Team Governance

Final Report

NAS2002: Advanced Cyber Security

A21 + A22 + A23

BACHELORS OF TECHNOLOGY

In

CSE (Cyber Security and Digital Forensics)

Submitted To:

Dr. Hemraj S. Lamakuche
Assistant Professor Grade II

SCHOOL OF COMPUTING SCIENCE ENGINEERING AND ARTIFICIAL INTELLIGENCE (SCAI)

Academic Year 2023-2024

VIT®
BHOPAL
www.vitbhopal.ac.in

Bonafide Certificate

Certified that this project report titled "Governance Function - Final Report" is the bonafide work of "Vaibhav Shrivastava (21BCY10227), Yash Garg (21BCY10032), Divyansh Choudhary (21BCY10060), Ansh H Mehta (21BCY10113), Swati (21BCY10210), Sherya Pawale (21BCY10030), Ben Tom Abey (21BCY10035), Gouri Nandana (21BCY10029), Afla (21BCY10133), Rahul kumar Suman (21BCY10130), Parth Sengar (21BCY10041), Hari Shankar (21BCY10195), Arush Chandana (21BCY10007) and Yagyarth Mishra (21BCY10034) " who carried out the project work under my supervision.

This project report was submitted on **14th May 2024.**

Supervisor

Dr. Hemraj S. Lamkuche

(Assistant Professor Gr-II)

(VIT Bhopal University)

Acknowledgement

We extend our heartfelt gratitude to Dr. Hemraj Shobharam Lamakuche Sir, whose visionary leadership and unwavering support have been pivotal in steering the Governance Team at VIT Bhopal University. His guidance has been instrumental in shaping our strategies and initiatives, ensuring the effective governance and smooth functioning of our institution.

I am also thankful to VIT Bhopal University for providing the resources and environment conducive to the successful completion of this Task. Furthermore, I am grateful to my family and friends for their understanding, encouragement, and patience during this journey. Their support has been a constant source of motivation and inspiration.

Lastly, I would like to express my gratitude to all those who have contributed directly or indirectly to this project, whether through feedback, discussions, or encouragement. Your contributions have played a significant role in shaping the outcome of this endeavor.

VIT®
BHOPAL
www.vitbhopal.ac.in

Governance Team

Task Report

Submitted by

Name	Registration Number	Role	Signature
Vaibhav Shrivastava	21BCY10227	Leader	
Yash Garg	21BCY10032	Member	
Ansh H Mehta	21BCY10113	Member	
Swati	21BCY10210	Member	
Divyansh Chaudhary	21BCY10060	Member	
Shreya Pawale	21BCY10030	Member	
Ben Tom Abey	21BCY10035	Member	
Gouri Nandana	21BCY10029	Member	
Ayshatha Afla	21BCY10133	Member	
Rahul Kumar Suman	21BCY10130	Member	
Prashant Chauhan	21BCY10114	Member	
Parth Sengar	21BCY10041	Member	
Hari Shankar PC	21BCY10195	Member	
Arush Chandna	21BCY10007	Member	
Yagyarth Mishra	21BCY10034	Member	

Task Index

Preface

This project is an initiative by Dr. Hemraj S. Lamkuche, under the course of NAS2002 Advanced Cyber Security, for slot A21+A22+A23. This project is aimed to provide better understanding of the Cybersecurity Framework and its implementation at an organizational level.

A security framework defines policies and procedures for establishing and maintaining security controls. Frameworks clarify processes used to protect an organization from cybersecurity risks. They help IT security professionals and security teams keep their organizations compliant and insulated from cyber threats.

The NIST Cybersecurity Framework 2.0 has been followed for this project. This framework is divided into 6 functional divisions, namely 1) Detect Function 2) Identity Function 3) Protect Function 4) Recover Function 5) Respond Function 6) **Governance Function**.

This team has been assigned with tasks that fall under the Governance Function. Tasks that fall under the Governance Functions have been further divided into six different categories. Each of these categories relate to separate aspects within the Governance Function and are assigned with a unique code.

1. **GV.OC** Organizational Context
2. **GV.RM** Risk Management Strategy
3. **GV.SC** Cybersecurity Supply Chain Risk
4. **GV.RR** Roles, Responsibilities, and Authorities
5. **GV.PO** Policies, Processes, and Procedures
6. **GV.OV** Oversight

Each of these categories consists of various tasks along with the appropriate tools required to accomplish those tasks. The tasks are named as GV.OC-01, GV.OC-02, and so on.

GV.OC -01 (VIT Bhopal: Mission and Cybersecurity Risk Management)

1. Introduction

This report explores the crucial interplay between the mission of Vellore Institute of Technology Bhopal (VIT Bhopal) and its cybersecurity risk management strategies. Understanding the institution's foundational goals and critical assets provides insight into how aligned cybersecurity efforts help maintain a secure and trustworthy environment, enabling VIT Bhopal to fulfill its mission effectively.

2. VIT Bhopal's Mission Statement

VIT Bhopal, as a vital part of the VIT University system, commits to the following mission objectives as stated on their official website:

01. **Educational Excellence:** Provide world-class education in Engineering, Science, Technology, and Management.
02. **Innovation and Research:** Foster significant innovation, entrepreneurship, and research capabilities.
03. **Social Contribution:** Contribute actively to the advancement of knowledge and societal welfare.

3. Identification of Critical Assets

Critical assets at VIT Bhopal include but are not limited to:

01. **Personal and Academic Data:** Encompasses all personal information, academic records, and research data of students and faculty.
02. **Educational and Research Infrastructure:** Comprises IT systems, laboratories, and facilities crucial for academic delivery and research.
03. **Intellectual Property:** Consists of research findings, patents, and other proprietary materials that necessitate stringent security measures to prevent unauthorized access and theft.

4. Threat Prioritization and Assessment

Given the critical assets, the primary cybersecurity threats identified are:

01. **Data Breaches:** Risk of compromising personal and academic data leading to identity theft, privacy breaches, and reputational damage.
02. **Ransomware Attacks:** Potential disruptions to IT infrastructure, severely impacting academic and research operations.

03. **Cyber Espionage:** Threats to intellectual property that could stifle innovation and damage the institution's standing in the academic and research community.

5. Cybersecurity Risk Tolerance and Resource Allocation

While specific details on VIT Bhopal's risk tolerance are not public, a conservative approach towards risks affecting academic integrity and data privacy is likely. Resource allocation is therefore focused on:

01. **Enhanced Data Security:** Robust solutions to protect sensitive information.
02. **IT Infrastructure Security:** Advanced measures against cyber threats and disruptions.
03. **Community Awareness Programs:** Extensive cybersecurity training for students, faculty, and staff.

6. Reputation Management and Trust Enhancement through Cybersecurity

Effective cybersecurity measures are crucial in safeguarding VIT Bhopal’s reputation as a trustworthy educational and research institution. This is vital for attracting new students, faculty, and research collaborations, thereby supporting the institution's mission.

7. Strategies for Continuous Improvement and Adaptability

Cybersecurity strategies at VIT Bhopal are dynamic, evolving with technological advances and emerging threats. Regular security assessments and updates are critical in maintaining a resilient cybersecurity posture.

8. Conclusion

VIT Bhopal’s alignment of its cybersecurity strategies with its mission underscores its commitment to providing a secure educational environment. Through proactive threat management, resource allocation, and ongoing community engagement, VIT Bhopal strives to uphold its educational standards and institutional integrity.

GV.OC-02 (VIT IT Infrastructure Guidelines Report – Internal and External Stakeholders)

1. Introduction

This report delves into the intricacies of governance within VIT Bhopal University, examining its organizational structure, decision-making processes, and mechanisms for ensuring the realization of its educational goals. By understanding the principles and practices of governance, we aim to shed light on how VIT Bhopal University navigates the complexities of the higher education landscape while upholding its commitment to quality education and research.

Internal Stakeholders:

Academics:

Academics plays a vital role in the internal stakeholder group. The main duty or purpose of this group is to teach the students of the college and help them in their researches and activities and also to perform personal research too.As every group has expectations there group to have CyberSecurity expectations,few are Data security, secure collaboration tools, awareness of online plagiarism tools, secure access to library resources

01. **StakeHolders:** Faculty, Teaching Assistants, Research Assistants, Librarians.
02. **Interests:** Secure access to research data, teaching materials, and intellectual property
03. **CyberSecurity Expectations:** Data security, secure collaboration tools, awareness of online plagiarism tools, secure access to library resources

Administration:

Administration also plays an important role in the internal stakeholder group.The main duty of this group is to manage the universities operations and workflows.Since this group contains people from from the top authorities there cybersecurity expectations are a Comprehensive cybersecurity program, regular security audits, incident response plan, employee training, continuous improvement

01. **StakeHolders:** University Administration, Financial Administration, Human Resources, IT Department
02. **Interests:** Regulatory compliance, data security and privacy, protection of university assets
03. **CyberSecurity Expectations:** Comprehensive cybersecurity program, regular security audits, incident response plan, employee training, continuous improvement

Student Support Services:

Student support groups play an important role in providing support and services to the students and parents.This is also considered as the main function or works. Their Cybersecurity

expectations are Data privacy, secure communication channels, awareness of cyber threats like phishing, HIPAA compliance.

01. **StakeHolders:** Admissions Office, Financial Aid Office, Registrar's Office, Health Services, Counseling Services
02. **Interests:** Secure student records, financial data, and medical information
03. **CyberSecurity Expectations:** Data privacy, secure communication channels, awareness of cyber threats like phishing, HIPAA compliance.

Other:

These are the other non-technical and technical members of the internal Stakeholders.They act as a support for the university.Their main role is to manage various aspects of the university life. They also have a both security and Cybersecurity expectations which are Physical security measures, data security for building management systems, secure online portals, awareness of sports-related cyber threats

01. **StakeHolders:** Facilities Management, Athletics Department, Alumni Relations
02. **Interests:** Secure access to buildings and facilities, athlete data privacy, secure alumni data
03. **CyberSecurity Expectations:** Physical security measures, data security for building management systems, secure online portals, awareness of sports-related cyber threats

External Stakeholders:

Suppliers:

Suppliers play an important role in the external stakeholder group.They are not a part of the University.There main job is to provide goods and services to the college and what they in turn expect for the college is that they receive Timely payments, fair contracts, partnerships - Stable demand, collaboration and growth. Being in the external group they also have Cybersecurity expectation they are Data security, secure collaboration tools.

01. **StakeHolders:** Providers of goods and services
02. **Description:** Timely payments, fair contracts, partnerships - Stable demand, collaboration, growth
03. **Concerns:** Late payments, contract changes, disputes, financial instability, competition
04. **CyberSecurity Expectations:** Data security, secure collaboration tools, awareness of online plagiarism tools, secure access to library resources

Investors:

Investors play a crucial role in the external stakeholder groups; they can also sometimes be added in internal stakeholders also. Their main job or purpose is to provide financial support to the college if needed only.They also have cybersecurity expectations like the administration ones

which are Comprehensive cybersecurity program, regular security audits, incident response plan, employee training, continuous improvement.

01. **StakeHolders:** Financial backers
02. **Description:** Financial returns, company growth, dividends - Responsible investment, ethics
03. **Concerns:** Financial performance, risk management, governance, transparency, environmental/social impact
04. **CyberSecurity Expectations:** Comprehensive cybersecurity program, regular security audits, incident response plan, employee training, continuous improvement

Governments & Regulators:

Legal and regulators also play an important role in the external stakeholder groups, they care responsible for all legal concerns of the university which includes Compliance with laws, tax collection, environment, consumer safety

01. **StakeHolders:** Law and policy enforcers
02. **Description:** Compliance with laws, tax collection, environment, consumer safety.
03. **Concerns :** Lack of trust, intellectual property conflicts, power dynamics, internal competition
04. **CyberSecurity Expectations:** Non-compliance, corruption, environmental damage, safety hazards, anti-competitive practices.

