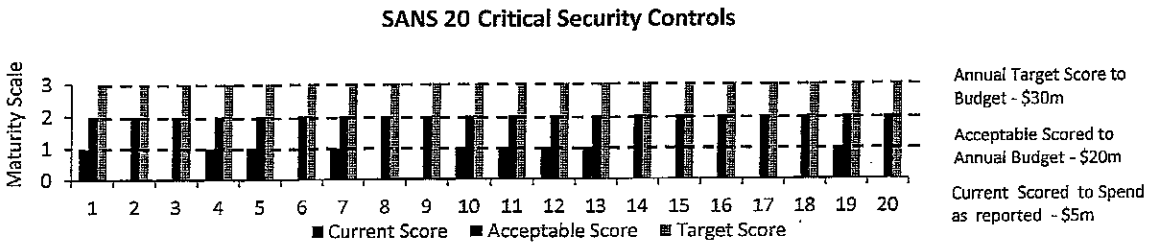
On July 22nd Rep. Burroughs asked two questions; how much and how long will it take? The funding for the program is critical to the success of the program and it's important to look at how funds are spent rather than just how much is spent. WISEGATE RESEARCH 2013 reported that, on average, 7.5% of the IT budget is spent on security. Gartner supports the consolidation of all Information Security functions to a single office as the most cost effective and efficient way to accomplish a mature security program. The time to realize real benefits should be less than two years and to full maturity around four years with proper funding.

Furthermore, the Twenty Critical Security Controls are used as a tool with which to measure the current and future information security capability within the State's enterprise, as well as the basis for individual goals that the proposed Kansas Information Security Office will work to obtain. It is proposed that these critical controls be implemented in phases as the people, process, and technology components of the security program are developed, with a high level of collaboration with the IT organizations of the State.

It should be understood that implementation of a comprehensive information security program, by its very nature, is disruptive. Information Security cannot be implemented as a wrapper with little to no impacts on the manner in which information technology is implemented and managed, or how users access and employ the technology and information at their disposal. While it is a clear goal of any security initiative to reduce the impacts to individuals as much as possible, some impact will remain in order for change to be had. It is, therefore, critical to the success of the Security Plan that support exists at all levels of the State administration. Without it, a successful implementation will be nearly impossible, and any adverse impacts will be magnified.

This plan was developed based on the collective security expertise of a number of security professionals, and with significant input from industry and governmental experts who may be beneficiaries of the success of the program. As such, a high level of confidence exists that the plan presented herein can be successful if appropriately funded and supported.

To determine the cost of implementing this plan, common solutions were identified to address each of the SANs 20 Critical Security Controls. In addition, a survey was conducted to determine what solutions are currently deployed as well as identifying who performs security tasks and functions; the following table illustrates the correlation of resources as they applied evenly across the security controls.



Note: The national average percentage of IT spend for Information Security is 7.5%, for Kansas that comes to approximately $30 million.

The above charts represents the amount of spend in relationship to completeness of the security program and the protection applied. Currently, the State has dodged many of the issues that other organization and states have faced. It is however a matter of time and our abilities to dodge, that will give way to the same issues others have faced. In order to avert that situation and achieve a level of security to protect the State of Kansas and the residents of Kansas we believe that through consolidation and realignment of resources, there are certain efficiencies that will be attained through the consistencies realized as a result of these efforts. Further, we estimate that the State will be able to attain an acceptable level of information security at a level far less than the national average.

2 FOUNDATIONAL INFORMATION SECURITY FUNCTIONS

The overall goal of information security is to protect the confidentiality, integrity, and availability of information and information systems. Combining the protection of these three elements provides a certain level of assurance to an organization that its information and other information resources are protected appropriately.

There are several information security functions that must be performed in order for comprehensive security to operate in an enterprise environment to protect information assets. These basic functions are all common to effective information security organizations in public or private sectors. A description of these functions is provided below.

2.1 Governance

In order to implement information security within any enterprise organization, authority over information security must be established. That authority must be sufficient to affect change, and be extensive enough to maintain insight over all potential impacts to information security within the State. Even if all other fundamental functions of information security exist within an organization, governance must be configured correctly in order for information security to be enabled.

