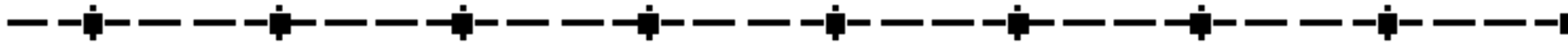




Department of Human Services

Information Security Office



Business Plan

2005-2007

Table of Contents

EXECUTIVE SUMMARY

Purpose of the Business Plan	3
Situational Analysis	3
Mission	7
Vision.....	7
Key Objectives.....	7
Programs, Services & Initiatives	8
Business Structure.....	9
Business Strategy.....	11
Operations.....	12

EXECUTIVE SUMMARY

ISO 2005-07 Business Plan

1. Purpose of the Business Plan

A formal business plan is just as important for an established office, irrespective of its size, as it is for startup. It serves four critical functions as follows:

- Helps management clarify, focus and research their business's or project's development and prospects.
- Provides a considered and logical framework within which an office/program can develop and pursue business strategies over the next biennium.
- Serves as a basis for discussion with third parties such as shareholders, partners other agencies, etc.
- Offers a benchmark against which actual performance can be measured and reviewed.

2. Situational Analysis

1. *State of the State*

DHS has established a formal Information Security Office (ISO) and Program.

- The ISO team is comprised of ten staff members (certified security experts, professional project & program managers, and administrative staff).

2. *History*

The Information Security Office (ISO) and the Information Security Program were established through policy in December 2002. The DHS Privacy Program was established in 2003 and is included within the ISO. The ISO organizational structure was established in April 2004. The ISO was partially funded in the 2003-05 Biennium with the base budget being established in the April 2004 DHS Agency Rebalance Plan. Staffing was a combination of permanent, Limited Duration and Job

ISO 2005-07 Business Plan

Rotational positions. Full funding is being established through the development of a 2005-07 Policy Option Package (POP# 123).

3. *Driving Forces*

3a. Security Rule

HIPAA established rules by which entities must adhere to when creating, processing, transmitting, and storing Electronic Protected Health Information (EPHI). The Rule (known collectively as the Security Rule) has broad applicability for all of DHS' business processes, applications, systems, networks, and procedures.

- Oregon DHS met the April 21 2005 compliance date.
- By the Security Rule Compliance date, DHS established an Information Security Compliance Program that monitors and maintains security policies and business processes.
- A full-time Security Officer position was established and resides in the DHS ISO.
- Six security policies were implemented.
- DHS employees were informed using a video awareness program (SECURE IT).
- The development of "Privacy/Security DHS and You" was implemented for new employees.
- Privacy/Security Incident Response Program was implemented

3b. Privacy Rule

The HIPAA Federal Privacy Rule provided the first comprehensive Federal protection for the privacy of health information.

- Oregon DHS met the April 14, 2003 compliance date.
- A full-time Privacy Officer position was established and resides in the DHS ISO.
- Nine privacy policies were implemented.

ISO 2005-07 Business Plan

- A “Notice of Privacy Practices” was provided to all clients and participants in DHS programs.
- Clients and participants have been informed of the additional client rights permitted under HIPAA.
- Privacy policy training was presented to 97% of the nearly 10,000-member DHS workforce prior to the compliance date.

3c. Formal Audits

DHS has undergone several formal audits between 1997 and 2005, including Secretary of State, SACWIS, IRS, SSA and Internal Audits. Audits revealed that DHS information security is poor to non-existent; severely lacking in controls and safeguards in many areas. The audits also indicated major deficiencies regarding systems access, network controls, application controls, file access controls, and separation of duties for DHS staff. With the implementation of HIPAA Security Rule;

- ISO has developed an Information Security Compliance Plan that addresses the HIPAA Security Rule compliance elements and formal audit recommendations
- Most areas of concern have been addressed (some projects and initiatives have been started that will address these areas).

4. Risk Analysis

DHS does not have a formal information security risk analysis (RA) process in place (Risk analysis, Business Impact Analysis, Risk Mitigation Planning) outside of what might be done as part of a project.

- Business Continuity Planning requires a formal risk analysis process
- ISO has begun a form of RA in response to previous audits

ISO 2005-07 Business Plan

- Audits results have been mapped to HIPAA, ISO17799, and National Institute for Standards and Technology and proposed DHS Information Security Policies and Standards.
- ISO intends to use audit results to develop mitigation strategies.
- ISO has implemented a Privacy and Security Incident Response Program (PSIRP) to respond to incidents.

ISO's approach to information security consultancy is to apply risk management practices to both products (deliverables) and business and technical processes, providing business units with options to resolve, transfer or assume the risk.

- Ensures that confidentiality, integrity and availability issues are equally and formally addressed.
- Ensures deliverables address DHS policies and standards, federal and state laws, industry standards.
- Threats and vulnerabilities are properly addressed so that DHS environments are stable and available.

ISO 2005-07 Business Plan

3. Mission

A mission statement sets out the purpose and guides the activities of large and complex organizations.

The ISO supports the departments mission of “Assisting people to become independent, healthy and safe” by:

Providing leadership and services that assist DHS in securing the confidentiality, integrity and availability of its information assets

4. Vision

Facilitate a culture that integrates privacy and security into processes and technology.