GV.OC-03 (VIT Bhopal: Comprehensive Review of Cybersecurity Compliance)

1. Executive Summary

This report details a thorough review of VIT Bhopal's cybersecurity compliance with legal, regulatory, and contractual requirements. It underscores the institution's proactive approach in managing cybersecurity risks and highlights the strategic measures adopted to uphold and enhance its cybersecurity framework.

2. Introduction

In the digital landscape, VIT Bhopal faces numerous cybersecurity challenges that necessitate diligent management of legal, regulatory, and contractual obligations. This report provides an overview of the institution’s adherence to these obligations and outlines the tools and strategies employed to maintain robust cybersecurity practices.

3. Review of Legal, Regulatory, and Contractual Obligations

01. **Legal Obligations:** VIT Bhopal adheres to national laws such as the Information Technology Act, 2000, which mandates reasonable security practices to protect sensitive personal data.
02. **Regulatory Obligations:** The institution follows guidelines set forth by the National Cyber Security Coordinator (NCSC) and the Ministry of Electronics and Information Technology (MeitY), which provide frameworks for securing digital infrastructures and managing cybersecurity risks.
03. **Contractual Obligations:** Contractual agreements with third-party vendors and partners include stringent cybersecurity clauses to ensure data protection and secure information handling in line with industry standards.

4. Adoption of Compliance Management Tools

01. **Selection Criteria:** Key criteria included scalability, user-friendliness, and integration capabilities with existing systems, ensuring that the chosen tool effectively supports the institution's compliance needs.
02. **Tool Features:** The selected compliance management software provides comprehensive features such as risk assessment modules, compliance tracking, and real-time reporting, enhancing the institution's ability to manage and monitor its cybersecurity obligations.
03. **Implementation Strategy:** Implementation involves phased roll-outs, training sessions for stakeholders, and ongoing support to ensure smooth adoption and optimal use of the tool across the institution.

5. Comprehensive Review Methodology

The methodology involved stakeholder interviews, policy and contract reviews, and assessments of current compliance practices. This facilitated a thorough understanding of existing measures and areas needing enhancement.

6. Monitoring and Improvement Mechanisms

01. **Monitoring Framework:** A robust framework using key performance indicators (KPIs) and compliance metrics has been established to monitor adherence to cybersecurity practices and identify areas for improvement.
02. **Continuous Improvement Strategy:** VIT Bhopal is committed to continuous improvement through regular reviews, updates to cybersecurity practices, and adoption of new technologies to address evolving cybersecurity threats.

7. Conclusion

This review demonstrates VIT Bhopal's strong commitment to cybersecurity governance and its proactive approach in ensuring compliance with various cybersecurity mandates. By leveraging advanced compliance tools and maintaining a dynamic improvement strategy, VIT Bhopal aims to sustain its reputation as a secure and trusted educational institution.

8. Strategic Recommendations

01. **Policy Updates:** Regular updates to policies to align with new legal and regulatory changes.
02. **Training Enhancements:** Ongoing cybersecurity training programs for all stakeholders to foster a culture of security awareness.
03. **Regular Audits:** Conduct comprehensive audits to ensure continuous compliance and identify security gaps.
04. **Technology Watch:** Stay updated on emerging cybersecurity technologies and threats to continually adapt and enhance security measures.

GV.OC-04 (VIT Bhopal: Strategic Framework for Critical Objectives, Capabilities, and Stakeholder Communication)

1. Executive Summary

This report outlines the strategic approach adopted by Vellore Institute of Technology (VIT) to identify and communicate its critical objectives, capabilities, and services. Ensuring stakeholders are well-informed and expectations are aligned with VIT's strategic goals is fundamental to the institution's success and adherence to its mission.

2. Introduction

VIT's commitment to excellence in education, research, and societal service requires a robust framework for managing and communicating the critical objectives and capabilities that underpin its mission. This document delineates the methodologies VIT employs to determine these critical aspects and the strategies used for effective communication to its diverse stakeholder groups.

3. Identification of Critical Objectives and Capabilities

01. Critical Objectives:

a. Excellence in education and research.
b. Innovation and entrepreneurship development.
c. Societal contribution and community engagement.

02. Capabilities:

a. Advanced academic programs and research facilities.
b. Comprehensive administrative and IT infrastructure.
c. Effective security measures to ensure data privacy and campus safety.

4. Stakeholder Identification and Expectations

01. Key Stakeholders:

a. Students, faculty, and staff.
b. Alumni, industry partners, and funding agencies.
c. Local and global communities.

02. Expectations:

a. High-quality education and innovative research output.
b. Secure and supportive campus environment.
c. Ethical conduct and societal impact.

5. Strategic Communication of Expectations

To effectively communicate the established objectives and capabilities, VIT utilizes:

01. Regular updates through email newsletters and official web portals.

02. Interactive sessions such as town hall meetings and feedback forums.
03. Social media platforms for broader engagement.

6. Cybersecurity Policy Framework

Given the digital and data-driven nature of VIT's operations, establishing a robust cybersecurity policy is crucial. This policy covers:

01. Acceptable Use Policy: Guidelines on the proper use of VIT's digital resources.
02. IT Hardware and Software Policies: Standards for procurement, installation, and licensing.
03. Network Security: Protocols to secure institutional data against unauthorized access.

7. Implementation Examples

01. 1st Party Risk:

a. **Criteria Establishment:** Define what constitutes a critical capability or service based on its impact on VIT's mission.
b. **Business Impact Analysis:** Identify assets and operations crucial to the mission and assess the impact of their potential loss.

02. 3rd Party Risk:

a. **Vendor Management:** Evaluate and manage risks associated with external vendors and service providers**.**

03. Resilience Objectives:

a. **Recovery Time Objectives:** Set and communicate objectives for quick recovery of services in different operational states (e.g., under cyber-attack).

8. Conclusion

This strategic framework enables VIT to align its operations with its mission effectively, ensuring that all stakeholders understand and support the institution's objectives and capabilities. Continuous improvement through feedback and adaptation to new challenges remains a cornerstone of VIT's strategy.

GV.OC-05 (VIT IT Infrastructure Guidelines Report - Entailing Outcomes, capabilities, and services to the organization)

1. Introduction

This report presents a comprehensive assessment of cybersecurity outcomes, capabilities, and services critical to VIT, with a particular focus on collaboration platforms like Microsoft Teams for internal communication. By documenting key findings and recommendations, this report aims to strengthen the university's cybersecurity posture and ensure the secure utilization of collaboration tools across its academic and administrative domains.

Documenting Critical Outcomes, Capabilities, and Services:

01. **Identify critical outcomes:** Ensure secure and efficient communication and collaboration among university staff, students, and stakeholders.
02. **Assess capabilities:** Evaluate the features and functionalities of collaboration platforms like Microsoft Teams in meeting the university's communication needs while maintaining cybersecurity standards.
03. **Document critical services:** Document the essential services provided by collaboration platforms, including messaging, file sharing, video conferencing, and integration with other productivity tools.

Assessment of Microsoft Teams for Internal Communication:

01. **Security features:** Evaluate built-in security features such as end-to-end encryption, multi-factor authentication, data encryption in transit and at rest, and role-based access controls.
02. **Compliance standards:** Assess compliance with relevant regulations and standards, such as GDPR, HIPAA, FERPA, and ISO 27001, to ensure data privacy and regulatory compliance.
03. **Vulnerability management:** Review Microsoft's approach to vulnerability management, patching cadence, and response to security incidents to mitigate potential risks.

Outcomes:

01. Critical Services

a. **Library:** VIT library has updated its entry system from the traditional manual way to biometric authentication, it stores the data of students in their database and authenticates accordingly.
b. **VTOP:** When it comes to crucial services, VTOP is at the top of the list. It consists of students' bank details, addresses, contact information, faculties information.

c. **CTS Office:** The CTS Office serves as the central system to maintain all technical services of the university. Their database consists of all the passwords and keys to major internet services of the university.
d. **CCTV Cameras:** If the CCTV cameras in the campus plays a vital role in the security of the University as it monitors the physical activities in and around the campus preventing any mishaps.
e. **Security Guards:** The personnel of the security agency in the university play a key role in avoiding any manual attack on the resources of the organization

02. Exploits

Library: VIT library has updated its entry system from the traditional manual way to biometric authentication, it stores the data of students in their database and authenticates accordingly.

a. **SQL Injection:** Attackers may exploit vulnerabilities in the database management systems to inject malicious SQL code. This can lead to unauthorized access, data manipulation, or complete database compromise.
b. **DDos:** Attackers may launch DDoS attacks against library database servers to overwhelm them with a flood of traffic, rendering them unavailable to legitimate users.

VTOP:

c. **Phishing Attacks:** Cybercriminals may attempt to trick students, faculty, or staff into divulging their login credentials through phishing emails or fake login pages. Once obtained, these credentials can be used to gain unauthorized access to the portal and sensitive information stored within it.
d. **Ransomware:** Malicious software could infect the portal's servers and encrypt the data stored within them, rendering it inaccessible until a ransom is paid. This could disrupt the portal's functionality and lead to data loss or financial losses if the ransom is paid.

CTS Office:

e. **Insider Threats:** Malicious insiders with access to the CTS Office's systems could abuse their privileges to steal or leak sensitive information, or to sabotage technical services. This could pose a significant security risk to the university's infrastructure and operations.
f. **Denial of Service (DoS) Attacks:** Hackers may launch DoS attacks against the CTS Office's systems to disrupt technical services or to overwhelm network infrastructure. This could lead to service outages and impact the university's operations.

CCTV Cameras:

a. **Unauthorized Access**: If the CCTV camera system is connected to the university network or accessible via the internet, hackers may exploit vulnerabilities in the camera firmware or software to gain unauthorized access. Once compromised, hackers can potentially use the cameras to spy on sensitive areas, monitor activities, or even disrupt operations.

Security Guards:

a. **Social Engineering:** Attackers may target security personnel through social engineering tactics to manipulate them into providing sensitive information or granting unauthorized access to facilities or systems. This could include pretexting, phishing, or impersonation techniques.
b. **Insider Threats:** While security personnel are tasked with protecting the organization, they could pose a risk if they become malicious insiders. They may abuse their access privileges to steal sensitive information, tamper with security controls, or facilitate cyber attacks from within the organization.
c. **Credential Theft:** Security personnel may be targeted for their access credentials to critical systems or physical locations. If their credentials are compromised, attackers could gain unauthorized access to sensitive resources, compromising the organization's security posture.
d. **Unintentional Data Disclosure:** Security personnel may unintentionally disclose sensitive information during their duties, such as discussing security protocols or sharing access codes. This information could be exploited by attackers to circumvent security measures or launch targeted cyber attacks.

Conclusion

By documenting outcomes, capabilities, and services critical to , particularly in the context of collaboration platforms like Microsoft Teams, the university can enhance its cybersecurity resilience and foster a safe and productive digital environment for its staff and students.

GV.RM-01 (VIT IT Infrastructure Guidelines Report - Enhanced with Technical Details and Cybersecurity Considerations)

1. Introduction

This report provides a comprehensive analysis of the VIT IT Infrastructure Guidelines document (GV.RM-01), focusing on its key elements: Risk Management Strategy and the Acceptable Use Policy (AUP). We will delve into the technical aspects of these policies and highlight cybersecurity considerations for a more secure IT environment.

2. Risk Management Strategy

The Risk Management Strategy aims to mitigate various cybersecurity threats to the VIT IT infrastructure. These threats can include:

01. **Malware:** Malicious software such as viruses, worms, and ransomware can infect devices, steal data, or disrupt operations.
02. **Phishing Attacks:** Deceptive emails or websites attempt to trick users into revealing sensitive information like passwords or financial details.
03. **Denial-of-Service (DoS) Attacks:** These attacks overwhelm a network with traffic, making it unavailable to legitimate users.
04. **Data Breaches:** Unauthorized access to sensitive data can occur through hacking, social engineering, or physical theft.