As it relates to the State of Kansas, governance includes proper placement of the KISO to govern information security within the political branches of the government, the reporting relationship of the senior leader of the office, and the extent of the authority over information security within the State. It is specifically recommended that the office report to the Security Council, with additional reporting responsibility to JCIT and ITEC. The office must remain independent of the State's service organizations in order to maintain strong security controls in the face of political pressures that could deprioritize the implementation of those controls. The office must have policy-making ability, insight into any impactful agency operation, and must be held accountable for progress of security posture in accordance with this plan.

2.2 Risk Management

Building information security into any enterprise organization has as its goal to manage a class of risks that face the organization. As such, management of threats to the confidentiality, integrity, and availability of information assets is the core mission of the KISO. In order to manage risk, sensitive data compilations and critical systems must be identified, tracked and monitored. Adequate controls must be placed around these information assets to ensure ongoing protection. Processes must be put into place to gain information on these information assets within all political subdivisions, and all projects that will interact with these assets must be subject to review and implementation of appropriate controls.

It should be understood that sound security practice does not necessarily eliminate risk. Risk may be managed through avoidance, reduction, transfer or acceptance. Risk may be characterized as the quotient of probability of a threat exploiting a vulnerability, with the impact of that exploitation. Risk management practices dictate that conditions that pose higher risks should be prioritized over those that present lower risks. In establishing and growing the KISO, risk management will dictate the priorities of that office, as well as the approach that the office personnel take in helping to mitigate the risks of the State.

2.3 Incident Response

Despite the best efforts of State personnel in establishing controls that defend and protect Kansas information assets, nefarious actors will continue to seek to exploit vulnerabilities, and personnel may make mistakes in provisioning and operating security controls. When these events occur, the KISO must be equipped to quickly respond to these incidents in order to contain, mitigate and recover from the incident as well as gather vital evidence and detail for any breach notification process. An incident response capability is dependent on a flexible and well-communicated incident response process, together with highly trained security professionals. Because incident response can be complicated and highly technical, the KISO must be able to quickly provide the capabilities to all Kansas entities that require help.

2.4 Vulnerability Management

Information system vulnerabilities provide a frequent attack vector for the exploitation of protected information. As such, managing vulnerabilities on information systems is one of the most important defenses for an enterprise security function to perform. This service is performed by monitoring systems that collect information, record transactions, and provide border defenses. Operating these security technologies that have reach into systems across the State is a vitally important task to a central security function.

2.5 Security Architecture & Engineering

In the same manner that an enterprise IT architecture is intended to establish a unified approach to technology implementations in the State, the establishment of common information security architecture is important to ensure that compatible security technologies are implemented in a consistent manner. Furthermore, security engineering experts must research new technologies needed to meet expanding needs of the State. These technologies currently include:

- Identity management solutions that can be used to authenticate State personnel to the many State information systems,

- Smartcard technologies that will provide common identification and credentials for logical and physical authentication across the State,
- Encryption technologies that protect data in transit and at rest.

These technologies must be integrated into the State security architecture. Security engineers, with project management expertise, must be included on technology projects across the State to determine the proper implementation of security controls, and compatibility with security architecture.

2.6 Security Administration and Operations

Once security technologies are established that allow individuals to be uniquely identified and authenticated to State information systems, the KISO will be expected to provide a level of user administration and operation with regard to State issued credentials. These security administration and operational functions are important to plan for as users adopt security technologies for authentication and authorization.

2.7 Policy and Awareness

In order to unify the implementation of security controls across the State, a security policy must be maintained that is applicable to all State entities. The policy must be flexible enough to take into account the intricacies and needs of different entities, but also consistent enough for control implementation to be adequate across the State. Great strides have been made with the recent publication of a new information security policy at the State, however, these documents must be regularly updated, the subject matter expanded to meet new technology needs, and tools developed to help State entities implement the controls proscribed in the policy.

