VIRGINIA TECH

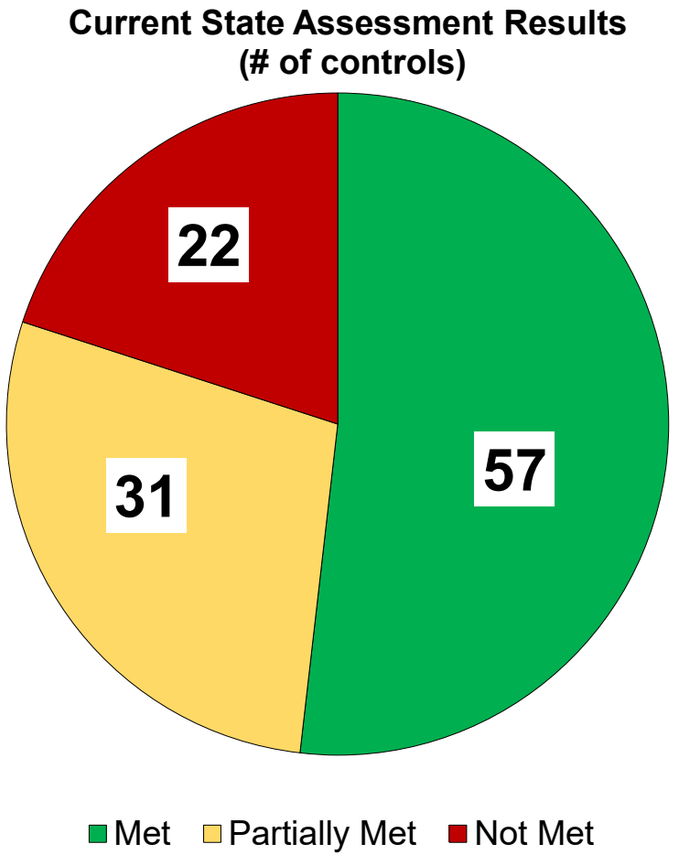
Deloitte.