The strategy should encompass technical safeguards like:

01. **Firewalls:** These act as barriers between the internal network and the internet, filtering incoming and outgoing traffic.
02. **Intrusion Detection/Prevention Systems (IDS/IPS):** These systems monitor network activity for suspicious behavior and can block potential attacks.
03. **Data Encryption:** Encrypting data at rest and in transit renders it unreadable to unauthorized users even if intercepted.
04. **Vulnerability Management:** Regularly patching software vulnerabilities eliminates potential entry points for attackers.

3. Resources Covered

The strategy protects a wide range of IT resources, each with its own security considerations:

01. **Network Devices (wired/wireless) and Internet Access:** Secure network configuration with strong encryption (WPA2/WPA3) for Wi-Fi and access controls limiting unauthorized connections are crucial.

02. **Official Websites and Web Applications:** Implementing secure coding practices, regular vulnerability assessments, and using multi-factor authentication for logins can significantly enhance security.
03. **Official Email Services:** User education on phishing attacks and implementing spam filters can help prevent malware infections and data breaches.
04. **Data Storage:** Utilizing access controls, data encryption, and secure disposal practices safeguards sensitive information.
05. **Mobile/Desktop/Server Computing Facilities:** Enforcing strong password policies, endpoint security software deployment, and restricting unauthorized software installation are essential security measures.
06. **Documentation Facilities (Printers & Scanners):** Securing these devices with strong passwords and access controls prevents unauthorized document access.
07. **Multimedia Content:** Implementing copyright protection measures and managing access controls for sensitive content are important considerations.

4. Acceptable Use Policy (AUP)

The AUP defines a set of rules for utilizing VIT's IT infrastructure. It aims to:

01. Reduce potential legal issues arising from user actions, such as copyright infringement or illegal downloads.
02. Ensure responsible and ethical use of resources, preventing activities like cyberbullying or hacking attempts.

The AUP outlines specific policies for different user groups, emphasizing cybersecurity awareness:

01. **Employee AUP:** Educating employees on safe browsing practices, password hygiene, and reporting suspicious activity is crucial.
02. **Student AUP:** Promoting responsible online behavior, including avoiding plagiarism and unauthorized use of licensed software, is essential.
03. **Vendor AUP:** Ensuring vendors adhere to data security best practices and contractual agreements regarding data access is vital.

5. AUP Policy Elements

The AUP further encompasses various sub-policies governing specific aspects of IT usage, with a focus on cybersecurity:

01. **Network Security Policy:** Defines guidelines for securing the network infrastructure, including measures against unauthorized access, malware propagation, and DoS attacks.
02. **Addressing and Domain Services:** Manages IP address allocation and domain name usage. This can include implementing techniques like whitelisting to restrict access to known malicious websites.

03. **Network Connections:** Regulates wired and wireless network access. Implementing network segmentation can limit the impact of a security breach within a specific network segment.
04. **External Traffic, Services & Requests:** Governs accessing external resources and services. Firewalls and web filters can be used to restrict access to malicious websites or prevent data exfiltration.
05. **Network Security:** Outlines procedures to maintain network security, including regular security audits and incident response protocols.
06. **Enforcement:** Describes how violations are addressed and disciplinary actions taken. This should include clear consequences for cybersecurity breaches.
07. **Monitoring and Auditing:** Defines methods for monitoring network activity and user compliance. This can involve log analysis to detect suspicious activity.
08. **Email Use Policy:** Regulates proper email usage within the VIT network. This includes prohibiting spam, phishing attempts, and promoting responsible email content.

6. Conclusion

The VIT IT Infrastructure Guidelines document (GV.RM-01) plays a The VIT IT Infrastructure Guidelines document (GV.RM-01) plays a crucial role in safeguarding the institution's IT resources. By understanding the Risk Management Strategy and the Acceptable Use Policy, along with the technical security measures outlined above, all stakeholders can contribute to a more secure IT environment within VIT.

Here are some additional recommendations for strengthening cybersecurity within the VIT IT infrastructure:

01. **Regular Security Awareness Training:** Educating all users on cybersecurity best practices, including identifying phishing attempts, creating strong passwords, and reporting suspicious activity, is an ongoing process.
02. **Data Backup and Recovery:** Implementing a robust backup and recovery plan ensures vital data can be restored in case of a cyberattack or system failure.
03. **Incident Response Plan:** Having a clear plan for identifying, responding to, and recovering from security incidents minimizes downtime and data loss.
04. **Security Information and Event Management (SIEM):** A SIEM system collects and analyzes security data from various sources, providing real-time insights into potential threats.
05. **Multi-Factor Authentication (MFA):** Enforcing MFA for all user accounts adds an extra layer of security beyond just passwords.

By adopting a comprehensive approach that combines policy, technical safeguards, and user awareness, VIT can create a more secure IT infrastructure that fosters a trusted learning and working environment.

GV.RM-02 (VIT IT Infrastructure Guidelines Report – Risk Management Strategy)

1. VIT Risk Appetite Statement

VIT is committed to achieving its strategic goals while upholding a responsible approach to risk management, which serves as the foundation for our operations. Proactive risk identification and mitigation are fundamental principles that guide our decision-making processes, ensuring that we are prepared to encounter and address potential challenges effectively. Our risk tolerance framework is strategically designed to adapt to various categories, allowing us to embrace calculated risks that align with our strategic objectives while maintaining a prudent assessment of potential outcomes. We understand the significance of striking a balance between risk and potential rewards, and our continuous efforts are centered on refining and enhancing our risk management practices to ensure that we are well-equipped to navigate the dynamic business environment with confidence and resilience.

2. VIT Risk Tolerance Level

Risk Category –

Financial

01. Description:

a. Financial risks facing our colleges include enrollment fluctuations impacting revenue, government funding cuts, underperforming endowments, balancing faculty costs with infrastructure needs, uncertain research funding, capital expenditures, market volatility, cybersecurity threats, and legal compliance risks. Mitigation strategies involve careful planning, revenue diversification, and proactive risk management to maintain stability.

02. Tolerance Level:

a. The maximum acceptable financial loss per year for our engineering college varies depending on its size, financial resources, and risk tolerance. However, a common approach is to aim for a loss that does not exceed a certain percentage of the college's annual budget. For example, if the college has a budget of Rs.10 Lakh per year, it might aim to keep the maximum acceptable financial loss to, say, 5% of the budget, which would be 50,000. This threshold allows the college to absorb unexpected losses without significantly impacting its operations or long-term financial health.

03. Metrics:

a. **Fraud Rate:** The fraud rate reflects the likelihood or incidence of fraudulent activities occurring within the college's financial operations. This includes misappropriation of funds, falsification of financial records, or other dishonest behaviors. Maintaining a low fraud rate is crucial for preserving the college's

financial integrity, trustworthiness, and reputation among stakeholders, including students, faculty, donors, and regulatory bodies.

b. **Return on Investment (ROI):** ROI measures the efficiency and effectiveness of the college's investments in various areas such as infrastructure development, research initiatives, academic programs, and student support services. A positive ROI indicates that investments are generating returns that exceed the initial investment, contributing to the college's financial sustainability and overall mission.

Operational

01. Description:

a. In our engineering college, risks include outdated curriculum affecting competitiveness, faculty issues impacting instruction quality, lack of student support hindering retention, aging infrastructure disrupting activities, outdated technology hampering learning, accreditation non-compliance jeopardizing funding and reputation, and supply chain disruptions impacting service delivery. Addressing these risks involves updating curriculum, investing in faculty development, enhancing support services, maintaining facilities, upgrading technology, ensuring compliance, and managing supply chain dependencies

02. Tolerance Level:

The maximum acceptable downtime for critical systems in an engineering college, such as student information systems, learning management systems, or research databases, depends on various factors, including the importance of the system to daily operations and the impact of downtime on productivity, learning, and research activities.

Typically, acceptable downtime for critical systems is measured in minutes or hours rather than days. A common benchmark for mission-critical systems is often less than one hour of downtime annually, although this can vary based on specific institutional needs and industry standards.

To determine the maximum acceptable downtime, colleges should conduct a thorough risk assessment, considering factors such as the system's importance, potential financial losses due to downtime, regulatory requirements, and stakeholder expectations. This assessment can help establish realistic downtime targets and guide investments in redundancy, disaster recovery, and system resilience to minimize disruptions and maintain operational continuity.

03. Metrics:

a. **Process Efficiency Metrics:** These metrics evaluate the effectiveness and productivity of various operational processes within the college, such as admissions, academic advising, financial aid processing, and facilities management.

b. **Cycle Time:** The time taken to complete a specific process from start to finish.

c. **Throughput:** The rate at which tasks or transactions are completed within a given timeframe.

d. **Resource Utilization:** The extent to which resources, such as staff, facilities, or funds, are effectively utilized to achieve desired outcomes.
e. **Error Rate:** The frequency of errors or mistakes occurring within a process, impacting quality and efficiency.
f. **Cost per Process:** The cost incurred to perform a specific process, including labor, materials, and overhead expenses.
g. **Customer Satisfaction Ratings:** These ratings measure the level of satisfaction among various stakeholders, including students, faculty, staff, alumni, and external partners, with the services and experiences provided by the college.
h. **Problem Resolution:** The college's ability to address issues, concerns, or complaints raised by stakeholders promptly and effectively.
i. **Overall Experience:** Stakeholders' overall perception and experience with the college, encompassing all interactions and touchpoints throughout their engagement.

Reputational

01. Description:

Risks that could damage a college's reputation and public image include academic integrity violations, faculty or staff misconduct, financial mismanagement, accreditation issues, legal and compliance violations, negative media coverage, safety and security incidents, alumni or donor relations issues, ethical research practices, and failures in environmental or social responsibility. Mitigating these risks requires proactive risk management, effective communication, transparent governance, and a commitment to upholding ethical standards and institutional values.

02. Tolerance Level:

With a zero-tolerance policy for major compliance violations, the college sets a stringent standard for ethical conduct and regulatory adherence. This stance communicates a commitment to upholding integrity and accountability across all levels of the institution. Any major breaches of compliance are swiftly addressed with disciplinary action, corrective measures, and transparency to maintain trust and credibility. This approach reinforces a culture of compliance, minimizes reputational risks, and ensures the college's continued adherence to legal and regulatory requirements.

03. Metrics:

Metrics for negative media mentions and public perception surveys provide essential insights into our college's reputation and image. Negative media mentions reflect the occurrence and impact of adverse publicity or controversies, guiding crisis management and communication strategies. Public perception surveys assess stakeholders' attitudes and opinions, informing efforts to enhance satisfaction, address concerns, and maintain a positive reputation. These metrics enable proactive reputation management and strategic decision-making to uphold the college's standing in the community.

GV.RM-03 (Integrating Cybersecurity into Enterprise Risk Management (ERM))

Challenge: Ensuring VIT Bhopal's ERM processes effectively handle cybersecurity risks alongside other enterprise risks.

Solution: Seamlessly integrate Cybersecurity Risk Management (CSRM) into VIT Bhopal's existing ERM framework.

Information Security Considerations

01. **Human Element:** Recognize the risks posed by human error and social engineering attacks. Address these through targeted employee training and awareness initiatives.
02. **CIA Triad:** The CSRM plan must address threats to the Confidentiality, Integrity, and Availability of critical data and systems at VIT Bhopal.

Integration Strategy

01. Assessment:

a. Review VIT Bhopal's current ERM framework, including processes for risk identification, assessment, and mitigation.
b. Perform a comprehensive assessment of cybersecurity risks, focusing on the CIA triad and data sensitivity (e.g., student records, financial data).