Once common policy is established, the tenets of that policy must be communicated, clarified, and marketed across the State. Furthermore, security best practices, behavioral guidelines, and the education of State personnel in the techniques used by nefarious actors should be conducted regularly. Creating a culture of awareness of information security within the State is one of the most important roles of the KISO.

2.8 Privacy

Privacy addresses the appropriate collection, use, protection, and sharing of personal information. This includes protecting consumers, citizens, and other constituents from the misuse of their information by providing elements of choice, control, and correction of that information. For both privacy and security to co-exist there must be a strong correlation and partnership between the two domains. Integrating privacy subject matter expertise into the KISO will help to ensure that private information within State information assets remains accurate and that it is appropriately safeguarded. Furthermore, security controls must be implemented in a manner as to not intrude upon the privacy rights of the subjects of those records.

2.9 Compliance

There are two primary compliance objectives that must be implemented into the KISO. The first is statutory and regulatory compliance. Because there exists a multitude of requirements in various federal and state statutes, regulations, and industry mandates to which entities may be subject, the KISO must understand these requirements and implement them into State security policy and standards. Entities should be able to look to a single policy in order to understand the mandates that

apply to them. This will require the KISO, in coordination with other agencies, to create an active program to review newly enacted and proposed legislation and integrate any relevant requirements into policy.

The second aspect of compliance with which the KISO must be concerned is entity compliance with State security policy. Compliance activities will be necessary to ensure that policy has actually been implemented within the various entities, and to understand any challenges relative to security policy control implementation. Compliance activities can be conducted through involvement in State projects, partnership with LPA during audits of agencies, and through annual reporting of entities on various topics. Regular compliance reviews will be necessary to ensure that Kansas information assets are protected on an ongoing basis.

2.10 Disaster Recovery and Business Continuity

Disaster recovery (DR) is the capability of critical IT systems and services to be restored in the event of catastrophic events. The level of DR capabilities appropriate for an information asset is dependent on the Business Continuity and or Continuity of Operations plans that leverage that asset. If a business process is not dependent on the information asset, then less DR capability needs to be built for that asset. Information security expertise typically includes DR engineering capability in support of maintaining availability of information assets. As such, security engineering within the KISO will be built in order to support DR needs within the State.

3 CURRENT ASSESSMENT OF INFORMATION SECURITY IN THE STATE

3.1 Twenty Critical Security Controls as a Measure

In recent years, both government and industry actors in the security community have built consensus around a set of twenty critical security controls, that when fully implemented in an enterprise environment, are most effective at protecting against advanced threats to information security.[1] As such, full implementation of these controls is an optimal goal of security organizations. The controls have a deliberate order to them, with the highest priority controls first. The intention is that the controls will be implemented in order to obtain the greatest benefits from them.

The critical security controls ("CSC's") can be used as a tool to assess information security based on whether each control is partially or fully implemented. For example, one point can be awarded for partial implementation of a control, and two points for full implementation. Progress towards full implementation of all controls (40 points) can be assessed.

3.2 Assessment of State of Kansas

A score of zero indicates that the majority of entities do not have the security controls implemented. A score of one indicates that the majority of entities have the controls partially implemented. A score of 2 indicates that the majority of entities have the controls fully implemented.

The individual controls, and their associated scoring based on the current knowledge of the Kansas Information Security Office is below:

Critical Security Controls	Score
1: Inventory of Authorized and Unauthorized Devices	1
2: Inventory of Authorized and Unauthorized Software	0
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	0
4: Continuous Vulnerability Assessment and Remediation	1
5: Malware Defenses	1
6: Application Software Security	0
7: Wireless Access Control	1
8: Data Recovery Capability	0
9: Security Skills Assessment and Appropriate Training to Fill Gaps	0
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	1
11: Limitation and Control of Network Ports, Protocols, and Services	1
12: Controlled Use of Administrative Privileges	1
13: Boundary Defense	1
14: Maintenance, Monitoring, and Analysis of Audit Logs	0
15: Controlled Access Based on the Need to Know	0