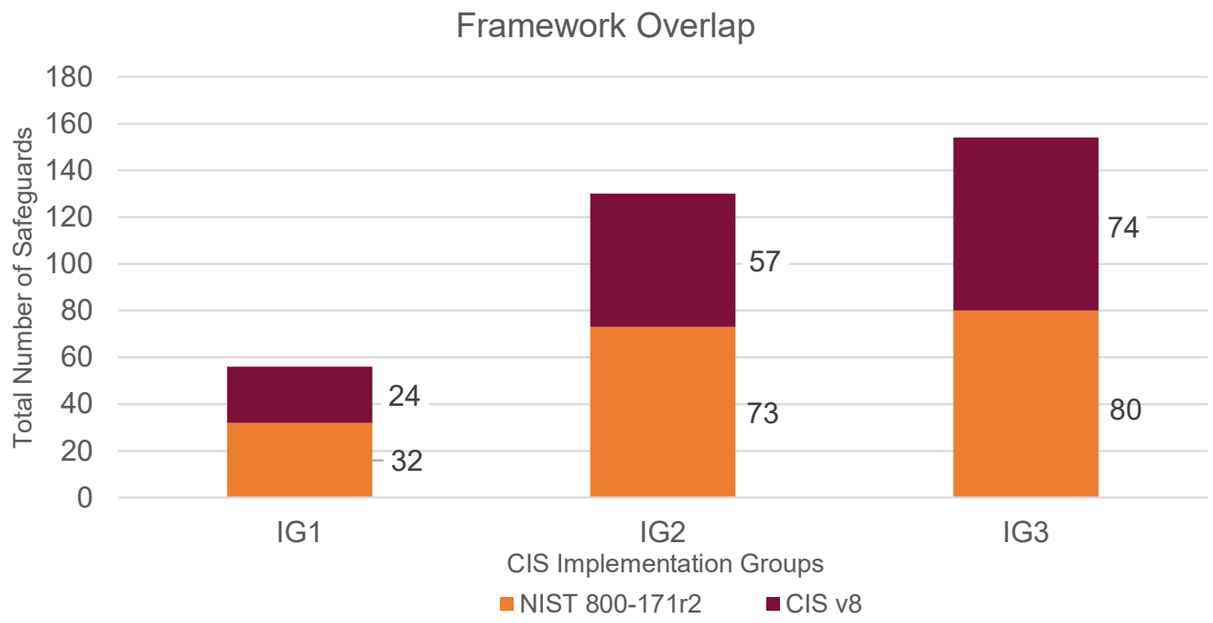
Cybersecurity Review

Future State Design: Cybersecurity Areas of Improvement | December 2021

BREAKDOWN OF ASSESSMENT CONTROLS

The below infographics illustrate the current state assessment results (left) and how CIS v8 works in tandem with NIST 800-171 to improve cybersecurity practices. NIST 800-171 has been adapted as a maturity framework to identify additional cybersecurity growth opportunities given Virginia Tech currently utilizes CIS v8 as its compliance standard. NIST 800-171 was used to create insight into the U.S. Department of Education's recommendation to higher institutions to learn more about the framework and to reduce the risk surrounding Controlled Unclassified Information (CUI), Financial Information Systems, and Student Information Systems.