02. Developing a CSRM Plan:

a. Create a detailed CSRM plan that includes:
b. Roles and responsibilities for CSRM within the ERM structure.
c. Methods for identifying, assessing, and prioritizing cybersecurity risks based on the CIA triad and data sensitivity.
d. Strategies for mitigation, such as security awareness training, patch management, and intrusion detection systems.
e. Monitoring and reporting procedures to measure the effectiveness of cybersecurity controls.
f. Align CSRM and ERM terminology, assessment methods, and reporting formats for consistency.

Implementation

01. **Updating ERM Tools:** Modify existing tools like risk registers and reporting templates to include cybersecurity risks.
02. **Integration with ERM Software:** Consider merging security risk management tools with ERM software for seamless data collection and analysis.

03. **Training Programs:** Offer training sessions for relevant staff on cybersecurity risk identification and reporting, their role in the ERM process, and best security practices.

Continuous Improvement

01. **Regular Reviews:** Conduct periodic reviews (quarterly or annually) of the CSRM plan and its integration with ERM.
02. **Plan Updates:** Adapt the plan to changes in the cybersecurity threat landscape, business needs, or ERM processes.
03. **Ongoing Risk Assessments:** Perform regular assessments to identify emerging or evolving cybersecurity threats.
04. **Performance Tracking:** Establish key performance indicators (KPIs) to measure CSRM's effectiveness within the ERM framework (e.g., number of incidents reported, employee training participation).

Utilizing Enterprise Risk Management Platforms

While optional, consider using ERM platforms to streamline the integration of CSRM into ERM. Benefits include:

01. **Centralized Risk Management:** Manage all enterprise risks, including cybersecurity, from a unified platform.
02. **Automated Workflows:** Automate tasks such as risk assessments and reporting for improved efficiency.
03. **Data Analytics:** Leverage risk data insights to identify trends and inform risk management decisions.

Conclusion

Integrating CSRM into the ERM framework while focusing on information security principles will help VIT Bhopal establish a more comprehensive and proactive approach to managing all enterprise risks, including cybersecurity threats. This integration will contribute to the institution's overall security and resilience.

GV.RM-04 (VIT IT Infrastructure Guidelines Report - Identify and prioritize suppliers by criticality to the organization.)

1. Introduction

To fortify VIT's cybersecurity supply chain risk management strategies. This report outlines key tasks in identifying and prioritizing suppliers by criticality to the organization, as well as implementing supplier risk assessment tools for effective evaluation and ranking based on criticality and risk.

Identifying and Prioritizing Suppliers:

01. **Define criticality factors:** Identify key criteria such as the importance of the supplied goods/services, access to sensitive data, and potential impact on university operations.
02. **Inventory suppliers:** Compile a comprehensive list of suppliers and categorize them based on criticality factors.
03. **Prioritization process:** Develop a systematic approach to prioritize suppliers, considering their criticality to the organization.

Supplier Risk Assessment Tools:

01. **Selection criteria:** Evaluate and choose appropriate supplier risk assessment tools based on their compatibility with university systems, comprehensiveness, ease of use, and cost-effectiveness.
02. **Implementation plan:** Outline steps to integrate selected tools into existing procurement and supplier management processes.
03. **Training and awareness:** Provide training sessions and resources to relevant staff members on how to effectively utilize the chosen assessment tools.
04. **Continuous improvement:** Establish mechanisms for regular reviews and updates to the supplier risk assessment process to adapt to evolving threats and organizational changes.

Critical Vendors of the Organisation

01. **Software Vendors:** Companies or organizations that provide software solutions used by the university for administrative purposes (e.g., enterprise resource planning systems), academic purposes (e.g., learning management systems), or research purposes (e.g., data analysis software).
02. **Hardware Suppliers:** Manufacturers or distributors of hardware components and devices used within the university's IT infrastructure, including servers, networking equipment, computers, and peripherals.
03. **Cloud Service Providers:** Companies that offer cloud-based services for storing data, hosting applications, or delivering computing resources. This includes providers of cloud storage, cloud computing platforms, and software-as-a-service (SaaS) applications.

04. **Third-party Service Providers:** External vendors or contractors that offer specialized services to the university, such as managed IT services, cybersecurity consulting, data management, or outsourced administrative functions.
05. **Educational Technology Providers:** Suppliers of educational technology solutions used for teaching, learning, and research purposes, including e-learning platforms, online courseware, virtual labs, and educational software applications.
06. **Physical Security Providers:** Companies that supply physical security systems and services, such as access control systems, surveillance cameras, alarm systems, and security personnel services.
07. **Telecommunications Providers:** Providers of telecommunications services, including internet service providers (ISPs), telecommunications carriers, and vendors of voice communication systems.

Identifying and prioritizing suppliers based on criticality to the organization, followed by evaluating and ranking them using risk assessment criteria:

Software Vendors:

01. **Criticality:** High, as software solutions are integral to administrative, academic, and research functions.
02. **Risk Assessment Criteria:** Data security measures, vulnerability management, software update frequency.
03. **Ranking:** Vendor A (strong security measures, regular updates), Vendor B (adequate security but infrequent updates), Vendor C (lacks comprehensive security measures).

Hardware Suppliers:

01. **Criticality:** High, as hardware components form the foundation of the university's IT infrastructure.
02. **Risk Assessment Criteria:** Hardware integrity, firmware security, supply chain transparency.
03. **Ranking:** Vendor X (trusted brand with transparent supply chain), Vendor Y (reliable hardware but limited transparency), Vendor Z (unknown reputation and supply chain).

Cloud Service Providers:

01. **Criticality:** High, as cloud services store sensitive university data and host critical applications.
02. **Risk Assessment Criteria:** Data encryption, compliance certifications, incident response capabilities.
03. **Ranking:** Provider P (compliant with industry standards, strong encryption), Provider Q (certified but lacks robust incident response), Provider R (insufficient encryption and compliance measures).

Third-party Service Providers:

01. **Criticality:** Medium to High, depending on the services provided and access to university systems.
02. **Risk Assessment Criteria:** Access controls, data handling practices, contractual obligations.
03. **Ranking:** Provider M (clear contractual terms, stringent access controls), Provider N (limited access controls, unclear data handling practices), Provider O (inadequate contractual protections).

Educational Technology Providers:

01. **Criticality:** Medium to High, as educational technology supports teaching and learning activities.
02. **Risk Assessment Criteria:** Data privacy features, integration capabilities, vendor reputation.
03. **Ranking:** Provider S (strong data privacy features, seamless integration), Provider T (limited integration capabilities, mixed reputation), Provider U (lacks essential data privacy features, unknown reputation).

Physical Security Providers:

01. **Criticality:** Medium, as physical security complements digital security measures.
02. **Risk Assessment Criteria:** Physical access controls, surveillance system integrity, personnel training.
03. **Ranking:** Provider V (robust access controls, reliable surveillance systems), Provider W (adequate controls but outdated surveillance technology), Provider X (limited access controls and training protocols).

Telecommunications Providers:

01. **Criticality:** Medium, as telecommunications services support communication and data transmission.
02. **Risk Assessment Criteria:** Network security measures, uptime reliability, compliance with privacy regulations.
03. **Ranking:** Provider D (strong network security, reliable uptime), Provider E (adequate security but occasional downtime issues), Provider F (lacks comprehensive security measures, compliance concerns).

GV.RM-05 (VIT IT Infrastructure Guidelines Report - Establishing lines of communication for cybersecurity risks and Securing messaging and communication tools for internal and external communication.)

1. Introduction

Creating lines of communication for cybersecurity risks, including supplier risks, is paramount in safeguarding the digital infrastructure of a university. Implementing secure messaging and communication tools both internally and externally fortifies defenses and ensures swift responses to potential threats, fostering a resilient cybersecurity environment.

Updating Senior Leadership on Cybersecurity Posture

01. **Executive Dashboards:** Develop an interactive dashboard specifically designed for senior leadership. This dashboard should focus on high-level metrics that provide a clear and concise overview of the organization's cybersecurity posture. Consider including
02. **Overall Security Posture:** A visual representation of the overall cybersecurity risk level (e.g., high, medium, low).
03. **Top Threats:** A list of the most critical threats currently facing the organization. Recent **Incidents:** A summary of recent cybersecurity incidents, including their nature and resolution. **Security Training Completion Rates:** A visualization of employee completion rates for cybersecurity awareness training programs.
04. **Security Briefings:** During briefings with senior leadership, tailor the discussion to focus on the business impact of security risks. Examples include:
    a. How a specific security vulnerability could disrupt critical operations or lead to financial losses.
    b. The potential reputational damage from a data breach.
    c. The return on investment (ROI) associated with proposed cybersecurity solutions.

2. Interdepartmental Communication on Cybersecurity Risks

01. **Cross-functional Teams:** Create cross-functional teams with representatives from the following departments:
02. **Management:** Provides leadership and allocates resources for cybersecurity initiatives.
03. **Operations:** Identifies risks associated with daily business processes and ensures operational controls are in place.
04. **Internal Audit:** Independently assesses the effectiveness of cybersecurity controls and identifies areas for improvement.
05. **Legal:** Provides guidance on legal requirements and implications related to cybersecurity incidents and data breaches.
06. **Acquisition:** Evaluates the cybersecurity posture of potential vendors and integrates security considerations into contracts.

07. **Physical Security:** Collaborates on securing physical access to IT systems and facilities.
08. **HR:** Develops and implements security awareness training programs for employees and manages the reporting of suspicious activity.
09. **Tabletop Exercises:** Design tabletop exercises that simulate cyber attacks relevant to different departments. For example:
    a. Simulate a phishing attack targeting the HR department to test their ability to identify and report suspicious emails.
    b. Simulate a ransomware attack impacting critical operational systems to test collaboration between operations and the IT security team.

3. Secure messaging communication tool Internal Communication:

Team Collaboration Platforms:

01. **Slack, Microsoft Teams:** Popular choices for real-time messaging, file sharing, and project management. They offer features like user permissions and encryption for secure communication within your organization.
02. **Discourse:** An open-source platform for creating internal forums for discussions, knowledge sharing, and collaboration. It offers strong administrative controls and user access management.
03. **Intranet Portals:** Secure internal websites for company announcements, policy documents, and employee resources. Often integrated with single sign-on (SSO) for secure access.
04. **Enterprise Video Conferencing:** Platforms like Zoom or Webex offer secure video conferencing options with features like encryption and waiting rooms for added security during internal meetings.

4. External Communication:

01. **Email with Encryption:** Consider using email encryption services like PGP or S/MIME for sensitive communication with external parties. These services ensure only authorized recipients can decrypt the message content.
02. **Secure File Sharing Platforms:** Platforms like Dropbox or Microsoft OneDrive offer business plans with features like password protection, access controls, and audit logs for secure file sharing with external contacts.
03. **Web Conferencing with Guest Access:** Many video conferencing platforms offer guest access options for external participants. Look for features like waiting rooms and screen sharing restrictions to maintain control of the communication flow.
04. **Customer Relationship Management (CRM) Systems:** These systems provide secure communication channels for interacting with customers, managing support tickets, and sharing limited information.

GV.SC-01 (VIT Bhopal University: Cyber Security Supply Chain Risk Management Program)

1. Executive Summary

This report outlines a comprehensive Cyber Security Supply Chain Risk Management (SCRM) program specifically designed for VIT Bhopal University. It aims to safeguard sensitive data, intellectual property, and critical infrastructure from cybersecurity threats originating from or affecting the supply chain.

2. Introduction

Given the interconnected nature of today's digital ecosystem, VIT Bhopal University acknowledges the critical need for robust cybersecurity practices across its entire supply chain. This report presents a structured approach to managing cybersecurity risks associated with third-party vendors and suppliers.

