



Enterprise Information Security Business Risk Assessment

Information Security and Privacy

May 11, 2009

State of Oregon

<http://www.oregon.gov/DAS/EISPD/ESO>

Executive Summary

In 2007 the Enterprise Information Security Business Risk Assessment was launched and focused on identifying key business functions and areas of information security concerns from agency executive management. The risk assessment is performed based on input from agency leaders regarding the key business functions and lines of business within each agency. The risk assessment is based primarily on structured individual and group interviews as well as observation and enquiry, corroborated by supporting documentation and other sources considered necessary. The security posture is then defined by identifying the information security level of both business risks and maturity for identified divisions/business units.

For the purposes of the Information Security Business Risk Assessment, information is defined as meaningful information that is used to enable critical business functions, and includes both electronic and paper information. Each agency's information security risk is assessed based on the threats to confidentiality, integrity, and availability of information.

The approach leverages the security domains and objectives for ISO 17799 (for 2008 ISO 27001 and 27002 were used) as the foundation for identifying information security business risks for an agency. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management framework was used in identifying initial risk categories for the agencies. Once risks were identified and prioritized, the maturity of the processes for the ISO control domains were measured using the maturity level guidelines from the Carnegie Mellon's Capability Maturity Model Integration© (CMMI) model.

The Information Security Business Risk Assessment is performed annually with twelve (12) base agencies that represent a cross section of state government and a rotation of two (2) additional agencies for a two-year period. The twelve (12) base agencies receive individual reports and the individual reports are aggregated to provide a statewide report. The results of the statewide report contribute to the enterprise information security Key Performance Measures.

The results of the 2007 assessment highlighted five theme areas that the State should focus on; Business Continuity Management, Information Owner and Classification, Incident Management, Security Awareness and Training, and Security of equipment on and off the State premises. The results of the 2008 assessment indicated significant improvement in the five aforementioned areas most notably in the specifics of security policies, security awareness and training, asset management and portable media security.

Description of the problem and solution

In the 2005 Legislative Session, Oregon Revised Statute (ORS) 182.122 passed designating the Department of Administrative Services (DAS) as the “single point of accountability” for information security at the State. In support of this mandate, the Enterprise Security Office (ESO) instituted a security strategy wherein DAS would work collaboratively with State agencies to ensure the State’s security posture is at an acceptable level.

A risk assessment serves as the first step in creating a foundation to measure the state of an organization’s information security position. DAS conducts assessments to determine the security posture of the State and to implement initiatives to reduce identified risks. DAS contracted with KPMG to conduct an initial Information Security Business Risk Assessment focused on information security business risks and not exclusively technology issues.

The risk assessment process leverages industry framework and standards and is intended to evaluate risk exposure and control domain maturity level. The State has used the results to foster a strategy to improve information risk management. For purposes of the Information Security Business Risk Assessment information is defined as meaningful information that is used to enable critical business functions, and includes both electronic and paper information.

The assessment in 2007 included thirteen (13) agencies which were selected based on size, location(s) and interactions with business partners, and types of services offered in an effort to achieve a representative cross-section of state agencies. Two additional agencies were added for the 2008 assessment and one agency of the original thirteen (13) chose not to participate.

To provide greater focus, the eleven (11) ISO security domains were grouped in the three (3) categories; Security Governance and Compliance, Security Infrastructure and Environment, and Tactical Security Operations. This model provides a common language for all to view and manage information security activities. It provides a framework for measuring and monitoring performance and integrating better management practices, which may more easily align to traditional organizational structures and responsibilities.

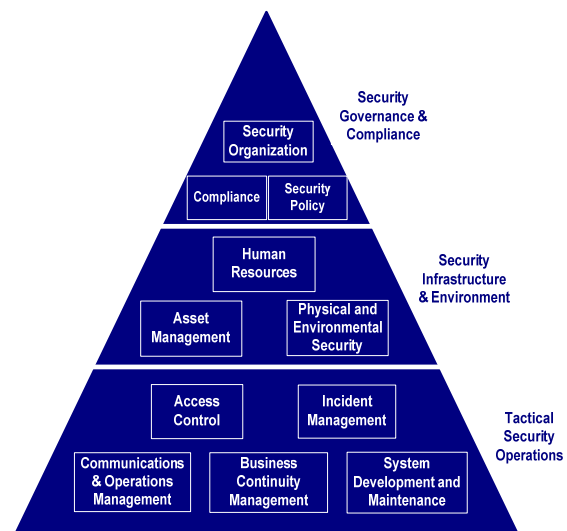


Diagram 1

The risk assessment consists of four (4) phases: Discovery, Assessment, Risk Summary and Analysis, and Reporting.