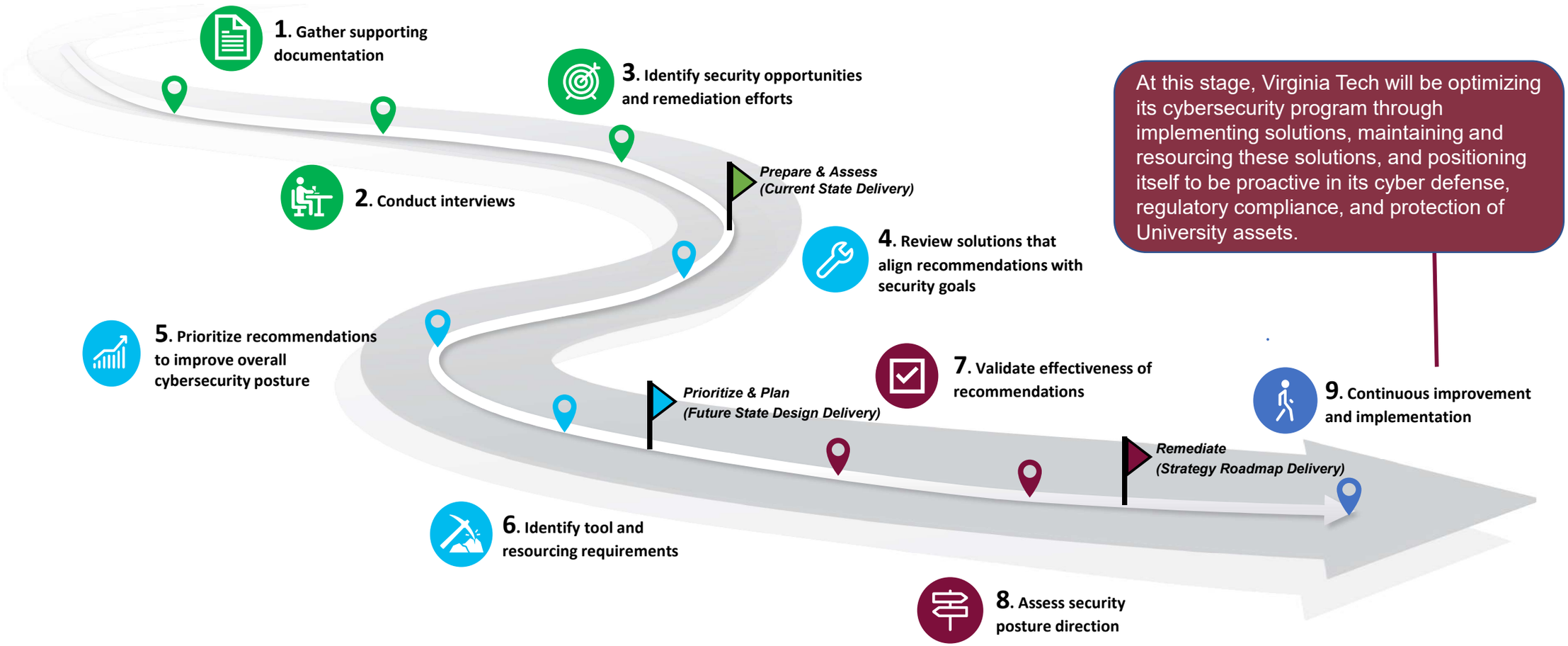




While Virginia Tech has adopted CIS v8, IG1 as its current security standard, NIST 800-171r2 presents an opportunity to further improve depth of security. The two frameworks overlap by more than 50% across implementation groups (IG1 - 57%, IG2 - 56%, and IG3 - 52%) and NIST provides additional coverage and granularity into physical security, access controls, identity and authentication, and system and communication protection.

STRATEGIC APPROACH

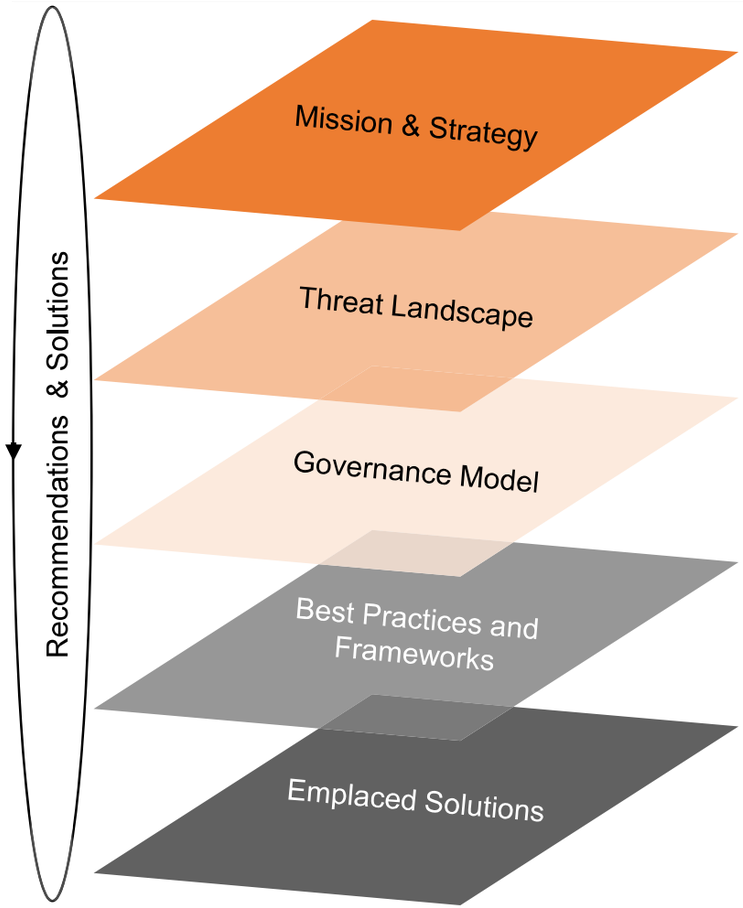
Detailed below is a high-level strategic approach across three phases; Prepare & Assess, Prioritize & Plan, and Remediate for Virginia Tech's current state, taking into consideration the target/future state and goals of the University. The current phase is Prioritize & Plan. As recommendations are developed, risk to the university is the prime consideration to drive priority and implementation order.



FUTURE STATE TACTICAL APPROACH

The Virginia Tech environment was assessed for initial findings across the University cybersecurity environment. The table and diagram below outline how recommendations are developed, identified, and prioritized, as well as what influences the approach.