3. Program Objectives and Importance

Objective: To protect VIT Bhopal University's assets, operations, and reputation from cybersecurity risks associated with the supply chain. The SCRM program will involve the entire university community and its external partners to ensure comprehensive risk management.

4. Risk Assessment and Planning

A detailed risk assessment will be conducted to identify potential cybersecurity threats linked to each vendor and supplier. The university will develop a risk management plan that includes specific strategies for mitigation, emphasizing the importance of aligning these strategies with overall institutional objectives.

5. Vendor Selection and Due Diligence

Vendor selection will be guided by stringent criteria that include security posture, compliance with standards, financial stability, and historical performance. Comprehensive due diligence will be performed to ensure that all vendors meet VIT Bhopal University's cybersecurity requirements.

6. Security Controls Implementation

Key measures will include:

01. **Data Protection:** Mandate encryption and secure data management practices.

02. **Access Controls:** Implement stringent access controls to limit exposure to potential breaches.
03. **Incident Reporting:** Vendors must comply with incident reporting obligations to ensure prompt response and mitigation.

7. Monitoring and Incident Response

The university will establish protocols for ongoing monitoring of vendor compliance with security requirements. An incident response framework will also be developed to manage and mitigate incidents efficiently, with clear roles and responsibilities defined.

8. Training and Awareness

Cybersecurity training programs will be mandatory for all university staff involved in managing or interacting with the supply chain. Vendors will also receive guidelines and training materials to ensure they are aware of and comply with VIT Bhopal University's cybersecurity expectations.

9. Continuous Improvement and Adaptability

The SCRM program will be subject to regular reviews and updates to adapt to new cybersecurity threats and changes in regulatory requirements. This will include periodic audits and reassessments to evaluate the effectiveness of implemented strategies.

10. Policy Documentation and Communication

Comprehensive documentation of all SCRM policies and procedures will be prepared. These documents will be communicated clearly to all relevant stakeholders within the university and across the supply chain to ensure understanding and compliance.

11. Conclusion

Implementing a tailored SCRM program will significantly enhance VIT Bhopal University's cybersecurity posture and resilience. By addressing supply chain-related risks proactively, the university will protect its operational capabilities and maintain its reputation as a secure and trusted institution.

GV.SC-02 (VIT IT Infrastructure Guidelines Report - Define and communicate cybersecurity roles for suppliers, customers, and partners.)

1. Introduction

This document outlines the plan to coordinate cybersecurity roles and responsibilities for suppliers, customers (students, faculty, staff), and partners at VIT Bhopal University, adhering to the NIST Cybersecurity Framework guideline GV.SC-02.

1. Defining Cybersecurity Roles

1.1 Cybersecurity Roles:

Suppliers:supplies to VIT Bhopal University encompass a range of entities providing goods and services critical to the institution's functioning. Defining cybersecurity roles and expectations for suppliers includes emphasizing compliance with security protocols, data protection measures, and timely reporting of security incidents.

Suppliers are expected to adhere to the following responsibilities:

01. Comply with the university's cybersecurity policies and standards.
02. Safeguard any sensitive information shared or accessed during the course of their engagement.
03. Promptly report any security incidents or breaches that may impact the university's systems or data.
04. Secure coding practices
05. Data security measures (encryption, access controls)
06. Incident reporting procedures
07. Identify cybersecurity focal points within supplier organizations.
08. Define responsibilities regarding secure data exchange and protection.
09. Communicate expectations for compliance with established security protocols and standards.

Customers (Students, Faculty, Staff): Students and faculty members constitute the primary stakeholders within the university community. Defining cybersecurity roles for students, faculty, and other staff members includes outlining responsibilities such as adherence to acceptable use policies, safeguarding sensitive information, and promptly reporting security concerns

01. Responsible use policies for IT resources (acceptable use policy)
02. Password management guidelines (strong password creation, rotation)
03. Phishing awareness training participation
04. Outline expectations for data protection and secure communication channels.
05. Provide guidance on reporting security incidents and vulnerabilities.
06. Collaborate on security risk assessments and mitigation strategies.

Students:

01. Adhere to the university's acceptable use policies regarding information technology resources.
02. Safeguard their login credentials, personal data, and any sensitive information accessed during academic or extracurricular activities.
03. Promptly report any suspicious activities, cybersecurity incidents, or potential vulnerabilities encountered.

Faculty:

01. Set an example by strictly adhering to the university's acceptable use policies and ensuring compliance among students and colleagues.
02. Safeguard sensitive research data, student records, and other confidential information through appropriate security measures.
03. Promptly report cybersecurity incidents or concerns to the university's IT department or designated personnel.

Partners:

01. Data sharing protocols (secure transfer methods, access restrictions)
02. Encryption standards for data at rest and in transit
03. Communication channels for reporting cybersecurity incidents

1.2 Communicating Defined Roles

Training and Communication Sessions

Conduct regular training sessions to educate stakeholders on their cybersecurity roles and responsibilities.

Foster open channels of communication to address queries and concerns related to security practices.

Encourage a culture of security awareness and vigilance across all stakeholder groups.

01. Training sessions will be conducted for:

a. Suppliers (onboarding and periodic)

b. Customers (students, faculty, staff) - integrated into existing training programs or dedicated sessions.

c. Partners (during collaboration initiation and periodically)

02. Training will cover:

a. Relevant aspects of the Cybersecurity Policy

b. Specific roles and responsibilities for each group

c. Best practices for secure behavior

1.3 Tracking Documentation and Compliance

Documentation Tracking

Tools will be implemented to track the distribution and acknowledgment of cybersecurity

01. policies by each stakeholder group. This could include:
02. E-signature platforms for electronic acknowledgment
03. Training registration systems with policy acceptance confirmation

Compliance Tracking Mechanisms

01. Mechanisms will be established to monitor adherence to defined cybersecurity protocols. Examples include:
02. Security assessments for suppliers (penetration testing, vulnerability scans)

03. Phishing simulations for customers to assess awareness and response
04. Periodic reviews of data sharing practices with partners

Maintaining Records

Detailed records will be maintained for:

01. Training participation (attendance records)
02. Policy acknowledgements (electronic signatures)
03. Compliance assessments (reports)

1.4 Implementation Timeline

A detailed timeline with milestones for completing each aspect of the plan (policy development, training sessions, tracking tool implementation) will be established.

1.5 Collaboration and Review

01. Collaboration will be sought from relevant departments (IT, procurement, legal, HR) to ensure alignment and support for the cybersecurity initiatives.
02. Regular reviews (annual or bi-annual) of the Cybersecurity Policy, training materials, and compliance mechanisms will be conducted to ensure effectiveness in the evolving cyber threat landscape.

1.6 Continuous Improvement:

Establish mechanisms for collecting feedback and suggestions for enhancing the effectiveness of the cybersecurity roles and responsibilities framework.

01. Conduct regular reviews and audits to identify gaps or weaknesses in implementation.
02. Stay updated on emerging cybersecurity threats and industry best practices to adapt the framework accordingly.

Conclusion

By implementing this plan, VIT Bhopal University will effectively define, communicate, and coordinate cybersecurity roles and responsibilities for suppliers, customers, and partners. This collaborative approach will contribute significantly to a more secure IT environment for the university community.

GV.SC-03 (VIT IT Infrastructure Guidelines Report - Integrate SCM into Risk Management)

1. Introduction

Integrating Supply Chain Management (SCM) into Risk Management is a strategic imperative for modern businesses aiming to navigate the complexities and uncertainties of global markets. Supply chains have become increasingly intricate, spanning multiple geographies, involving numerous stakeholders, and subject to various risks ranging from geopolitical tensions to natural disasters. Therefore, embedding risk management practices within SCM frameworks is crucial for enhancing resilience, maintaining operational continuity, and safeguarding organizational objectives.

In today's globalized business landscape, effective supply chain management (SCM) is essential for ensuring operational efficiency and meeting customer demands. However, supply chains are increasingly exposed to various risks that can disrupt operations and threaten business continuity. Integrating SCM into risk management practices is crucial for identifying, assessing, and mitigating these risks proactively. This report explores the importance of integrating SCM into risk management and provides strategies for organizations to enhance their resilience and mitigate supply chain risks effectively.

Supply chain disruptions can result from various factors such as natural disasters, geopolitical instability, supplier failures, and demand fluctuations. These disruptions can have significant consequences, including production delays, inventory shortages, increased costs, and reputational damage. Therefore, organizations need to integrate risk management practices into their SCM strategies to anticipate and mitigate potential threats

2. Importance of Integration:

01. **Comprehensive Risk Management:** Integrating SCRM into overall cybersecurity and ERM processes allows organizations to address supply chain risks holistically, considering both cyber threats and other risk factors.
02. **Enhanced Resilience:** By aligning SCRM with cybersecurity and ERM, organizations can build resilient supply chains capable of withstanding disruptions and adapting to changing threat landscapes.
03. **Streamlined Processes**: Integration streamlines risk management processes by eliminating silos and promoting cross-functional collaboration, leading to more efficient risk identification, assessment, and mitigation.
04. **Strategic Alignment**: Integrating SCRM with overall cybersecurity and ERM ensures alignment with organizational objectives, enabling informed decision-making and resource allocation.

3. Benefits of Integrating SCM into Risk Management:

01. **Enhanced Resilience**: Integrating SCM into risk management enables organizations to build resilient supply chains capable of withstanding disruptions and adapting to changing conditions.

    Improved Decision-Making: By incorporating risk management principles into SCM, organizations can make informed decisions about supplier selection, inventory management, and logistical strategies based on risk assessments.

02. **Cost Reduction**: Proactive risk management helps organizations identify cost-saving opportunities, such as optimizing inventory levels, reducing reliance on high-risk suppliers, and streamlining logistics processes.

    Safeguarding Reputation: Effective risk management in SCM minimizes the likelihood of supply chain disruptions, thereby protecting the organization's reputation and maintaining customer trust.

4. Strategies for Integrating SCM into Risk Management:

01. **Risk Identification**: Conduct comprehensive risk assessments to identify potential threats to the supply chain, including supplier vulnerabilities, geopolitical risks, natural disasters, and operational challenges.
02. **Risk Assessment**: Evaluate the likelihood and potential impact of identified risks on supply chain operations, financial performance, and strategic objectives.
03. **Risk Mitigation**: Develop risk mitigation strategies to address identified threats, such as diversifying supplier networks, implementing contingency plans, and investing in technology solutions for real-time monitoring.
04. **Collaboration and Communication**: Foster collaboration and communication among internal stakeholders, suppliers, and partners to share information, align risk management strategies, and respond effectively to disruptions.
05. **Scenario Planning**: Conduct scenario planning exercises to simulate various risk scenarios and assess the resilience of supply chain operations under different conditions. This enables organizations to develop contingency plans and build adaptive capabilities.
06. **Continuous Monitoring:** Establish robust monitoring mechanisms to track changes in risk profiles, emerging threats, and external factors that may influence the supply chain environment.
07. **Performance Measuremen**t: Define key performance indicators (KPIs) to measure the effectiveness of risk management initiatives and drive continuous improvement efforts across the supply chain.