During the discovery phase meetings were held with agency executive management to identify key information security concerns as well as key business functions. Additionally, specific departments critical to the success of the agency were identified.

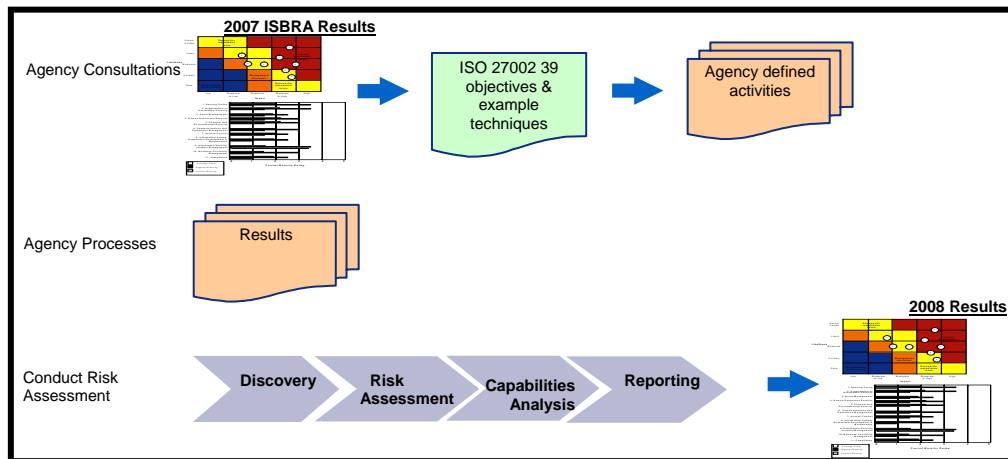


Diagram 2

The assessment phase identified information assets critical to the success of the key business functions and security risks to those information assets. During this phase the focus was on processes improvement where existing controls could be improved.

Normalization and analysis of the information gathered during the discovery and assessment phase occurred during the risk summary and analysis phase. The identified risks were plotted based on the most appropriate ISO control domain. The level of maturity for the controls applied were analyzed using the CMMI as a guideline. These risk elements were plotted on a Risk Heat Map identifying remediation priorities.

Beyond the addition of two (2) new agencies to the assessment process in 2008, an effort to add performance measurement was undertaken. This was introduced as a basic requirement for an agency to understand its current information security status and to determine the level of management and controls to be implemented. Each agency must decide on the "right level" based on analysis of its information assets, information security risks, appropriate maturity level, and the overall cost and resource availability to obtain that level.

The maturity model utilized provides a process which is qualitative based on the following attributes:

- Awareness and communication;
- Policies, plans, and procedures;
- Roles and responsibilities;
- Skills and expertise; and
- Tools, products, goal setting and measurement.

The maturity model evaluates the maturity of the attributes not necessarily the effectiveness and coverage of the controls. It is designed to provide context to assist the agency in determining the extent of resources, effort, formality, and sophistication, which are or should be deployed to meet business, regulatory and control objectives. The model is used as a tool to assist each agency to define the level of maturity that provides the best fit for their business processes.

Significance to the improvement of the operation of government

The initialization of the Information Security Business Risk Assessment was the first step in meeting the requirements of ORS 182.122 which designated the State of Oregon Department of Administrative Services (DAS) as the “single point of accountability” for information security at the State. While ORS 182.122 is very specific to “information systems” the DAS and the ESO recognize the need to address all forms of information that agencies are responsible for collecting, maintaining, protecting and at some point dispositioning for disposal. The Information Security Business Risk Assessment is one method to assist agencies in prioritizing the use of resources and providing a secure operational environment for all information.