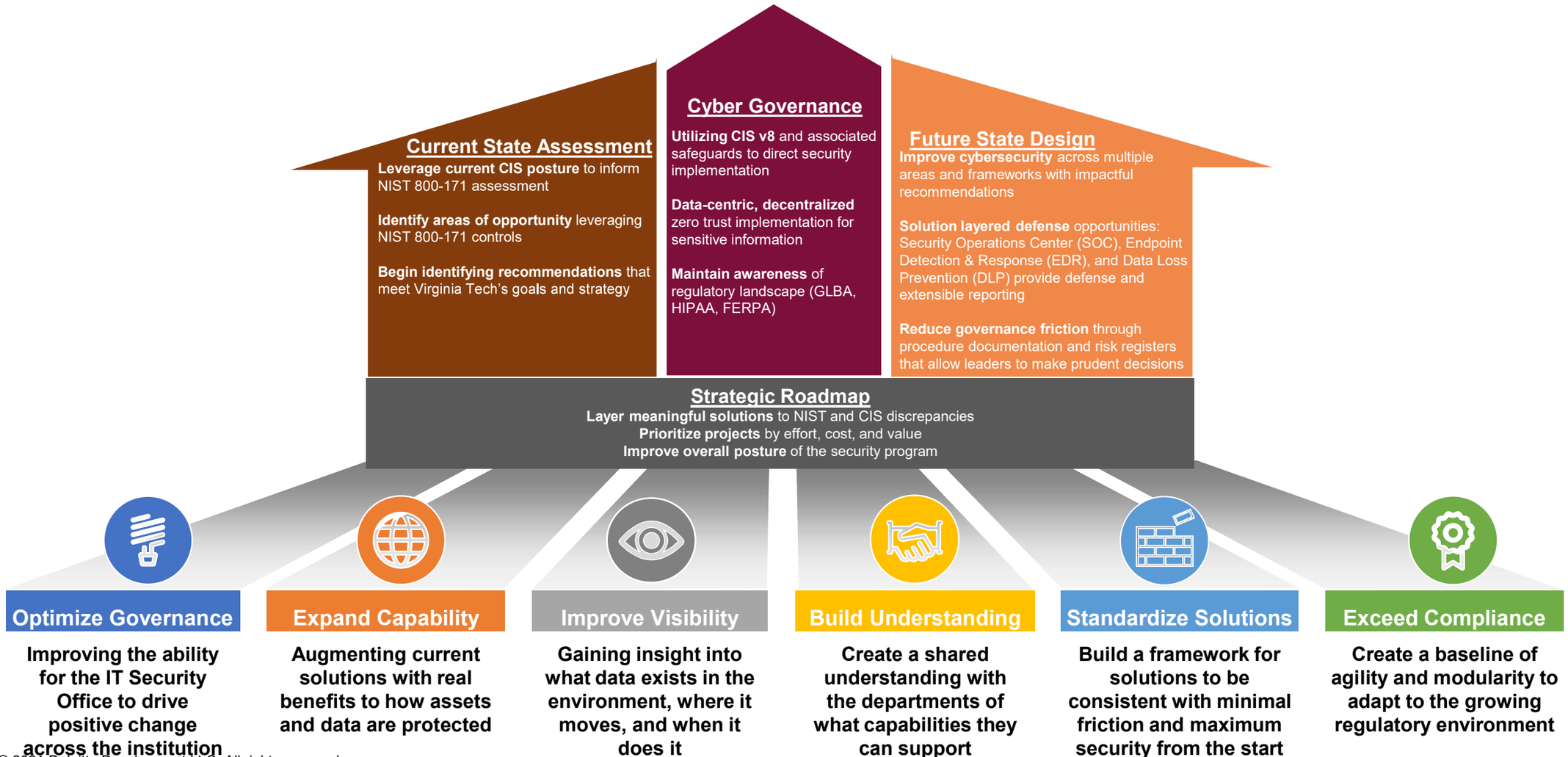
Priority and Hierarchy of Recommendation Development