Capabilities of Integrated Risk Management Platforms:

01. **Supply Chain Visibility**: Integrated risk management platforms offer visibility into supply chain networks, enabling organizations to map relationships, dependencies, and potential points of failure. This visibility allows stakeholders to identify and assess supply chain risks proactively.
02. **Risk Assessment and Quantification**: These platforms provide tools for conducting risk assessments and quantifying the impact of supply chain risks on business objectives. By analyzing the likelihood and potential consequences of disruptions, organizations can prioritize mitigation efforts effectively.
03. **Vendor Risk Management**: Integrated risk management platforms include features for managing vendor risks throughout the procurement lifecycle. Organizations can assess vendor cybersecurity posture, financial stability, and compliance with regulatory requirements to mitigate supply chain risks associated with third-party vendors.
04. **Incident Response and Continuity Planning**: In the event of supply chain disruptions, IRM platforms facilitate incident response and continuity planning. Stakeholders can collaborate in real-time to mitigate the impact of disruptions, activate contingency plans, and restore operations swiftly.
05. **Regulatory Compliance:** These platforms help organizations stay compliant with regulatory requirements related to supply chain risk management, such as data privacy regulations and industry standards. By automating compliance workflows and documentation, organizations can reduce the risk of non-compliance penalties.
06. **Analytics and Reporting:** Integrated risk management platforms offer advanced analytics and reporting capabilities, allowing organizations to analyze trends, identify patterns, and visualize supply chain risks effectively. Stakeholders can generate customized reports and dashboards to communicate risk insights to senior management and board members.

Integrated Risk Management Platforms:

01. **Scalability**: Ensure that the platform can scale to accommodate the organization's growing risk management needs and evolving supply chain complexities.
02. **Interoperability**: Choose a platform that integrates seamlessly with existing systems and data sources, enabling smooth data exchange and collaboration across departments.
03. **Customization**: Look for platforms that offer customization options to tailor risk management processes and workflows to the organization's unique requirements and industry-specific challenges.
04. **Usability**: Prioritize platforms with intuitive interfaces and user-friendly features to facilitate adoption and engagement among stakeholders across the organization.
05. **Security**: Verify that the platform adheres to industry best practices for data security and privacy, including encryption, access controls, and compliance certifications.

Cybersecurity clauses:

01. **Compliance with Cybersecurity Standards**: A clause requiring third parties to comply with VIT's cybersecurity standards and policies, including specific requirements related to data protection, access controls, and incident response.

02. **Data Protection and Privacy**: Provisions outlining how third parties will protect VIT's data, including requirements for encryption, data storage, and data access

Conclusion:

Integrating SCM into risk management is essential for organizations to build resilient supply chains capable of withstanding disruptions and delivering value to customers consistently. By adopting proactive risk management practices, organizations can enhance their competitiveness, protect their reputation, and ensure long-term sustainability in today's dynamic business environment. It is imperative for organizations to prioritize the integration of SCM into risk management to mitigate supply chain risks effectively and achieve operational excellence.

By integrating SCM into risk management, organizations can enhance their ability to anticipate, mitigate, and recover from supply chain disruptions, thereby safeguarding their competitive advantage, ensuring customer satisfaction, and fostering long-term sustainability in an increasingly volatile and uncertain business landscape.

GV.SC-04 (VIT IT Infrastructure Guidelines Report - Identify and prioritize suppliers by criticality to the organization.)

1. Introduction

To fortify VIT's cybersecurity supply chain risk management strategies. This report outlines key tasks in identifying and prioritizing suppliers by criticality to the organization, as well as implementing supplier risk assessment tools for effective evaluation and ranking based on criticality and risk.

Identifying and Prioritizing Suppliers:

01. **Define criticality factors:** Identify key criteria such as the importance of the supplied goods/services, access to sensitive data, and potential impact on university operations.
02. **Inventory suppliers:** Compile a comprehensive list of suppliers and categorize them based on criticality factors.
03. **Prioritization process:** Develop a systematic approach to prioritize suppliers, considering their criticality to the organization.

Supplier Risk Assessment Tools:

01. **Selection criteria:** Evaluate and choose appropriate supplier risk assessment tools based on their compatibility with university systems, comprehensiveness, ease of use, and cost-effectiveness.
02. **Implementation plan:** Outline steps to integrate selected tools into existing procurement and supplier management processes.
03. **Training and awareness:** Provide training sessions and resources to relevant staff members on how to effectively utilize the chosen assessment tools.
04. **Continuous improvement:** Establish mechanisms for regular reviews and updates to the supplier risk assessment process to adapt to evolving threats and organizational changes.

Critical Vendors of the Organisation

01. **Software Vendors:** Companies or organizations that provide software solutions used by the university for administrative purposes (e.g., enterprise resource planning systems), academic purposes (e.g., learning management systems), or research purposes (e.g., data analysis software).
02. **Hardware Suppliers:** Manufacturers or distributors of hardware components and devices used within the university's IT infrastructure, including servers, networking equipment, computers, and peripherals.

03. **Cloud Service Providers:** Companies that offer cloud-based services for storing data, hosting applications, or delivering computing resources. This includes providers of cloud storage, cloud computing platforms, and software-as-a-service (SaaS) applications.
04. **Third-party Service Providers:** External vendors or contractors that offer specialized services to the university, such as managed IT services, cybersecurity consulting, data management, or outsourced administrative functions.
05. **Educational Technology Providers:** Suppliers of educational technology solutions used for teaching, learning, and research purposes, including e-learning platforms, online courseware, virtual labs, and educational software applications.
06. **Physical Security Providers:** Companies that supply physical security systems and services, such as access control systems, surveillance cameras, alarm systems, and security personnel services.
07. **Telecommunications Providers:** Providers of telecommunications services, including internet service providers (ISPs), telecommunications carriers, and vendors of voice communication systems.

Identifying and prioritizing suppliers based on criticality to the organization, followed by evaluating and ranking them using risk assessment criteria:

01. Software Vendors:
   a. **Criticality:** High, as software solutions are integral to administrative, academic, and research functions.
   b. **Risk Assessment Criteria:** Data security measures, vulnerability management, software update frequency.
   c. **Ranking:** Vendor A (strong security measures, regular updates), Vendor B (adequate security but infrequent updates), Vendor C (lacks comprehensive security measures).

02. Hardware Suppliers:
   a. **Criticality:** High, as hardware components form the foundation of the university's IT infrastructure.
   b. **Risk Assessment Criteria:** Hardware integrity, firmware security, supply chain transparency.
   c. **Ranking:** Vendor X (trusted brand with transparent supply chain), Vendor Y (reliable hardware but limited transparency), Vendor Z (unknown reputation and supply chain).

03. Cloud Service Providers:
   a. **Criticality:** High, as cloud services store sensitive university data and host critical applications.
   b. **Risk Assessment Criteria:** Data encryption, compliance certifications, incident response capabilities.
   c. **Ranking:** Provider P (compliant with industry standards, strong encryption), Provider Q (certified but lacks robust incident response), Provider R (insufficient encryption and compliance measures).

04. Third-party Service Providers:

a. **Criticality:** Medium to High, depending on the services provided and access to university systems.
b. **Risk Assessment Criteria:** Access controls, data handling practices, contractual obligations.
c. **Ranking:** Provider M (clear contractual terms, stringent access controls), Provider N (limited access controls, unclear data handling practices), Provider O (inadequate contractual protections).

05. Educational Technology Providers:

a. **Criticality:** Medium to High, as educational technology supports teaching and learning activities.
b. **Risk Assessment Criteria:** Data privacy features, integration capabilities, vendor reputation.
c. **Ranking:** Provider S (strong data privacy features, seamless integration), Provider T (limited integration capabilities, mixed reputation), Provider U (lacks essential data privacy features, unknown reputation).

06. Physical Security Providers:

a. **Criticality:** Medium, as physical security complements digital security measures.
b. **Risk Assessment Criteria:** Physical access controls, surveillance system integrity, personnel training.
c. **Ranking:** Provider V (robust access controls, reliable surveillance systems), Provider W (adequate controls but outdated surveillance technology), Provider X (limited access controls and training protocols).

07. Telecommunications Providers:

a. **Criticality:** Medium, as telecommunications services support communication and data transmission.
b. **Risk Assessment Criteria:** Network security measures, uptime reliability, compliance with privacy regulations.
c. **Ranking:** Provider D (strong network security, reliable uptime), Provider E (adequate security but occasional downtime issues), Provider F (lacks comprehensive security measures, compliance concerns).

GV.SC-05 (VIT IT Infrastructure Guidelines Report - Develop and integrate cybersecurity risk requirements into contracts and agreements with third parties.)

1. Introduction

The VIT IT Infrastructure Guidelines Report focuses on the critical task of developing and integrating cybersecurity risk requirements into contracts and agreements with third parties. This report emphasizes the importance of ensuring that all external partners, suppliers, and service providers adhere to the highest cybersecurity standards, protecting the integrity and security of VIT's IT infrastructure.

2. Develop and integrate cybersecurity risk requirements:

01. **Assessment of Cybersecurity Risks**: Conduct a thorough assessment of cybersecurity risks associated with the specific third-party engagement. Identify potential vulnerabilities and threats that could impact VIT's IT infrastructure.
02. **Define Cybersecurity Requirements**: Based on the risk assessment, define clear and specific cybersecurity requirements that third parties must adhere to. This may include requirements for data protection, access controls, encryption, and incident response.
03. **Incorporate Requirements into Contracts**: Integrate the cybersecurity requirements into contracts and agreements with third parties. Clearly outline the expectations and responsibilities regarding cybersecurity in the contract language.
04. **Review and Approval Process**: Establish a review and approval process for contracts to ensure that cybersecurity requirements are met. This may involve collaboration between legal, IT, and cybersecurity teams.

Contract management software:

01. **Centralized Storage:** These tools provide a centralized repository for contracts, making it easier to manage and access all contract-related documents. This ensures that cybersecurity requirements are documented and easily accessible.
02. **Template Management:** Contract management software often includes template libraries for standard contract types. This can help ensure that cybersecurity requirements are included in all relevant contracts by incorporating them into standard templates.
03. **Automated Workflows:** These tools often offer automated workflows for contract approval and execution. Cybersecurity requirements can be included as part of these workflows, ensuring that they are reviewed and approved before contracts are finalized.
04. **Compliance Tracking:** Contract management software can track compliance with cybersecurity requirements over time. It can alert stakeholders when requirements are not met or when contracts need to be updated to reflect new cybersecurity standards.

05. **Reporting and Analytics:** These tools provide reporting and analytics capabilities that can help identify trends related to cybersecurity risk management in contracts. This information can be used to improve cybersecurity risk management practices over time.

Cybersecurity clauses:

01. **Compliance with Cybersecurity Standards:** A clause requiring third parties to comply with VIT's cybersecurity standards and policies, including specific requirements related to data protection, access controls, and incident response.
02. **Data Protection and Privacy:** Provisions outlining how third parties will protect VIT's data, including requirements for encryption, data storage, and data access.
03. **Incident Response and Reporting:** Requirements for third parties to promptly report cybersecurity incidents to VIT and to cooperate in the investigation and remediation of such incidents.

Develop and integrate cybersecurity risk requirements into contracts and agreements with third parties to ensure cybersecurity clauses are included and managed effectively:

01. Risk Assessment and Requirement Identification:
   a. Conduct a comprehensive risk assessment to identify cybersecurity risks associated with the engagement of third parties.
   b. Define specific cybersecurity risk requirements based on the identified risks, considering factors such as data sensitivity, access controls, and compliance requirements.

02. Clause Development:
   a. Develop clear and concise cybersecurity clauses that outline the cybersecurity risk requirements for third parties.
   b. Include clauses related to data protection, incident response, compliance, breach notification, liability, and insurance, as previously discussed.

03. Contract Template Creation:
   a. Create contract templates that include standard cybersecurity clauses for use in all contracts and agreements with third parties.
   b. Ensure that these templates are easily accessible and up-to-date with current cybersecurity standards and regulations.

04. Integration into Contracts:
   a. Integrate the cybersecurity clauses into all contracts and agreements with third parties.
   b. Ensure that the language is specific and legally enforceable, clearly outlining the rights and responsibilities of each party regarding cybersecurity.

05. Contract Review and Approval:
   a. Establish a review and approval process for contracts to ensure that cybersecurity clauses are included and meet the organization's standards.

b. Involve legal, IT, and cybersecurity teams in the review process to ensure comprehensive coverage of cybersecurity requirements.

