



State of Minnesota
Minnesota State Colleges and Universities

Information Security Assessment Program

2008 NASCIO Recognition Award Nomination
Category 9: Information Security and Privacy

EXECUTIVE SUMMARY

Minnesota State Colleges and Universities (the system) is comprised of 32 colleges and universities located throughout Minnesota. Information technology personnel are distributed across the system, including a CIO at each college and university. Each institution's CIO and IT personnel select and manage the local technology services and operations for their institution. The Office of the Chancellor (the system office) provides systemwide network connectivity and infrastructure between the institutions, as well as enterprise application and data services.

In 2007, the Information Security Office within the system office, together with the Center for Strategic Information Technology and Security at Metropolitan State University, developed the Information Security Assessment Program (ISAP). This program provided a baseline of the current security practices and posture for protecting private data of the students, alumni, staff and faculty at each of the institutions and identified common issues that can be addressed through systemwide initiatives.

The ISAP was developed and designed with the following goals:

- Establish benchmarks for the security posture of each institution and the system;
- Identify gaps and opportunities in current institution and system security programs;
- Create a clear set of information security objectives and milestones;
- Prioritize security initiatives to focus effective use of budget, time and staff;
- Identify and leverage existing knowledge, solutions and practices across the system;
- Increase information security awareness across the system; and
- Aggregate assessment results from all institutions to identify systemwide initiatives.

The ISAP is based on existing security industry standards and best practices and delivered a consistent method to measure the current level and effectiveness of information security practices at every institution. The ISAP was developed and facilitated by information security professionals, providing awareness and expertise to institutional staff (business units and IT) through dialogue and the ISAP interview process. By working with business units at each institution, the process identified current needs and business practices, and compared them to the services and procedures of the IT department. This process culminated in presenting individualized reports to the CIO at each institution providing project recommendations to improve information security and IT processes.

By collaborating with on-campus IT staff and business users, the ISAP established a deeper awareness of campus operational constraints, established a stronger working relationship between campus and system staff, identified institutions that excelled in specific areas of security, increased awareness of best practices, and fostered a security mindset. The project has already had an impact on campus and systemwide initiatives and will continue to guide the development of future information security projects.

Ultimately, the program has benefited every institution, the system, and all individuals within the system by identifying opportunities to improve current controls protected private data, and to mitigate risks to an acceptable level.

DESCRIPTION OF BUSINESS PROBLEM AND SOLUTION

Business Problem

The protection of private data about students, alumni, staff and faculty members is vital to the reputation and integrity of the individual, the institutions and the system as a whole.

Additionally, state and federal laws and regulations require the protection of private data. These laws and regulations include the Family Educational Rights and Privacy Act (FERPA), the Minnesota Government Data Practices Act (MGDPA) and the Payment Card Industry Data Security Standards (PCI DSS). The MGDPA defines private data as: *"any government data which is classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic."*

Understanding the current safeguards and data handling practices that protect private information maintained by both the institutions and the system office required a comprehensive systemwide assessment of information security. The ISAP was developed to provide a baseline of the current information security practices and posture for protecting private data at each of the system institutions, as well as to identify common issues that can be addressed through systemwide initiatives.

Our Solution

The Office of the Chancellor's Information Security Office, together with the Center for Strategic Information Technology and Security at Metropolitan State University, developed an Information Security Assessment Program to provide a point-in-time snapshot of information security, data handling and protection practices across the system. The ISAP was not intended to be an audit or provide all-inclusive compliance checklists. The ISAP sought to establish an accurate baseline of each institution by working on-site with the local IT staff to assess their current practices and collaborate with them to identify security projects and set priorities to improve the security posture of the institution and the system.

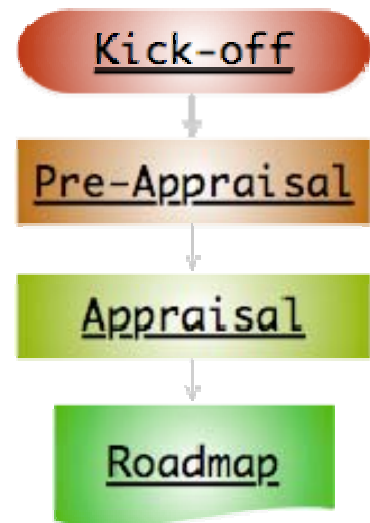
A core team, with support from senior management, finalized the process and documentation that was utilized for each assessment. Incorporating state and federal laws, industry regulations, system policies and best practices, this process was structured into three primary areas of focus: organization, controls and governance; policies, processes and procedures; and technical implementation of organizational and policy controls.



Between March and May 2007, the core team piloted the program with three institutions of different sizes to verify that the process was structured enough to be repeatable, yet adaptable enough that it could be used in vastly differing technology environments. The most important lesson learned from the pilot phase was the time required to complete an assessment. As a result, the team collaborated with faculty and IT staff from computer studies and computer science departments (field assessors) from six institutions across the system to participate in the assessments. All 32 colleges and universities and the system office had an assessment completed between June 2007 and June 2008.

The process for the assessment conducted at each institution included the following components:

1. An on-site kick-off meeting introduced the ISAP and provided an overview of the process and goals.
2. A pre-appraisal document was completed by each institution's CIO and IT staff, providing the assessment team with an overview of the institution's current IT and operational environment prior to going on-site for the appraisal.
3. An assessment team conducted the appraisal on-site. An *Appraisal Work Plan* document contained the details from these on-site activities.
4. The roadmap was the deliverable report presented to each CIO at an exit meeting, providing an opportunity for discussion, additional details, and an opportunity to correct any errors and acknowledge the resolution of any observations made between the appraisal and exit meeting.