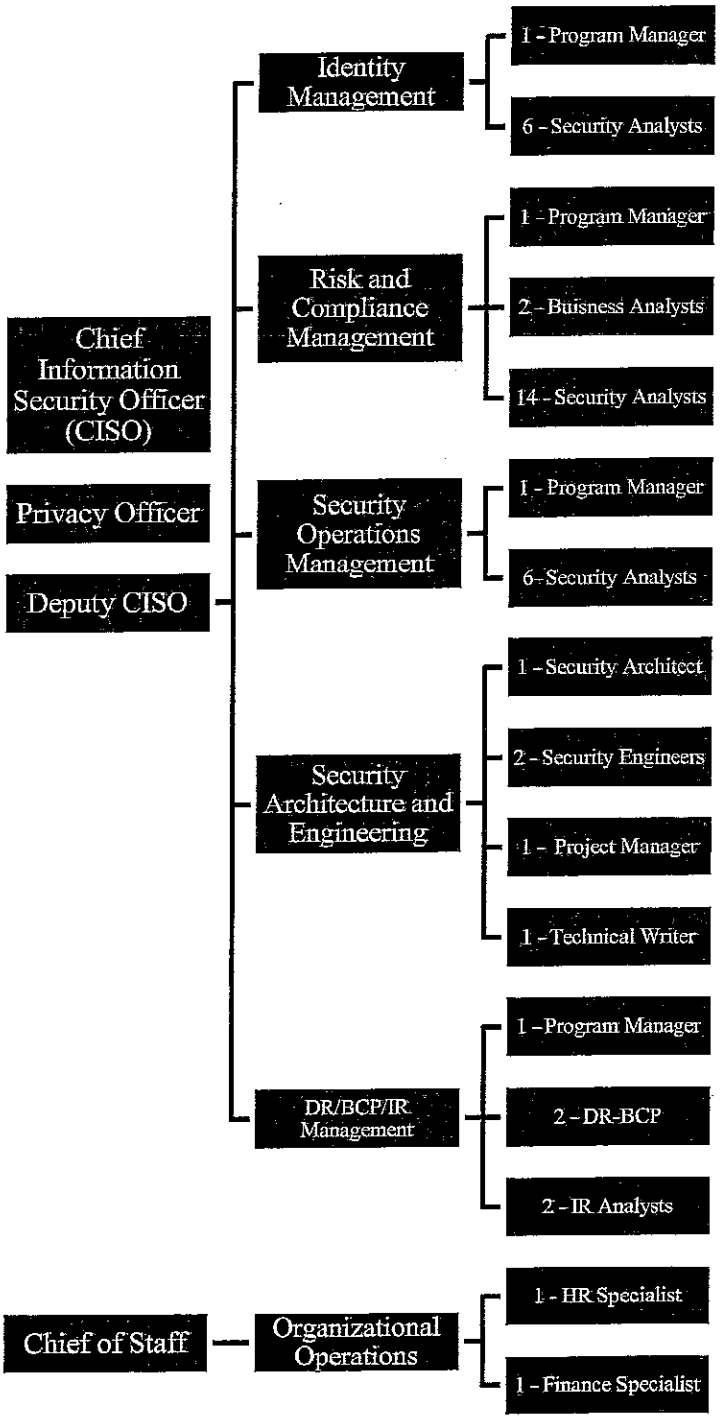
[1] http://www.sans.org/critical-security-controls

16: Account Monitoring and Control	0
17: Data Protection	0
18: Incident Response and Management	0
19: Secure Network Engineering	1
20: Penetration Tests and Red Team Exercises	0
TOTAL SCORE	**9**

While some agencies may and do deploy security controls that provide the minimum adherence to standards, as other agencies do not; therefore, the State of Kansas security control environment on the whole is lacking in the deployment of security standards. As such this creates an environment which is insufficient to protect the information assets of the State in a uniform manner. As with most protection measures you are only as strong as that weakest part of the organization. A review of audit findings for the last five years demonstrates that even those that do it better for the most part suffer the same repeated failures audit after audit. The continued audit failings indicate a systemic problem with applying security control standards, which can easily be attributed to the absence of a central authority with the primary task of ensuring that information security across all agencies is consistently delivered, measured and compliant with all applicable standards, regulations and policies.