06. Contract Management Software Utilization:

a. Use contract management software to store and manage contracts, ensuring that cybersecurity clauses are included and tracked effectively.
b. Leverage the software's features for template management and compliance tracking to streamline the integration process.

07. Monitoring and Enforcement:

a. Establish mechanisms for monitoring and enforcing compliance with cybersecurity clauses.
b. Regularly audit and assess third parties' adherence to cybersecurity requirements and take appropriate action in case of non-compliance.

08. Continuous Improvement:

a. Continuously review and update cybersecurity clauses and requirements based on evolving threats and best practices.
b. Incorporate lessons learned from cybersecurity incidents and breaches into the development and management of cybersecurity clauses.

Conclusion:

In conclusion, developing and integrating cybersecurity risk requirements into contracts and agreements with third parties is essential for ensuring the security and integrity of VIT's IT infrastructure. By following the guidelines outlined in this report, VIT can effectively manage cybersecurity risks associated with third-party engagements and protect against potential threats. The use of contract management software, clear and concise cybersecurity clauses, and a robust review and approval process can help ensure that cybersecurity requirements are included and managed effectively in contracts. Continuous monitoring, enforcement, and improvement of cybersecurity clauses are crucial for maintaining compliance with cybersecurity standards and mitigating risks over time. By implementing these recommendations, VIT can enhance its cybersecurity posture and protect its IT infrastructure from cyber threats.

GV.SC-06 (VIT IT Infrastructure Guidelines Report - Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.)

1. Introduction

The "VIT IT Infrastructure Guidelines Report" seems to prioritize planning and due diligence when engaging with suppliers or third-party entities. This approach is essential for reducing risks associated with these relationships. By conducting thorough planning and due diligence, potential pitfalls can be identified and mitigated early on, ensuring smoother partnerships and minimizing disruptions to IT infrastructure.

Certainly, here are some detailed points that the VIT IT Infrastructure Guidelines Report might include regarding planning and due diligence before entering into formal supplier or other third-party relationships:

2. Risk Assessment:

01. Identify and assess potential risks associated with engaging with a new supplier or third party.
02. Evaluate the impact of these risks on VIT's IT infrastructure, operations, and objectives.

3. Supplier Evaluation Criteria:

01. Define specific criteria for evaluating potential suppliers or third parties.
02. Consider factors such as reputation, experience, financial stability, technical capabilities, and adherence to industry standards.

4. Legal and Compliance Review:

01. Ensure that suppliers or third parties comply with relevant legal and regulatory requirements, including data protection laws, intellectual property rights, and contractual obligations.
02. Review contracts and agreements carefully to clarify responsibilities, liabilities, and dispute resolution mechanisms.

5. Security Assessment:

01. Assess the security measures and protocols implemented by suppliers or third parties to protect sensitive data and information.
02. Verify compliance with cybersecurity standards and best practices to mitigate the risk of data breaches or cyber attacks.

6. Performance and Reliability:

01. Evaluate the performance history and reliability of potential suppliers or third parties through references, case studies, or performance metrics.
02. Determine the supplier's ability to meet VIT's requirements in terms of service levels, uptime, and responsiveness.

7. Cultural Fit and Compatibility:

01. Assess the cultural fit between VIT and potential suppliers or third parties, considering factors such as communication style, corporate values, and organizational culture.
02. Ensure compatibility with VIT's IT infrastructure, systems, and processes to facilitate seamless integration and collaboration.

8. Financial Due Diligence:

01. Conduct financial due diligence to assess the financial health and stability of potential suppliers or third parties.
02. Evaluate factors such as profitability, liquidity, debt levels, and creditworthiness to minimize the risk of business disruptions due to financial instability.

9. Contingency Planning:

01. Develop contingency plans to address potential risks and disruptions associated with supplier or third-party relationships.
02. Identify alternative suppliers or mitigation strategies to minimize the impact of unforeseen events or failures.

Conclusion :

By incorporating these detailed points into the planning and due diligence process, VIT can make well-informed decisions when entering into formal relationships with suppliers or other third parties, thereby reducing risks and maximizing the potential for successful collaborations.

GV.SC-07 (The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.)

1. Executive Summary:

In today's interconnected business environment, the risks associated with suppliers, their products and services, and other third parties have become a significant concern for organizations. This report focuses on the identification, recording, prioritization, assessment, response, and monitoring of these risks over the course of a relationship.

2. Introduction:

Organizations are increasingly reliant on external entities, including suppliers and third-party vendors, for products, services, and support. While these relationships offer numerous benefits, they also introduce cybersecurity risks that must be effectively managed to protect the organization's assets, reputation, and operations.

3. Identification of Risks:

01. Sources of Risks:

a. **Supplier Vulnerabilities:** Weak cybersecurity practices, outdated systems, and lack of security awareness.
b. **Product/Service Flaws:** Software vulnerabilities, insecure configurations, and inadequate security controls.
c. **Third-party Risks:** Data breaches, unauthorized access, and non-compliance with security standards.

02. Methods of Identification:

a. Regular security assessments and audits.
b. Vendor questionnaires and security reviews.
c. Monitoring threat intelligence feeds for information related to suppliers and third parties.

4. Recording and Documentation:

Maintaining a comprehensive record of identified risks is crucial for accountability and informed decision-making. This includes:

01. Detailed descriptions of each identified risk.
02. Relevant supporting evidence.
03. Risk owners and stakeholders.

5. Prioritization and Assessment:

Not all risks have the same impact or likelihood. Therefore, a risk prioritization process should be established to focus resources on the most critical risks. Factors to consider include:

01. Potential impact on business operations, data integrity, and confidentiality.
02. Likelihood of occurrence.
03. Regulatory and compliance implications.

6. Response Strategies:

Based on the prioritized risks, appropriate response strategies should be developed and implemented. This may include:

01. Mitigation measures to reduce the risk.
02. Acceptance of the risk with informed decision-making.
03. Termination or modification of the relationship with the supplier or third party.

7. Monitoring and Review:

Continuous monitoring of the risks associated with suppliers, products, services, and third parties is essential to ensure that controls remain effective and new risks are promptly identified and addressed. This involves:

01. Regular security assessments and audits.
02. Ongoing communication and collaboration with suppliers and third parties.
03. Periodic review and update of risk assessments and response strategies.

8. Benefits of Effective Third-Party Risk Management

By implementing a robust third-party risk management program, organizations can achieve several key benefits:

01. Reduced Risk of Cyber Attacks: Proactive identification and mitigation of third-party risks can significantly reduce the overall threat landscape.
02. Enhanced Data Security: By ensuring that third parties have appropriate security controls in place, organizations can better protect their sensitive data.
03. Improved Business Continuity: A comprehensive understanding of third-party risks enables organizations to develop contingency plans to minimize disruptions in the event of a security incident involving a third party.
04. Compliance with Regulations: Many industries have regulations that require organizations to manage third-party risks. A well-defined program can help ensure compliance with these regulations.

Conclusion:

Managing cybersecurity risks associated with suppliers, their products and services, and other third parties requires a proactive and systematic approach. By identifying, recording, prioritizing, assessing, responding to, and monitoring these risks throughout the relationship lifecycle, organizations can effectively mitigate potential threats and safeguard their assets.

Recommendations:

01. Establish a formalized risk management process specifically tailored to suppliers and third-party relationships.
02. Implement regular security assessments and audits for suppliers and third parties.
03. Foster open communication and collaboration with suppliers and third parties to promote a shared understanding of cybersecurity risks and responsibilities.

GV.SC-08 (VIT IT Infrastructure Guidelines Report -Relevant suppliers and other third parties are included in incident planning, response, and recovery activities)

1. Introduction

To fortify VIT's cybersecurity supply chain risk management strategies. This report outlines key tasks in identifying and prioritizing suppliers by criticality to the organization, as well as implementing supplier risk assessment tools for effective evaluation and ranking based on criticality and risk.

Relevant suppliers:

01. Software Vendors:

a. Companies or organizations that provide software solutions used by the university for administrative purposes (e.g., enterprise resource planning systems), academic purposes (e.g., learning management systems), or research purposes (e.g., data analysis software).

02. Hardware Suppliers:

a. Manufacturers or distributors of hardware components and devices used within the university's IT infrastructure, including servers, networking equipment, computers, and peripherals.

03. Cloud Service Providers:

a. Companies that offer cloud-based services for storing data, hosting applications, or delivering computing resources. This includes providers of cloud storage, cloud computing platforms, and software-as-a-service (SaaS) applications.

04. Third-party Service Providers:

a. External vendors or contractors that offer specialized services to the university, such as managed IT services, cybersecurity consulting, data management, or outsourced administrative functions.

05. Educational Technology Providers:

a. Suppliers of educational technology solutions used for teaching, learning, and research purposes, including e-learning platforms, online courseware, virtual labs, and educational software applications.

06. Physical Security Providers:

a. Companies that supply physical security systems and services, such as access control systems, surveillance cameras, alarm systems, and security personnel services.

07. Telecommunications Providers:

a. Providers of telecommunications services, including internet service providers (ISPs), telecommunications carriers, and vendors of voice communication systems.

Incorporating relevant suppliers and other third parties into the incident planning, response, and recovery activities of an engineering college is crucial for ensuring robust preparedness against various emergencies or disruptions. This approach not only enhances the college's resilience but also ensures that critical services and supplies can be maintained during and after an incident. Here's how you might consider integrating these external entities:

1. Identify Critical Suppliers and Third Parties Technology Vendors:

For hardware, software, and IT infrastructure crucial for educational and administrative functions.

01. **Utility Providers:** Electricity, water, and other utilities must be included to manage outages effectively.
02. **Contracted Security and Maintenance:** Ensuring safety and operational integrity of the college premises.
03. **Communication Providers:** Essential for maintaining communication channels during an incident**.**
04. **Suppliers of Laboratory Equipment and Materials:** Important in engineering colleges for the continuity of practical and research work.

2. Develop Relationships and Communication Plans

01. **Regular Meetings and Updates:** Hold meetings to discuss roles, responsibilities, and expectations during an incident.
02. **Contact Lists:** Maintain updated lists of key contacts who need to be reached during an emergency.
03. **Mutual Understanding of Capabilities and Limitations:** Understand what each party can realistically provide during various types of incidents.

3. Integrate into Incident Response Plans

01. **Specific Roles and Responsibilities:** Clearly define what each supplier and third party is expected to do during different types of emergencies.
02. **Joint Training Sessions:** Include third parties in drills and training sessions to ensure everyone knows their roles and can function effectively under pressure.
03. **Access and Credentialing:** Plan for how external personnel will access the campus during an incident if necessary.

4. Contractual Agreements and SLAs

01. **Service Level Agreements (SLAs):** Define the expected service levels from third parties, including response times and priority during emergencies.
02. **Contracts:** Ensure contracts have clauses that specify the expected involvement and readiness for emergencies.

5. Review and Update Incident Plans Regularly

01. **Feedback Mechanisms:** After drills or actual incidents, gather feedback to identify any gaps or areas for improvement. This involves all stakeholders, including suppliers and third parties, in the review process.
02. **Update Plans:** Regularly revisit and update emergency plans and SLAs based on new risks, past incident learnings, or changes in the operational environment or in the services provided by third parties.
03. **Continuity Exercises:** Schedule regular continuity exercises that involve critical suppliers and third parties to ensure that the processes, roles, and communication channels are effective and known to all involved.

6. Legal and Compliance Considerations

01. **Compliance Requirements:** Ensure all plans and activities comply with local laws and regulations. This includes understanding and incorporating requirements specific to various types of incidents, such as chemical spills in labs or data breaches in IT systems.
02. **Data Privacy and Security:** Carefully manage how sensitive information is handled, particularly during IT-related incidents, ensuring that all third-party actions conform to data protection regulations.
03. **Insurance:**Review insurance policies to confirm coverage includes scenarios involving third parties and the specific types of incidents that may impact the college.

