Executive Summary

The University of Alaska is the only public institution of higher learning in the State of Alaska. It is comprised of separately accredited Universities in Fairbanks (UAF), Anchorage (UAA), and Juneau (UAS), as well as 14 remote campuses throughout the state. UA's system administration is conducted by a separate administrative unit, UA Statewide. Together, these 4 Major Administrative Units (MAU's) support more than 32,000 students throughout the state.

Information resources for UA Statewide and UA Fairbanks are managed by the Office of Information Technology (OIT). OIT's mission is to provide University consumers with the technology, tools, and resources to support and enhance learning, research, and outreach for Alaskans. OIT is organized by four primary service areas; Applications Services, Infrastructure Technology Services, Technology Oversight Services, and User Services.

Contract Objective

CH2M HILL was contracted to conduct an Information Technology Security Review. The security review comprised of three primary objectives:

1. Evaluate the University's business practices and procedures. Make recommendations for improving business processes.
2. Ensure adequate controls are in place to protect Confidentiality, Integrity, and Availability.
3. Identify vulnerabilities, determine their risks, and make recommendations to resolve or mitigate those risks.

From June 22nd to August 21st, 2007 CH2M HILL conducted a security review of administrative, technical, and physical controls. Areas reviewed included Data Management Policies and Practices, the IT Security Program, Networks, Identity Management Directory, Authentication and Authorization Services, Database, Application Development/Support, Windows and Unix Servers, Desktop Support, Data Center Operations, Help Desk, and Telephony.

Each area was assessed against a set of 42 common control objectives. Each control objective was mapped to regulatory requirements, best practices, and guidelines, including the International Organization for Standards (ISO) 17799, Control Objectives for IT and Related Technology (COBIT) 4.0, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Federal Financial Institutions Examination Council (FFIEC) guidelines, and the Payment Card Industry Data Security Standards (PCI DSS). While compliance to these requirements will vary depending on the data, processes, and risks to the University, they provide a baseline of best-practice information and guidelines for assessing, implementing, monitoring, and auditing the University's security program.

To achieve the most comprehensive view of the environment, vulnerability scanning was performed from both external and internal locations using two different commercial tools (Qualys and Rapid7), and several open source security tools used by system administrators and auditors (such as NMAP, CIS Benchmarks, MBSA, etc.). In addition to the vulnerability scanning activities, CH2M HILL performed background research, policy and procedure analysis, and conducted interviews to assess the current state of security controls that would otherwise not have been identified through technical

testing alone. The interviews also assisted the team in developing recommendations to improve security controls.

This report serves as a summary of the review. During the course of this review, potential issues identified as "critical" (such as any high risk vulnerability discovered during network scans) were escalated to UAF personnel to facilitate immediate remediation, along with being reported herein. Technical reports and raw findings have been provided to OIT staff in separate appendices.

Summary of Findings

CH2M HILL assessed the current security posture of the University's Administrative, Technical, and Physical controls. The following summaries provide an executive overview of our findings. Each area is addressed in greater detail later in this report. Raw technical data and detailed remediation advice has been submitted to OIT staff separately.

Common Controls

Of the 42 control objectives reviewed, 10 areas were assessed as meeting the control objective (Green), 31 areas partially met the objective (Yellow), and 1 area did not meet the objective (Red).

10 areas were assessed as meeting control objectives. The network administrators and managers have implemented several security practices to oversee segregation of duties, limit access creep, maintain appropriate service levels, and conduct regular system maintenance.

The majority of control objectives (31) were partially met, but were missing one or more elements in order to achieve full compliance. Several of these objectives could be corrected by conducting a comprehensive risk assessment, establishing additional security policies, and creating a business continuity plan based on a formal business impact analysis. These programs are not "quick fixes" and require long term commitments to ensure that they are sustainable once they are implemented.

Media Disposition and Sanitization were assessed as high risk, due to the lack of an information classification program, sensitive data inventories, and destruction standards for all media which may contain sensitive information (such as USB drives, removable hard drives, PDA's, etc.). Without a comprehensive inventory of sensitive data stores and acceptable storage devices, the University may not be able to detect if sensitive data is compromised or lost, or to minimize the potential impact of a data breach.

The table below provides a high level summary of the control objectives and our findings.