While the overall movement on the maturity model appears relatively modest, the efforts of each agency have been significant. Several agencies made substantial strides in areas where their critical business functions demanded a change in processes. One agency created an Information Security Officer position, hired a qualified person and established an office within the agency to support the position and their efforts.

Not all agencies have the resources to undertake such major organizational changes and therefore sought creative ways to accomplish similar outcomes. One agency reassessed the use of an existing cross-functional team and changed their focus to evaluate various security related issues and develop agency wide solutions to those problems. Another agency used an existing vacancy and modified the position description to include security related tasks as the primary duties.

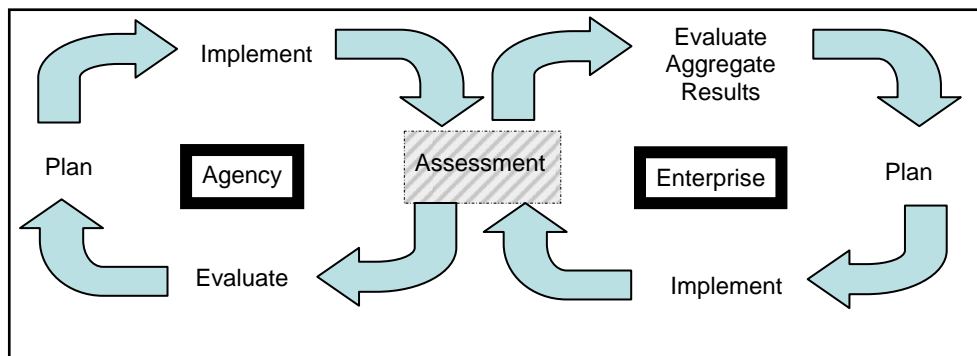


Diagram 3¹

¹ The results of each agency assessment assist them in determining areas to focus on for improvement. The aggregate results inform the enterprise of issues affecting agencies so statewide plans can be adjusted and therefore more responsive.

As part of its enterprise program, the DAS ESO continues to hold communications forums to familiarize agencies with new statewide policies. Some of these policies evolved from risks identified during the assessments and the forums provide an opportunity to educate agencies on appropriate controls. DAS ESO also sponsors an Information Security Council comprised of agency business and security representatives. An agenda item at each monthly meeting focuses on one of the eleven ISO 27002 domains. The council provides the DAS ESO with input and feedback on security topics to address at the enterprise level. The Enterprise Information Security Advisory Board, comprised of agency directors provides input on strategic enterprise information security. They also champion information security, as a critical business issue with their peers in state government.

Benefit of the Project

At an enterprise level, this initiative provides a recognized, standard methodology to measure improvement in the state’s security posture. Agencies involved in the program have demonstrated an increased awareness of the relationship of information assets, (data and technologies) to their business processes. Each agency has implemented changes in their organization to better protect their information and has committed to taking steps to ensure incremental improvement in the future. All participating agencies have acknowledged this initiative as adding tangible value to their information security efforts. Several non-participating agencies have requested an opportunity to be involved so they can implement a structured approach to reducing their risk exposure.

Capability Maturity Model Integration²

Maturity Level	Maturity Description
Initial (Maturity Level 1)	<ul style="list-style-type: none"> • Success based on <u>individual</u> heroics and competence. • Non-repeatable success and abandon process during crisis.
Managed (Maturity Level 2)	<ul style="list-style-type: none"> • Commitment from Stakeholders • Work products are reviewed with the stakeholders • Satisfy the specified requirement, objectives and standards • Process is managed according to documented plans
Defined (Maturity Level 3)	<ul style="list-style-type: none"> • Establishes process objectives • Process are well characterized and understood • Organization’s standards are needs based • Standards improve overtime
Quantitatively Managed (Maturity Level 4)	<ul style="list-style-type: none"> • Establish quantitative objectives to manage processes. • Detailed measure of process performance are collected and analyzed
Optimizing (Maturity Level 5)	<ul style="list-style-type: none"> • Continual improvement based on qualitative measurements • Ability to respond to changes and opportunities is enhanced by finding ways to accelerate and shared learning.