Over the course of two to four days, the team of field assessors through interviews conducted the appraisal portion of the ISAP process with business units (the data owners) and IT staff members (the data custodians). These interviews provided an understanding of the business departments' needs and data handling practices, which were compared with the current controls implemented by IT. If there were any gaps observed between the business departments' data handling practices and the technical safeguards implemented by IT, the finding was noted for inclusion in the roadmap.

The appraisal also included an in-depth look at the institution's technical infrastructure and security management practices for networks, the perimeter, servers, workstations, and user access controls. While working with on-campus IT staff, each field assessor emphasized the concept of defense in depth, structuring the ideal protection of private data in multiple layers and avoiding single points of failure.

The process culminated in individualized roadmaps for each institution, providing recommendations to improve information security and IT processes. These observations and recommendations were categorized and prioritized, then presented to the institution's CIO. Recommendations did not include specific products or solutions; they instead provided high-level direction, allowing each institution the freedom to pursue its optimal solution.

SIGNIFICANCE TO THE OPERATION OF THE SYSTEM

In governing technology and information security in this distributed and autonomous system of colleges and universities, three of the biggest challenges encountered systemwide were:

- An IT focus on operations versus information security
- Limited resources to develop information security skills and expertise
- Delayed participation in systemwide projects

Institutions are responsible for information security at their college or university; however, as we move to online learning, our students expect all of their applications and data to be accessible every day, around the clock. This demand for high availability of IT applications and systems leaves little room for downtime, and is critical to day-to-day operations of the institution, consuming the vast majority of the IT staff's workload. As a result, each institution's IT staff have limited time and resources for information security. College and university IT staff did not have the capacity to conduct an assessment like the ISAP. By serving as a resource to institution IT staff and minimizing the demand on their time, the ISAP was able to provide them with insight into their information security posture.

The operational focus and constraints of campus IT staff, mentioned above, has constrained the resources to develop information security expertise and skills at the institution level. College and university IT staff have traditionally implemented security based on personal knowledge and past experience, but there has been little consistency between institutions. The ISAP was developed and facilitated by information security professionals, providing awareness and expertise to institutional staff (business units and IT) through dialogue and the ISAP interview process. The roadmap results from the ISAP provided institutions with information and details around security best practices. The program also highlighted the need for training in information security, and as a result, a security training program is currently being developed for delivery in the next fiscal year.

Historically, getting full participation from all institutions for systemwide projects has been a challenge. The autonomy of the colleges and universities has, by design, allowed each institution the freedom to conduct local operations and pursue solutions that best meet their needs. The ISAP was designed and developed to provide value to every institution, large or small, with a goal of 100 percent participation. By using a structured approach that included on-site face-to-face meetings and assessment activities, the ISAP met that goal. The program added value to the institution regardless of size, and it fostered relationships with the institution's business and IT staff that did not previously exist in other enterprise projects. As a result, there has already been increased participation in several other system security projects.

BENEFITS OF THE PROGRAM

The ISAP was designed with specific goals and stakeholders in mind that would benefit from the program. The success of the ISAP was dependent on meeting the program goals and delivering value to these stakeholders.

Ultimately, the program has benefited every institution, the system, and all individuals within the system by identifying opportunities to improve current controls around the protection of private data, and to mitigate risks to an acceptable level.

Benefits to the Institutions

The ISAP provided institution CIOs with an understanding of their current information security posture. This program has provided them with a comprehensive look at the business and data handling practices at their institution, and an assessment of the technical controls that protect the private data entrusted to the institution. The roadmap results provided CIOs with guidance on information security risks that are present in their environment, and recommendations to mitigate those risks to an acceptable level. Specifically, it:

- Produced a measurable method for determining information security effectiveness for institutions.
- Identified gaps and opportunities in the current security program.
- Prioritized initiatives to create focus and ensure effective use of budget, time and staff.
- Defined a clear set of objectives and milestones.
- Increased information security awareness on campuses.

Benefits to the system

The ISAP was designed to provide system senior leadership with a timely report of aggregate results from all 32 institutions. These results will assist senior leadership by better informing their decisions and investments in appropriately mitigating risks to an acceptable level for the system as a whole. The program has:

- Created benchmarks and identified effectiveness of current technologies.
- Developed a reporting methodology for long-term security trends.
- Produced a baseline for the system within one year.
- Increased information security awareness across the system.
- Collaborated and shared knowledge and experience in implementing security controls across the system.

Benefits to the Students, Alumni, Staff, and Faculty

The Minnesota State Colleges and Universities system of distinct and collaborative institutions offers higher education that meets the personal and career goals of a wide range of individual learners, enhances the quality of life for all Minnesotans, and sustains vibrant economies throughout the state. As an educational entity, protection of the private data of our students,

alumni, staff, and faculty is paramount to preserving the reputation and integrity of the individual, the institutions and the system as a whole. Through an involved and proactive approach to information security, the ISAP has increased the protection of private data entrusted to the system, helping fulfill its mission. It:

- Proactively identifies opportunities to improve private data protection.
- Enhances systemwide knowledge in security.
- Mitigates risks to an acceptable level.