EXCELSIOR HILL
UNIVERSITY

CYBERSECURITY RISK ASSESSMENT

April 29th, 2025

Table of Contents

Executive Summary

The following is an assessment of Excelsior Hill University's Information Security policy conducted on April 29th, 2025.

To determine findings, I examined the 108 controls listed in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) Version 1.1 against Excelsior Hill University's Information Security policy.

I evaluated each risk (ranked one through seven) using the Maturity Level Scores from the Nationwide Cybersecurity Review (NCSR).

These controls aid in identifying and ranking risks, as well as matching policy, business goals, and technology to manage those risks.

While the organization scored highly, as nearly every score was at least a five -- ensuring the organization at the very least had formally documented policies in place for most controls -- there are a few areas that could be of concern.

The key findings uncovered were:

- **No clear documentation regarding the organization's role in critical infrastructure:** This could result in a failure to respond effectively during an emergency.

- **No formal policy regarding the organization's role in the industry sector:** Lack of clearly communicated roles and responsibilities could lead to inconsistent operations and accountability.

- **No process in place to stay informed about the latest threats:** This could increase the organization's vulnerability to new attacks.

To strengthen its protection, Excelsior Hill University should clearly define and communicate its supply chain role and permissions, document its place in critical infrastructure with regular updates for compliance, and routinely monitor verified sources and forums to assess current and emerging threats.

Objective and Scope

Evaluating the efficiency of Excelsior Hill University's Information and Security policy was the focus of this assessment. Its policies concerning access control software, hardware, on campus devices, cloud security, etc. were all addressed during this assessment. Each control was ranked one through seven by the Maturity Level, measuring the overall strength and impact of the organization's policy.

Methodology

To achieve the objectives of this assessment, I utilized controls found directly in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) Version 1.1.

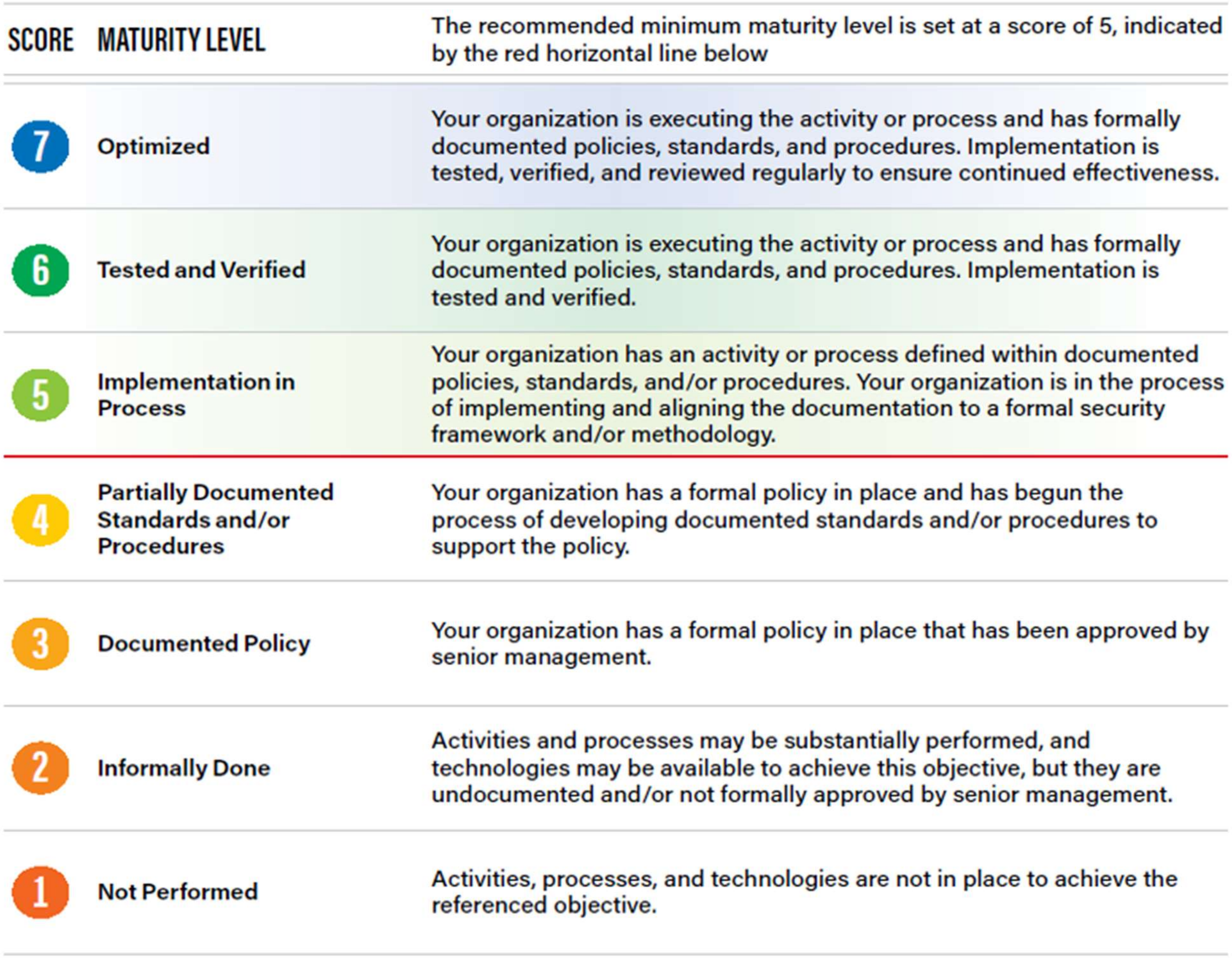
I calculated Overall Maturity Level Scores using the official chart from the Nationwide Cybersecurity Review (NCSR).