Overall Mission and Cybersecurity Strategy	• Focus on building recommendations to provide value to Virginia Tech extending beyond assessments and frameworks • **Identify opportunities to improve capabilities** based on themes found in the Current State assessment • Assess which process and technology solutions best support Virginia Tech's overall mission from a student, faculty, staff, and research perspective based on a NIST 800-171 assessment
Threat Landscape	• Identify tools, processes, approaches, and industry leading practices that would enable Virginia Tech to reduce risk in the University • **Build recommendations around the future of cybersecurity** practices to provide a level of agility and adaptability into the system by design
Governance Model	• Investigate IT security influence in Virginia Tech and how roles and responsibilities are organized • Define the University IT Operating Model to clarify roles and responsibilities, identify reporting lines, and assess effectiveness of collaboration as it pertains to security functions • Review IT security policies and standards to identify delegated responsibilities and authority across the University • Conduct interviews to gain understanding of existing security practices • **Identify breaks or improvement opportunities** for accountability of risk
Best Practices and Frameworks	• Map NIST Special Publication (SP) 800-171 rev. 2 Controls to CIS v8 safeguards to find areas of overlap, taking a blended approach to exceed minimum-security requirements • Assess the direction of the University relative to its peers and identify a path from IG1 to IG2 and beyond • Enable direct recommendations for specific controls that emphasize value and ease of implementation
Emplaced Solutions	• Recommend solutions with an understanding of solutions already in place at Virginia Tech • **Leverage diverse solutions for greater transformation** and identify those which need replacement

CREATING LONG TERM IMPACT

The diagram below represents the intent of the recommendations with foundational 'pillars' across governance, capability, visibility, understanding, standardization, and compliance as they relate to Virginia Tech's cybersecurity posture. Recommendations and themes are also weighed against confidentiality, integrity, and availability to protect data from disclosure, modification, and destruction pursuant to University and regulatory objectives.



RECOMMENDATION #1: ELEVATE VIRGINIA TECH TO CIS IG2

Expanding the compliance of the university to CIS IG2 and IG3 would significantly reduce risk by protecting assets (people, systems, data) from threat actors with a layered defense strategy while also increasing uniformity of control application across the University. This approach also blends frameworks and increases crossover between CIS and similar security frameworks.

Requirements

Focus Area	Remarks
People	The addition of FTEs or 3rd party personnel would reduce time to completion and be necessary to maintain the new posture.
Process	This recommendation is very process-heavy in its addition of safeguards and the need to add processes and procedures.
Technology	Additional technologies will need to be procured in the transition to IG2, but they can be deferred to later stages of adoption.

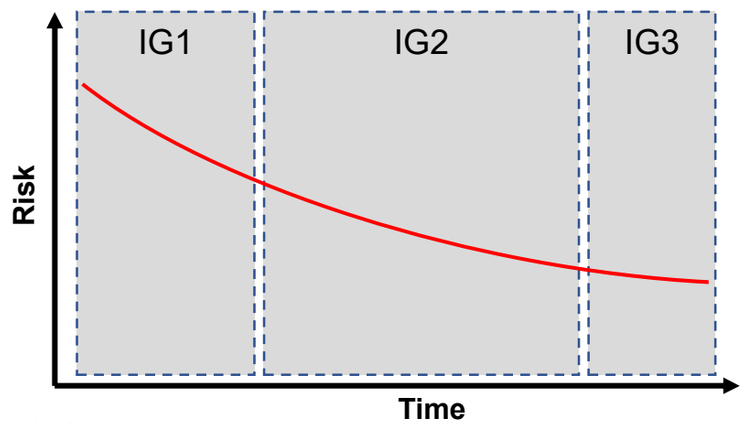
Description

CIS leverages levels of maturity called 'implementation groups,' which contains IG1 (56 safeguards), IG2 (130 safeguards), and IG3 (154 safeguards). The lowest risk to university operations and assets exists at IG3, with the caveat being that it's the most expensive (FTEs, CAPEX, OPEX) to implement properly and consistently across the University.

The current cybersecurity strategy is to increase alignment with CIS and using IG3 as the 'north star.' This has been a slow adoption and would benefit from additional personnel, tools, and resources to guide the departments.