Table 1

² Carnegie Mellon

Non-Financial Return on Investment

Through the active involvement of the agencies and the intensified analysis of their security posture the agencies now have a heightened awareness throughout their management structure and across their lines of business. These efforts serve as a mechanism to reduce the cost associated with a security breach, whether it is due to loss of data or application downtime impacting access by users. The agencies also have the ability to reduce the threat of fines through actively meeting and monitoring their regulatory compliance requirements. Finally, the process reduces costs associated with unauthorized individuals gaining access to state information assets through enhanced management controls.

The Enterprise Security Office and the twelve (12) original agencies will meet over the next six (6) months to develop performance measures that can be implemented uniformly across the agencies to inform the enterprise key performance measure. The measurement techniques will strive to recognize the varying level of maturity and business functions of the different agencies to keep the measure both reliable and consistent.

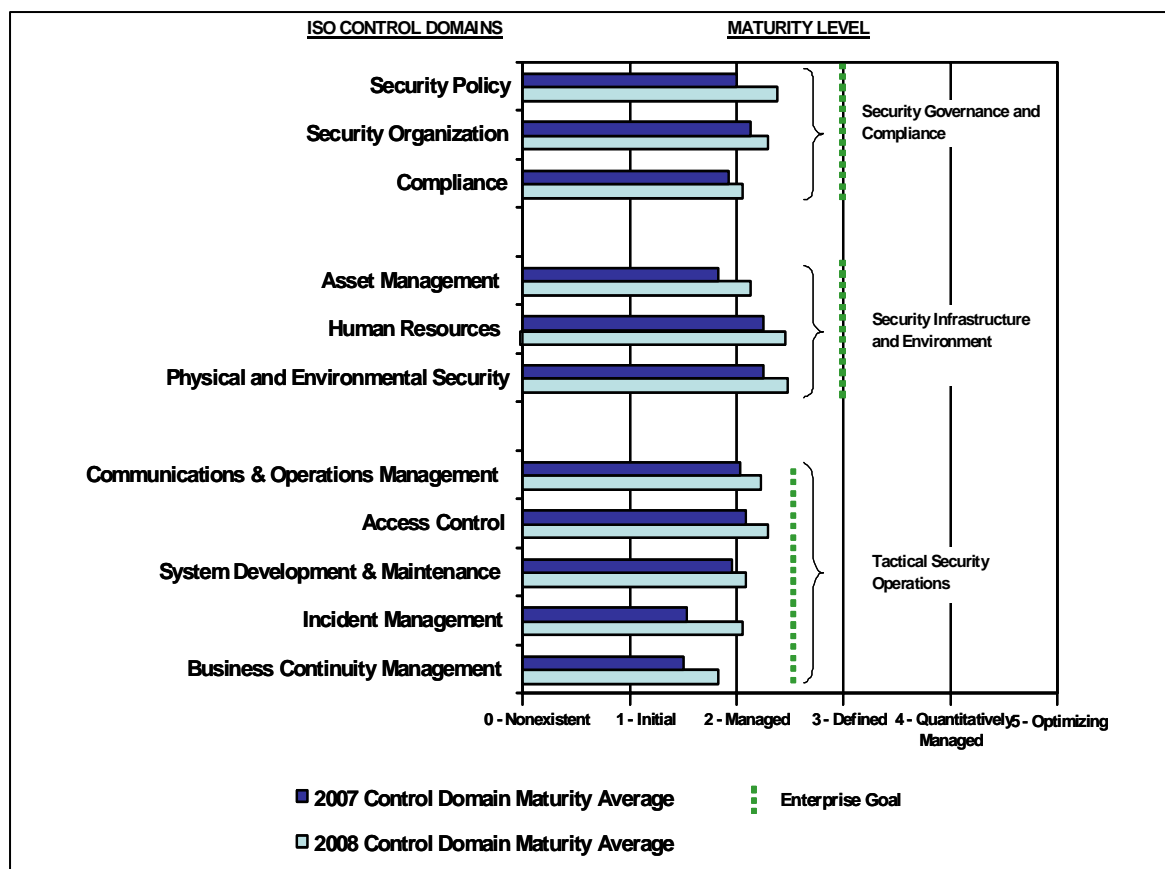


Diagram 4