The controls are split into five categories: Identify, Protect, Detect, Respond, Recover.

Each control group was then given an overall score also ranked from 1-7.

I compiled this data directly from the latest version of Excelsior Hill University's Information Security Policy.

A detailed breakdown of the Maturity Levels is as follows:



SCORE	MATURITY LEVEL	The recommended minimum maturity level is set at a score of 5, indicated by the red horizontal line below
7	Optimized	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4	Partially Documented Standards and/or Procedures	Your organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
3	Documented Policy	Your organization has a formal policy in place that has been approved by senior management.
2	Informally Done	Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by senior management.
1	Not Performed	Activities, processes, and technologies are not in place to achieve the referenced objective.

Findings

Excelsior Hill University has done a great job with its security, covering nearly all its bases. However, here are a few minor gaps in its policies that could be better addressed.

The following is a detailed breakdown of the control groups outlined in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) Version 1.1., their subsets, Overall Maturity Level Score, and Evaluation.

Identify (ID) -- Understand the organization's environment to manage cybersecurity risk.

Subsets:

- ID.AM (Asset Management): Inventory of hardware, software, and systems.
- ID.BE (Business Environment): Organization's mission, role, and dependencies.
- ID.GV (Governance): Policies, legal requirements, and risk management processes.
- ID.RA (Risk Assessment): Risk identification and threat modeling.
- ID.RM (Risk Management Strategy): Risk tolerance and prioritization.
- ID.SC (Supply Chain Management): Organization's policies with third-party partners and systems.

Overall Maturity Level Score: 5

Evaluation: Implementation In Process. Excelsior Hill University scored the lowest here, due to its need for better documentation and communication for its Business Environment and Risk Assessment policies.

Control ID.BE-1 states ***the organization's role in the supply chain is identified and communicated***. I found no clear evidence of this control.

One of the major risks of not clearly communicating its role in the supply chain is lack of accountability. If something were to go awry, not knowing who had access to what, why, and when could send the organization reeling.

Control ID.BE-2 states ***the organization's place in critical infrastructure and its industry sector is identified and communicated.*** Again, I found no direct evidence of the following control being implemented.

Without knowledge of the organization's role in critical infrastructure and the industry sector, there could be gaps in contingency planning, the wrong security strategy may be implanted, and the organization's reputation as well as its services could be severely impacted.