4 PROPOSED KANSAS INFORMATION SECURITY OFFICE ORGANIZATION

Building the organization that performs each of the core security functions outlined above will leverage management experience in enterprise security organizations. The numbers of individuals needed is based on the need to fill current deficiencies that exist in the State. The following organizational structure and number of security personnel to staff the KISO is proposed:



5 OVERALL INFORMATION SECURITY STRATEGY

The proposed Information Security Strategy for the State of Kansas provides a phased approach to building an information security capability sufficient to protect Kansas information assets. It is envisioned that the phases will begin serially, but overlap significantly. Each phase, once begun, will continue until the desired maturity level has been reached:

I. **PHASE 1: People and Process** – Build KISO with competent people and effective processes.
II. **PHASE 2: Technologies** – Implement technologies necessary to monitor and secure State information assets.
III. **PHASE 3: Collaboration** – Collaborate with IT and compliance organizations in the State to refine processes.
IV. **PHASE 4: Increase Maturity of Security Capabilities** – Collaborate with the rest of the enterprise to ensure widespread implementation and support.

5.1 PHASE 1: People and Process

Implementing effective information security is dependent on People, Process and Technology. Gathering individuals with expertise in information security that can perform in the foundational functions discussed above is the most important deficiency to address in the State. These individuals must be brought together in a new organization with a clearly defined mission, and clear lines of authority. These people are necessary to make risk-based decisions on further priorities, to build critical processes, and to help educate and change the culture of the State. Once the people are in place, each of the core security functions will begin to operate and significant improvements in the information security posture of the state will be realized.

Building appropriate security processes is the most important second step, and included in Phase 1 of the plan. Processes that provide the KISO with feedback and insight into security vulnerabilities, ensure that technology initiatives are reviewed for security impact, and allow incident response where appropriate are examples of extremely important processes to implement state-wide.

In addition to putting in place the organization, the KISO will work to implement controls 1-10 in the majority of entities within the State, changing each of those scores to at least 1. At a minimum, the overall CSC score should be 14 at the end of Phase 1.

5.2 PHASE 2: Technology

As the third component, technology can be used to automate and enhance processes that have been established in Phase 1. Additionally, a number of core security technologies in the State must be evaluated and implemented in order to unify security authentication and access to State information resources. The most important of these technologies will be a State-wide identity management solution. Building a digital foundation is paramount to building and maintaining a secure enterprise environment.

In addition to adding the core technological solutions in place, the KISO will work to complete the implementation of controls 1-5 across the State and to begin implementation of controls 11-15. At the end of Phase 2, the minimum CSC score of 21 will be achieved.

5.3 PHASE 3: Collaboration

Effective information security is dependent on effective Information Technology practices. Collaboration between IT organizations in the State and the KISO on IT best practices will be necessary in order to significantly improve the security posture of the State. Proper configuration and deployment of networking equipment, operating system software, applications, storage devices, and endpoints such as desktops, laptops, and mobile devices all contribute to the State's security posture. In this phase, the KISO will work with central IT and entity IT organizations to apply controls and to increase the maturity of IT processes that affect information security across the State.

In addition to collaboration on basic IT technologies, the implementation of security technologies and architectures from Phase 2 will take dedicated effort by both KISO and entity IT staff. This phase will work to implement these technologies within entity infrastructures while minimizing adverse impacts to end-users. It will be imperative, in this and future interactions, that those security personnel establish solid functional working relationships throughout the State.

In addition to putting in place much needed collaboration in the State, the KISO will work to fully implement controls 6-10, and to begin implementation of controls 16-20. At the end of Phase 3, the target minimum CSC score will be 30.

5.4 PHASE 4: Increase Maturity of Security Capabilities

With the Strategic Plan substantially in place, Phase 4 will involve further increasing the efficiency of the processes and organization established in earlier phases. Additionally, the KISO will work to fully implement controls 11-20. This will bring the overall CSC score to 40, and provide for a comprehensive security program that can competently address security events as they arise in the State.