Domain Ref	Control Objective #	Control Objective	Meets Control Objective
1	Control Environment and Oversight		
	1.1	Planning and Oversight	▲
	1.2	Identify and Manage Risk	▲
	1.3	Create and Manage Policy	▲
	1.4	Develop Issue Specific Policies	▲
	1.5	Information Classification and Handling	▲
	1.6	Manage Employees and Contractors	▲
	1.7	Manage Vendors and Acquisitions	▲
2	Logical and Physical Access Control		
	2.1	Identify Sensitive Physical Areas	▲
	2.2	Protect Sensitive Physical Areas	▲
	2.3	Manage Visitors to Sensitive Areas	●
	2.4	Identify and Implement Logical Security Domains	▲
	2.5	Secure Identification, Authentication and Authorization	▲
	2.6	Secure User Accounts	▲
	2.7	Establish and Manage Access	▲
	2.8	Segregation of Duties	●
	2.9	Remote Access	●
3	Product and Services Lifecycles		
	3.1	Security Development Lifecycle	▲
	3.2	Change Management	▲
	3.3	Configuration Management	●
	3.4	Applications Security	▲
	3.5	Media Disposition and Handling	●
	3.6	Manage Cryptography	▲
	3.7	Manage Outsourced Services	▲
	3.8	Patch Management	●
	3.9	Malicious Code and Anti-Virus Management	●
	3.10	Network Security	▲
	3.11	Wireless Network Security	▲
	3.12	Maintenance	●
	3.13	Maintain Documentation	▲
	3.14	Inventory Management	▲
	3.15	Project Management	●
4	Monitoring and Event Management		
	4.1	Establish Audit Trails	▲
	4.2	Ensure Actionable Event Information	▲
	4.3	Security of Event Logs	▲
	4.4	Monitoring Operations	▲
	4.5	Managing Security Incidents	▲
5	Quality and Continuity of Service		
	5.1	Business Continuity	▲
	5.2	Data Back-up and Process Recovery	●
	5.3	Environmental Controls	▲
	5.4	Service Monitoring	●
6	Program Audit, Testing, and Certification		
	6.1	Independent Audit and Accreditation	▲
	6.2	Security Program Testing	▲

Vulnerability Scans

CH2M HILL conducted vulnerability scans from the Internet and from a trusted location on the UAF campus. Approximately 50 unique vulnerabilities were discovered from the Internet, and 130 unique vulnerabilities were discovered from internal scans. The majority of vulnerabilities identified were rated as low or medium risk. Some vulnerabilities were identified with High, Critical, or Urgent risks, although they appear to be on a limited number of hosts. The number of vulnerabilities identified at UAF was less than the average number of vulnerabilities for other Universities of the same size and complexity as UAF, indicating that patch management is being proactively addressed.

Configuration Testing

CH2M HILL reviewed 10 systems, and compared running configurations against security best practice guidelines. On Average, 41% of the configurations reviewed were not aligned with best practices. Several of the areas reviewed indicated that best practice guidance is understood, but may not be fully adhered to due to system limitations or business justification (password length is 6 characters instead of the recommended 8 characters). In some instances, the setting implemented by the University exceeded or met the best practice guidelines, but did not exactly match the best practice setting (i.e. the warning banner was customized for UAF and did not match the exact verbiage of the baseline).

COBIT Maturity Model

The COBIT maturity model is a ranking of an organization's maturity from a scale of 1 -5. Based on our review, we believe that the University would be ranked as a "Level 2" rating for the entire enterprise in accordance with the metrics defined by COBIT (which are summarized in the box below). Some departments and processes are more mature, and have elements that could be measured as a Level 3, Level 4, or Level 5, but the University as a whole is at a Level 2 rating. For organizations using COBIT metrics, all strive to achieve "Level 5," a fully integrated, comprehensive, information security program.

The University has implemented several controls (technical, physical, and administrative) to protect its information assets. In some cases, the University has implemented very strong controls (such as ZUAUSR documentation), and in other areas controls are not adequate (such as data classification and sensitive data inventories). In order to increase the organizations maturity within the COBIT framework, additional procedures should be defined (such as establishing consistent reporting criteria in all areas of information security), and independents tests should be established to validate the adequacy of the controls. Corrective action should be taken in areas where controls are not being followed or are not adequately designed. Ultimately, detailed metrics and consistent reports will provide management with a measure of the effectiveness of the controls, justifying resources and priorities.

COBIT Maturity Model

Level 1	Level 2	Level 3	Level 4	Level 5
Control objective documented in a security policy	Security controls documented as procedures ☑ **Current Level of the University**	Procedures have been implemented	Procedures and security controls are tested and reviewed	Procedures and security controls are fully integrated into a comprehensive program
Control Design Adequacy →		**Control Effectiveness** →		