ID.RA-2 states ***cyber threat intelligence and vulnerability information is received from information sharing forums and sources.*** I found no trace of this control being enforced.

Not being up to date on the latest cyber threats could literally and figuratively leave the organization in the dark. Staying up to date at least gives the organization a fighting chance at whatever threat it faces.

Protect (PR) -- Safeguard critical infrastructure and limit or contain the impact of cybersecurity events.

Subsets:

- PR.AC (Identify Management and Access Control): Limit access to authorized users.
- PR.AT (Awareness and Training): Ensures users are aware of risks and trained.PR.DS (Data Security): Protect data integrity and confidentiality.
- PR.IP (Information Protection Processes): Maintain and improve protection mechanisms
- PR.MA (Maintenance): Perform system maintenance with proper controls.
- PR.PT (Protective Technology): Implement and manage proactive systems.

Overall Maturity Level Score: 6

Evaluation: Tested and Verified. Excelsior Hill University has many strong, foundational security controls for safeguarding its systems and data, including access controls, awareness training, and its information protection processes.

Detect (DE) -- Identify the occurrence of cybersecurity events.

Subsets:

- DE.AE (Anomalies and Events): Detect unusual activity.
- DE.CM (Security Continuous Monitoring): Monitor information systems to detect threats.
- DE.DP (Detection Processes): Maintain and test detection processes.

Overall Maturity Level Score: 6

Evaluation: Tested and Verified. While some of these controls may not be applied consistently, Excelsior Hill University has the capabilities to recognize cybersecurity threats in real time and could enhance these capabilities further if needed.

Respond (RS) -- Take action regarding a detected cybersecurity incident.

Subsets:

- RS.RP (Response Planning): Develop and test incident response plans.
- RS.CO (Communications): Coordinate internal and external communications.
- RS.AN (Analysis): Analyze incidents to ensure effective response.
- RS.MI (Mitigation): Contain and eradicate incidents.
- RS.IM (Improvements): Review and improve response efforts.

Overall Maturity Level Score: 6

Evaluation: Tested and Verified. Excelsior Hill University's incident response policy is impressive. Isolating the contaminated information system or system component, eradicating the information from the contaminated information system or component, and identifying other information systems or system components that may have been subsequently contaminated are just a few of its highlights.

Recover (RC) -- Restore services and capabilities after an incident.

Subsets:

- RC.RP (Recovery Planning): Develop and implement recovery plans.
- RC.IM (Improvements): Update recovery strategies based on lessons learned.
- RC.CO (Communications): Communicate recovery efforts to stakeholders.

Overall Maturity Level Score: 6

Evaluation: Tested and Verified. Excelsior Hill University updates its Contingency Planning Policy at least every three years and its Procedures annually.

Summary of the Control Group, Overall Maturity Level Score, and Control Evaluation:

Control Group Name and ID	Overall Maturity Level Score	Control Evaluation
Identify (ID)	5	Implementation In Process
Protect (PR)	6	Tested and Verified
Detect (DE)	6	Tested and Verified
Respond (RS)	6	Tested and Verified
Recover (RC)	6	Tested and Verified

Recommendations

Excelsior Hill University can't be praised enough for its high level of security, protecting its staff and clientele in equal measures, however, it would benefit greatly from implementing the following recommendations:

- Cleary communicate the organization's role and permissions in the supply chain and its importance. (pg. 6, control ID.BE-1)
- Draft a formal document stating the organization's place in the critical infrastructure and industry sector should be in place and updated as often as necessary to meet compliance. (pg. 6, control ID.BE-2)
- Routinely monitor verified sources and information sharing forums to assess current and emerging threats. (pg. 6, control ID.RA-2)

Though there were only three areas to improve in, lack of closing those security gaps could lead to a major headache in the future.

As the cyber war rages on, businesses can no longer afford to play it safe.

With respect to adhering to your mission and not derailing the business to a standstill, I hope you will take my risk assessment to task and implement any changes should you find them necessary.

If you have any questions, I'm available at the following address: jkinfluker@gmail.com

Thank you,

J. Fluker

GRC Analyst