Migrating and enforcing a standard of IG2 or better in conjunction with NIST 800-171 for systems that process sensitive (medium or high risk, according to *Virginia Tech Risk Classifications*) data would be impactful to Virginia Tech's cybersecurity posture.

Risk Profile Over Time



Implementing IG2 would reduce and manage risk across cybersecurity domains and would assist in remediating 4 of the current state themes: Governance and Standardization, Real-Time Monitoring, Data Protection, and Application Control.

RECOMMENDATION #6: DEVELOP PROCEDURE GUIDES

Where CIS v8 and the IT Security Office's minimum security standard drive the great majority of configuration and standards, they aren't prescriptive enough to enable consistency across the University. Consistency eases administrative overhead, assists in spotting security anomalies across the University, and can be enabled with the development of prescriptive documentation on 'how' to implement proper security controls. It also alleviates non-compliance stemming from resourcing issues, security skill gaps, and time restraints within challenged departments.

Requirements

Focus Area	Remarks
People	The addition of FTEs or 3rd party personnel would be necessary to develop the documents, provide training, and maintain the documents regularly.
Process	This solution is purely process-oriented and would add a layer of information to current governance practices that will aid departments in execution.
Technology	This recommendation requires minimal if any acquisition of new technologies as it can exist in a variety of forms already available to Virginia Tech.

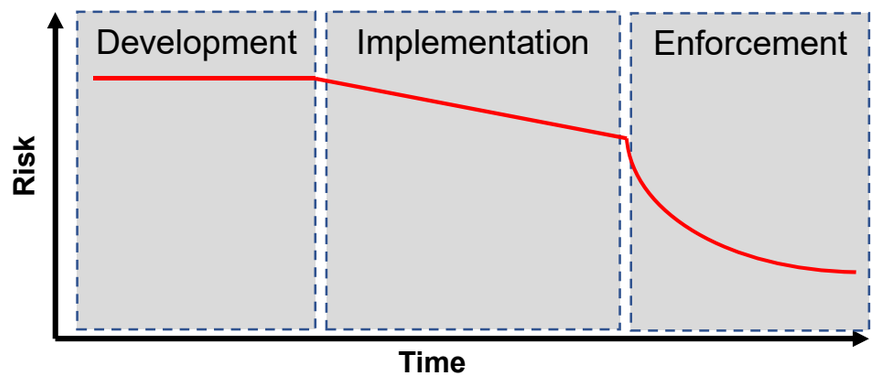
Description

The minimum security standard is an impactful step in the right direction for the decentralized governance model that the IT Security Office and Central IT leverage. One common issue that arose from interviews was a resource issue within the IT Security Office preventing the infrastructure security activities from being conducted and enforced.

Developing procedure guides is the next logical administrative step for directing exactly how to secure systems, and it has potential to alleviate the issues associated with the disconnect and staffing shortage. By clearly outlining how to implement the minimum security standards for each system, overhead on the IT Security Office can be lowered and consistency can be improved.

The risk associated with this recommendation is directly tied to how it integrates with other recommendations, current security assets, and how the departments can adopt the new procedures across implementation and enforcement phases.

Risk Profile Over Time



Developing procedure guides would reduce and manage risk across cybersecurity domains and would assist in remediating all 5 of the current state themes: Governance and Standardization, Real-Time Monitoring, Data Protection, Awareness and Training, and Application Control.

PROCESS RECOMMENDATIONS

The table below highlights additional process recommendations based on the Current State Analysis utilizing NIST 800-171 and weighing current needs in CIS v8. These recommendations can be seen as broad strokes or can satisfy outlier controls within the assessment framework.