5. Key Objectives (3)

- Align agency information security and privacy policies, procedures and controls with federal and state regulations, industry best practices and contractual obligations. (Policies and Standards Objective)
- Apply a level of security to information resources commensurate to its value to the organization and sufficient to contain risk to an acceptable level. (Risk Management Objective)
- Program / service delivery and ISO staff will become jointly responsible for successful implementation of privacy and information security measures within DHS programs and service processes. (Ownership and Accountability Objective)

ISO 2005-07 Business Plan

6. Programs, Services & Initiatives that support

ISO goals and strategies

1. Programs:

a. Security Program

- Privacy
- Policies and Procedures
- Risk Assessment/Evaluation/Management
- Exception Assessments
- Audits
- Information Exchange
- Secure Email

b. E-Authenticate

- Role-Based Access Control (RBAC)

c. Privacy Program

d. Awareness & Education (A&E)

e. Privacy and Security Incident Response

Program (PSIRP)

2. Services:

a. Consult

- Vulnerability/Assessment
- MMIS
- Enterprise –wide projects
- Application Review
- System Application Development

b. Coordinate

- Business and Information Systems improvements
- Information Security Incident Response

3. Initiatives:

- Federal HIPAA Business Continuity Planning Phase (BCP)
- Federal HIPAA Security Compliance Phase II
- Federal HIPAA Role-Based Access Control (RBAC)
- MMIS
- Enterprise-wide initiatives (E-Authenticate, Data Ctr. etc)

ISO 2005-07 Business Plan

7. Business Structure

Information Security is about risk management through assessment and planning. Information Security programs provide the framework and the processes for DHS to identify threats, vulnerabilities, and consequences. The processes and activities used in our programs provide a means for DHS to identify and classify information assets and take the appropriate steps to understand the risk to the department.

Through its programs, the ISO strives to create a privacy and security program that is driven by business risk management. It will assist the department in dealing with change and complexity within the department and enterprise wide. The ISO focuses on processes and procedures that make up a good security program such as;

- *Risk and assessment* - - A systematic, comprehensive approach to information security that includes all business aspects of the department Includes security drivers (ie HIPAA, Audits etc.) and their impact in the development of security programs
Feedback mechanisms that make it possible to measure the success of our program
- *Policies and Procedures* that are current, revised often to their relevancy of current business practices and technology
- *Awareness and Education* – an awareness program that targets all employees, volunteers, partners and contracts

ISO 2005-07 Business Plan

8. Business Strategy

FINAL ISO Business Plan/Idrive/ Leadeship/business plan/pmccary/ 1-16-06

ISO 2005-07 Business Plan

1. Customers

The ISO recognizes the following as its customer; Clients, Managers, DHS Employees, Volunteers, Partners, Contractors and DAS.

Go to Publications & Reports on the ISO web page for the latest Communication, Education & Awareness Plan:

<http://www.oregon.gov/DHS/admin/infosec/>

2. ISO Goals

The ISO overarching goals are broad in the sense that they support the DHS goals and include elements that support the Governor's

Principles: (see the Governor's principles: <http://egov.oregon.gov/Gov/future.shtml>)

- To enhance the knowledge level of information security for staff, volunteers, partners and contracts
- To improve audit and risk assessment results
- To decrease the amount of information security incidents
- To ensure the protection of the departments confidential information (assets)
- To provide statewide leadership/coordination

3. Strategic Plan

The strategic plan contains the strategies to achieve the ISO goals. The relationship of these strategies to ISO services, programs and projects is shown:

- To enhance the knowledge level of information security for staff, volunteers, partners and contractors
- To improve audit and risk assessment results
- To decrease the amount of information security incidents
- To ensure the protection of the departments confidential information (assets)

ISO 2005-07 Business Plan

- To provide statewide leadership/coordination

9. Operations

Operational and Risk Management Elements in Support of all ISO Programs and Project Initiatives:

- Policies and Procedures
- Communication Plan
- Awareness & Education Program
- Risk Management

1. *Staffing*

All staff will have job descriptions, a career and training history file, and a record of employee reviews. ISO staff consists of certified security experts, professional project & program managers, and administrative staff. Permanent funding was established, in a 2005-07 Policy Option Package (POP# 123).

1a. In addition to program staff, ISO needs the involvement and participation of DHS units to ensure the success of the ISO Business Plan.

- **Cabinet** – To approve and support Department-wide information security initiatives, provide decision-making on security risks, issues and strategies that promotes the confidentiality, integrity and availability of DHS information assets.
- **Sponsorship** - The Information Security Office Sponsor's serve as Ambassador's and Advisor's, providing leadership, guidance and direction on program and project status, issues and decisions.
- **Cluster Executive Management** – To provide feedback and expertise on their cluster information security business needs, barriers, risks and recommended strategies for successful department-wide project implementation.

ISO 2005-07 Business Plan

- **Program Managers** – To personally participate or allow their staff to participate on information security project teams to ensure their program area is represented, provide leadership in project implementation activities and promote information security best practices.
- **Internal Audit** - To provide expertise and recommendations to ISO regarding information security risks and issues.
- **OIS** - Provide leadership, expertise and recommendations to ISO regarding technology improvement and practices.

ISO 2005-07 Business Plan

2. ISO Operational Plan to Secure the DHS Environment

ISO's Role in DHS:

- Information Security and Privacy Consulting and Guidance to DHS Clusters
- Information Security and Privacy Monitoring
- Information Security and Privacy Incident Response
- Coordination of Information Security and Privacy Business Processes and Information Systems Improvements

A. ISO has a strategic plan to support its Objectives and Strategies

3. Financial Plan

A. 2005-07 Biennium

The ISO submitted a 2005-07 POP#123 to fund the completion of the implementation of security measures necessary to meet compliance with HIPAA Security Rule and achieve essential information security performance thresholds specified by Department of Administrative Service's Cyber Security Program. The components of the POP are as follows:

1. HIPAA Security Rule Compliance Plan Phase 2 – Security Access Control Implementation Project
2. Cyber Security Program
3. Business Continuity Planning

ISO 2005-07 Business Plan

Information Security Office Business Plan Approved

Name: _____ Date: _____

Kyle E. Miller, ISO Information Security Officer