5.5 Sustainability Timeline

To a certainty it is difficult to give a defined date of completion of the various phases. Many elements drive the successful completion of each phase. In general, Phase 1 will take approximately 18 months to complete full staffing and implement various processes to ensure a secure environment. Phase 2, to some degree is currently underway; however, more knowledge and insight will be gained as Phase 1 is implemented. This synergy will gain speed over the course of the development of Phase 1 and will result in better selection of technology to deploy. Current enterprise solutions that are underway will remain as they have been vetted to be superior products and have a high rate of acceptance in industry. Other solutions deployed may have to be replaced to provide better enterprise technical solutions to solve larger enterprise issues. Phase 2 should be completed within 24 to 30 months of initiation of the formation of the Kansas Information Security Office. Phase 3 collaboration efforts are ongoing, however, widespread collaboration can only be realized when Security standards are universally adopted and implemented throughout the enterprise. We anticipate a fully functional collaboration effort by the end of month 36-42. Phase 4 and increased maturity will be ongoing with the formation of the KISO. It is anticipate that peak maturity when weighed against cost should be obtained at around month 42 and onward.

The initial funding efforts will be greatest in month 13 through 42, after which there will be a gradual reduction of cost to achieve an ongoing required funding effort to maintain an increased maturity model. It has been reported that of this date, 48 states have some form of formal funding for security; Kansas is one of the two states that does not formally fund security. It will require a commitment by the State to ensure that we do not think that a one-time funding of security is all that is required. It must be ongoing and sustained effort by the State as a whole; security cannot be an afterthought or considered an option in today's world. In fact, information security should be considered the enabler for business. Without security, business cannot function to the degree that is required either by regulation, law, or by the citizens whose information we, the State, have been entrusted to protect.

Kansas residents deserve our best effort, our due diligence and continued effort in protecting their information. Security provides many functions for the State; we have recently become involved in the detection of fraud for unemployment insurance and implementing security measures designed to assist in the detection of fraud. Implementing enterprise solutions that, when fully implemented with Kansas Department of Labor, can be used elsewhere by all agencies and branches of government to standardize and more effectively report on Governance, Risk and Compliance for the State of Kansas. This, when married to various enterprise solutions for security, will give the agencies a view of risk associated with the business practices, allowing for the necessary changes and correction to become more efficient with the utilization of their resources. These accomplishments come about through the utilization of Security technology, processes and practices with business units. Utilization of security to assist in the solving of challenges is one of the greatest values that enterprise security brings to the organization.

6 CURRENT VIEW OF KANSAS INFORMATION SECURITY OFFICE

6.1 Summary

The findings below are based on the results from a survey sent to State Agencies to help determine what we currently spend on Information Security. While our goal is to consolidate and provide information security for all state government, the following information is focused primarily on the Executive Branch and should provide adequate information to address additional resources needed to attain an acceptable level of information security.

	Agencies
109	Total number of agencies, boards and commissions
26	Number of responding agencies
23.85%	Percentage of responding agencies
	Employees
20,286	Total number of employees
11,905	Total number of employees assigned to responding agencies
58.69%	Percentage of total employees

The numbers above represent the sample used to estimate what is currently spent annually on information security. It is important to emphasize that although the number of responding agencies is low, the agencies included represent the vast majority of the population of the Executive Branch. While these numbers are not all inclusive, it does indicate how inadequate our current expenditures are.

	Security Professionals by title and job
12	Number of employees performing Information Security functions that hold an Information Security position
24,960	Number of hours performing security functions per year
$798,720.00	Total annual spend using an estimated median wage value of $29 per hour

As the label indicates, these employees are those that perform information security functions on a daily basis. What is not represented in these numbers is that virtually all do more than just information security.

	IT Professionals by title and job
122	Number of employees performing Information Security functions that do not hold an Information Security position
64,340	Number of hours performing security functions per year
$1,865,848.40	Total annual spend using an estimated median wage value of $27 per hour

The bulk of employees represented in these numbers are IT consultants and technicians. While some of these talented employees may have some security experience, the vast majorities do not and consequently the security related tasks they perform are substandard, if not wrong. Further, the workload of these employees has increased dramatically over the past several years and to expect them to provide adequate attention to information security only compounds the problem.