#	Process	Impact and Risk to Virginia Tech	Requirements	Value to Virginia Tech
1	Create or leverage (from another department) personnel standards to align with NIST 800-171 controls	The current lack of documentation support for vetting faculty and staff leaves room and risk to onboard faculty and staff who may have records of divulging or damaging sensitive information	Amend or create standards-documentation to augment personnel controls	NIST has a personnel security control family that is designed to create due diligence checklists that vet all users for need-to-know and a need for access to systems; implementing these procedures could create higher confidence that users have the appropriate powers that align to their role in the University
2	Combine processes for revocation of rights (access, administrator, etc.) with HR functions such as termination, movement within the University, and change of responsibility	The current lack of synchronous rights management creates opportunities for disgruntled faculty and staff (insider threat) to exploit and damage Virginia Tech resources	Amend or create a workflow that integrates personnel actions with security activities	By integrating certain key security processes into the HR process workflows, it can alleviate overhead associated with managing users and it can prevent users from retaining unneeded rights
3	Conduct 'hands-on' assessments of department security implementation to supplement ISORA reporting	The current method of self-reporting compliance creates room for error and introduces risk that implementations of security functions are not correct, increasing the chances for Virginia Tech to suffer from breach or asset/reputation damage	This solution requires IT Security Office or external security practitioners to verify correct implementation of security standards at each department	This solution is a due diligence activity that increases fidelity of alignment with IT Security Office standards and provides greater accuracy in department reporting of security alignment
4	Maintain a milestone document to track security progress and key milestones (commonly called a plan of action and milestones, or POA&M) in compliance and maturity of the University's cybersecurity program	Without a milestone document, efforts are challenging to synchronize across workstreams and creates opportunities for crucial functions to be forgotten or incorrectly deprioritized while making accountability difficult	Multiple templates for this documentation exist through reputable sources to aid in guiding organizations to a goal within security	A milestone document provides a tool to track progress across departments toward better alignment to security standards with the possibility of being commensurate to a follow-up assessment

PROCESS RECOMMENDATIONS CONTINUED

The table below highlights additional process recommendations based on the Current State Analysis utilizing NIST 800-171 and weighing current needs in CIS v8. These recommendations can be seen as broad strokes or can satisfy outlier controls within the assessment framework.

#	Process	Impact and Risk to Virginia Tech	Requirements	Value to Virginia Tech
5	Conduct mobile code assessments through procedure documents for departments developing and utilizing mobile applications	The lack of mobile code assessments in alignment with risk to the university is not performed allowing inconsistencies in mobile code development allowing heightened risk to the university and its network	Amended standards and procedures should be drafted directing the utilization of IT Security Office for software used in the University, but this can be augmented with regular assessments as mentioned previously	A mechanism to enforce full reviews by the IT Security Office (while possibly leveraging frameworks like NIST SP 800-218, Secure Software Development Framework) that supplements the minimum security standard could reduce risk associated with application-sprawl and applications procured outside of ITPALS (if any exist)
6	Conduct tabletop exercises for additional incident response training	Current practices limit incident response training to the IT Security Office, though response should be a responsibility of every staff and faculty member. The lack of synchronization exercises delays incident response and gives threat actors more time to compromise VT assets	A training program would need to be established on a semi-annual basis to bring key stakeholders together and identify weak points in knowledge and security in the event of a disaster	Tabletop exercises serve to synchronize the incident response approach, socialize the IT Security Office methodology, and 'war game' the indicators of compromise
7	Update policies and standards with greater frequency, at least annually	The lack of annual policy and standard refresh allows for uncertainty and awareness of basic compliance, in addition to not being representative of current practices within VT and in industry best practices	Policies and standards should be living documents that receive at the very least, annual reviews and recertification to remain applicable to current practice. This would be conducted as a governance function rather than a security-specific function	This solution is a due diligence activity that increases accuracy of governance documentation while also providing a degree of adaptability for the threat landscape. Establishing a more regular cadence of review keeps governance documentation relevant to the University and the IT and security practices across the industry.
8	Charter an IT Risk Management (ITRM) Working Group	With the lack of an ITRM charter, risks are not properly vetted, and accountability is not shared across the university as it could relate to a potential business impact	This recommendation requires the charter and meeting cadence established for a working group while also including change and risk stakeholders	Risk is currently delegated to data owners, though a working group can increase active resolution of risks in the University, communicate risks to key stakeholders, and synchronize risk management efforts