Also in these numbers are numerous entry level employees that perform user administration functions such as adding and disabling users, and resetting passwords. As we begin the process of improving information security for the state this function must change; Identity Management is a primary key to this plan and these functions are part of that process – with a small team of skilled security professionals

this will make a significant improvement. The future of Identity management is a role based security design incorporating many security features such as multi-factor authentication and management of security tokens, which requires a higher level skill set than those currently performing these functions.

Most important in these numbers is the number of hours spent performing security functions per year. This number is significant because it demonstrates that there are unfortunately 30 mostly unqualified FTEs providing substandard information security as reported from both state and federal auditors on numerous consecutive audits. If these functions were executed by a team of qualified security professionals the outcome could be significantly improved, as would the security of the state; information security levels would increase, and overburdened IT professionals could refocus their attention on their primary responsibilities.

	Software
$1,087,922.35	Total annual spend on security software and maintenance per year
	Hardware
$1,890,514.60	Total spend on security hardware (currently owned)
	Professional Services
$684,280.00	Total annual spend on professional services for security

These services include Security Operation Center (SOC) activities, staff augmentation, consulting, and external testing.

	Totals
$3,752,490.75	Total annual security spend less hardware (includes staff, software and professional services)
$4,382,662.28	Total security spend including 3 year refresh plan for hardware
$216.04	Total security spend per employee

Note: The largest executive branch agencies are included; e.g. extrapolating across remaining agencies would dramatically skew results

Detailed information for KISO Five Year Funding is provided as a supplement to this document.

7 FUTURE VIEW OF CYBER SECURITY KANSAS

The implementation of this plan will establish the ability for the State of Kansas to protect the information to which the State has been entrusted by both the residents of Kansas and the partners with whom the State of Kansas does business.

Business will benefit from the protection of their data that they have provided to the State. The federal government partners of the State also will benefit in the ability of the State to protect taxpayer's information, medical information, and personal identifiable information maintained by the State.

Corporate and small business will benefit in that not only does this program provide for the protection of information, it also is a key enabler for business by ensuring applications and business processes operate in a consistent and stable environment. By providing this stable, secure operating environment and incorporating an identity access management system, many functions that today are not possible, not available or not secure become possible, available and secure.

The regents and university systems will benefit in a cooperative working relationship with the State to provide greater opportunities for development of applications for State organizations by the partnership. State university systems over time will be able to provide the State with highly trained resources to assist in future development of State Cyber-Security.

The design of the future Kansas Information Security Office also allows for assistance to counties and local government organizations throughout the State of Kansas. Cities, townships and local governments are saddled with some of the same federal requirements that we the State have. The Kansas Information Security Office will provide needed resources and assistance as well as help to ensure that the local communities can and do operate to an acceptable level. This assistance will also apply to grades K-12 and, with the assistance through partnerships with Regents Institutions, provide one of the most robust security programs in the nation. Often overlooked, grades K-12 struggle to meet the challenges of maintaining compliance with Federal regulations for the protection of student information. By partnering with Regents institutions to provide assistance to school districts it will help reduce overall costs associated with outsourcing and more importantly promote a safer environment for our most vulnerable K-12 citizens while at the same time developing many new and creative educational opportunities for higher education.

By contracting on an enterprise scale and by ensuring that contracts for the State government are also available to local governments, costs for Kansas residents will be reduced.

It is anticipated that within the first three years the table in section 3.2 will show that the majority of entities will have all controls implemented, as well as audit findings over the last six years should be dramatically reduced if not fully remediated.

This plan must be updated and refreshed as technology, processes, and procedures change and new standards are put into place. This will allow the State to adopt new technologies, and new standards to ensure the future success of the security program for the State. Our goal is to provide a high level of security for the tax payers and the State of Kansas while remaining cognizant of the cost. This plan we believe provides an approach to achieve a very robust and comprehensive security program.