7. Technology and Data Sharing

01. **Shared Platforms:** Utilize technology platforms that can be accessed mutually for real-time updates and information sharing during an incident. This could include incident management software or a dedicated communication channel.
02. **Backup and Redundancy Plans:** Ensure that critical third-party services have robust backup and redundancy strategies in place to mitigate risks associated with service interruptions.
03. **Cybersecurity Measures:** Include cybersecurity best practices and requirements in the integration of third-party services, especially those that handle or store sensitive college data.

8. Public Relations and Communication Coordination

01. **Unified Communication Strategy:**Coordinate with third parties on how to communicate during crises to present a united and organized front to students, parents, the media, and the public.
02. **Crisis Communication Teams:** Form teams that include representatives from the college and critical third parties to handle communication during incidents. Ensure these teams are trained and prepared to respond promptly and effectively.

03. **Information Accuracy:** Develop a protocol to ensure that all communicated information is accurate and consistent, thereby avoiding confusion and misinformation during sensitive situations.

By methodically integrating these strategies, an engineering college can build a comprehensive incident management framework that includes critical suppliers and third parties. This integration not only enhances the resilience of the college in facing emergencies but also ensures that all partners are ready and able to perform their roles efficiently during critical times, thereby minimizing impact and speeding up recovery.

GV.SC-09 (Supply Chain Security Report: VIT Bhopal)

1. Executive Summary

This report provides an overview of the integration and performance monitoring of supply chain security practices at VIT Bhopal, emphasizing the crucial roles these practices play within the broader scope of cybersecurity and enterprise risk management. Given the increased dependencies on digital technologies and the potential vulnerabilities within supply chains, VIT Bhopal recognizes the necessity to develop a robust framework that ensures the security and integrity of its technology products and services throughout their lifecycle.

2. Introduction

Supply chain security is a critical aspect of overall cybersecurity strategy, particularly for educational institutions like VIT Bhopal that rely on a myriad of technology solutions for administrative functions, academic activities, and infrastructure management. The risks associated with supply chain disruptions, malicious software injections, unauthorized data access, and compromised hardware must be systematically addressed.

3. Objectives

01. **Risk Identification:** To identify and categorize risks associated with the supply chain in technology acquisition and deployment.
02. **Integration into Risk Management:** To integrate these risks into the existing enterprise risk management framework effectively.
03. **Performance Monitoring:** To establish protocols for continuous monitoring of the security practices throughout the product and service life cycles.

4. Context and Current State at VIT Bhopal

VIT Bhopal is an institution that employs a range of technological products and services, sourced from various vendors. These include educational platforms, administrative software, digital communication tools, and network infrastructure components. The inherent risk in this diverse supply chain landscape necessitates a comprehensive approach to security.

Current Practices:

01. **Vendor Assessment:** Preliminary security assessments during the vendor selection process.
02. **Contractual Obligations:** Inclusion of security requirements in contracts with suppliers.

03. **Regular Audits:** Periodic security audits of supplied systems and services**.**

Implementation Strategy for Improved Supply Chain Security

1. Governance

01. Establish a dedicated supply chain security management team.
02. Develop governance frameworks that align with international standards like ISO 28000 (Specification for security management systems for the supply chain).

2. Risk Management Integration

01. Implement a framework for continuous risk assessment specific to supply chain vulnerabilities.
02. Integrate supply chain risk data into the overarching enterprise risk management program using tools like GRC (Governance, Risk Management, and Compliance) software.

3. Security Requirements

01. Standardize security requirements across all vendor contracts, with stipulations for compliance, audit rights, and breach notifications.
02. Employ the use of Secure Development Lifecycle (SDL) practices to ensure security is integrated at every phase of acquisition and deployment.

4. Monitoring and Reporting

01. Utilize continuous monitoring tools to track and report on supply chain integrity and security.
02. Implement a supplier scorecard system to evaluate and rate vendors on their security practices regularly.

5. Education and Awareness

01. Train procurement teams on the importance of cybersecurity in vendor selection and management.
02. Hold regular workshops for staff and stakeholders on the latest trends in supply chain threats and mitigation strategies.

Performance Metrics

01. **Incident Response Time:** Measure the time taken to respond to supply chain-related security incidents.

02. **Vendor Compliance Rates:** Track and report the percentage of vendors complying with security requirements.
03. **Audit Findings Closure:** Monitor the rate at which identified vulnerabilities during audits are mitigated.

Conclusion

Integrating robust supply chain security practices within the cybersecurity and enterprise risk management frameworks is not only essential for protecting VIT Bhopal's assets but also ensures the continuity and reliability of its educational services. By implementing the strategies outlined above, VIT Bhopal can enhance its resilience against supply chain disruptions and cyber threats, safeguarding its reputation and operational capabilities.

Recommendations

01. Immediate Implementation of GRC Integration: This will ensure that supply chain risks are visible within the broader risk management strategy.
02. Continuous Improvement: Supply chain security is a dynamic field; ongoing adjustments and improvements based on new threats and vulnerabilities are crucial.

This strategy and these recommendations aim to support VIT Bhopal in its mission to provide a secure and efficient educational environment through robust supply chain security practices.

GV.SC-10 (Cybersecurity Supply Chain Risk Management Plans - Activities that occur after the Conclusion of a Partnership or Service Agreement)

1. Introduction

In today's interconnected digital landscape, organizations rely heavily on third-party vendors and suppliers to support their operations and deliver products and services efficiently. However, this dependence introduces significant cybersecurity risks, as these external entities can inadvertently expose organizations to threats such as data breaches, supply chain attacks, and other cyber incidents. To effectively mitigate these risks and safeguard their assets, organizations must implement robust Cybersecurity Supply Chain Risk Management (GV.SC) plans.

GV.SC plans are strategic frameworks designed to identify, assess, and mitigate cybersecurity risks associated with the acquisition and integration of third-party products, services, and technologies within an organization's IT infrastructure. By proactively addressing potential vulnerabilities and threats throughout the supply chain, these plans enable organizations to maintain the integrity, confidentiality, and availability of their critical assets while fostering trust and resilience in their business operations.

In this guide, we will delve into the key components of Cybersecurity Supply Chain Risk Management plans, explore best practices for implementing effective risk management strategies, and discuss the importance of collaboration, transparency, and continuous monitoring in safeguarding against emerging threats. Through a proactive and comprehensive approach to GV.SC, organizations can strengthen their security posture, protect their valuable assets, and mitigate the impact of cyber threats originating from the supply chain ecosystem.

2. Cybersecurity Supply Chain Risk Management Plans

Cybersecurity supply chain risk management plans are comprehensive strategies designed to identify, assess, and mitigate risks associated with the acquisition and integration of third-party products, services, and technologies within an organization's IT infrastructure. These plans typically include the following components:

01. **Risk Assessment:** Conducting thorough assessments of potential risks associated with third-party suppliers, including evaluating their security practices, compliance with industry standards, and potential vulnerabilities.
02. **Vendor Selection and Due Diligence:** Implementing robust vendor selection processes that include due diligence activities to ensure that selected vendors meet cybersecurity requirements and standards.
03. **Contractual Obligations:** Incorporating cybersecurity requirements into contractual agreements with vendors, including provisions for security audits, incident response procedures, and compliance monitoring.

04. **Continuous Monitoring:** Establishing mechanisms for ongoing monitoring of vendor performance and security posture throughout the duration of the partnership or service agreement.
05. **Incident Response Planning:** Developing and maintaining incident response plans that outline procedures for responding to cybersecurity incidents involving third-party suppliers, including communication protocols and escalation procedures.
06. **Supply Chain Transparency:** Promoting transparency within the supply chain by encouraging vendors to disclose information about their security practices, supply chain dependencies, and potential risks.
07. **Training and Awareness:** Providing training and awareness programs for employees involved in vendor management and procurement to ensure that they understand the importance of cybersecurity in the supply chain.
08. **Resilience and Contingency Planning:** Developing resilience and contingency plans to minimize the impact of cybersecurity incidents involving third-party suppliers on the organization's operations and reputation.

By implementing these measures, organizations can effectively manage cybersecurity risks within their supply chains and mitigate potential threats posed by third-party vendors and suppliers.

Activities that occur after the Conclusion of a Partnership or Service Agreement Cybersecurity supply chain risk management plans often include provisions for post-partnership or service agreement activities to ensure ongoing security. These plans extend beyond the initial partnership or service agreement. This could involve:

01. **Continual Monitoring:** Regularly monitoring the partner's or service provider's systems and practices to detect any emerging risks or vulnerabilities.
02. **Incident Response:** Establishing protocols for how to respond to security incidents that may occur after the conclusion of the agreement, ensuring swift and effective action.
03. **Updating Policies:** Updating internal policies and procedures based on lessons learned from the partnership or service agreement, to strengthen future security measures.
04. **Contractual Obligations:** Ensuring that the contract includes provisions for ongoing security obligations, such as periodic audits or updates to security standards.
05. **Knowledge Transfer:** Facilitating the transfer of knowledge and best practices between the parties involved, even after the conclusion of the partnership, to maintain a strong security posture.
06. **Disengagement Planning:** Planning for a smooth disengagement process, including securely transferring any relevant data or assets back to the organization or to a new provider.
07. **Data deletion and disposal:** Ensure procedures are in place for the secure deletion or transfer of your organization's data stored by the supplier after the agreement ends.
08. **Vulnerability remediation:** Address any identified vulnerabilities within the supplier's systems that may have lingering effects on your organization's security posture.

09. **Access revocation:** Revoke any access rights granted to the supplier's personnel to your systems or data upon termination of the agreement.
10. **Audit trails:** Maintain audit logs to track data access and activity even after the agreement concludes. This can help identify and address any potential security incidents.

By incorporating these provisions, C-SCRM plans ensure ongoing protection even after a supplier relationship ends. These measures help mitigate risks associated with the termination of partnerships or service agreements, ensuring that cybersecurity remains a priority even after the formal relationship ends.

4. Conclusion

In conclusion, Cybersecurity Supply Chain Risk Management (GV.SC) plans are essential for organizations to mitigate the inherent risks associated with third-party partnerships and service agreements. By implementing robust GV.SC strategies, organizations can identify, assess, and address potential vulnerabilities throughout the supply chain, safeguarding their critical assets and maintaining operational resilience.

Furthermore, the inclusion of provisions for activities that occur after the conclusion of a partnership or service agreement is crucial for sustaining cybersecurity posture over time. Post-agreement activities, such as continuous monitoring, incident response planning, and knowledge transfer, ensure that security remains a priority even after formal relationships end. By proactively addressing potential risks and vulnerabilities, organizations can minimize the impact of cyber threats originating from the supply chain ecosystem.

In today's dynamic and interconnected business environment, effective GV.SC plans are essential for protecting against emerging cyber threats and maintaining trust and confidence among stakeholders. By leveraging best practices, standards, and frameworks, organizations can enhance their ability to detect, prevent, and respond to cybersecurity incidents, ultimately strengthening their overall security posture and resilience in the face of evolving threats.

GV.RR-01 (Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving)

1. Introduction

The digital age has brought immense opportunities for organizations of all sizes. However, the ever-expanding reliance on technology has also exposed organizations to a growing number of cyber threats. Cybersecurity breaches can have devastating consequences, causing financial losses, reputational damage, and disruption of operations.

Mitigating these risks requires a comprehensive approach that goes beyond technical solutions. A critical factor in building a robust cybersecurity posture is strong leadership commitment. Effective cybersecurity leadership fosters accountability, performance assessment, and continuous improvement within the organization.

This report explores the critical role of leadership in establishing a culture of cybersecurity awareness and responsibility. It outlines ten key solutions that leaders can implement to create a more secure environment and empower staff and students to contribute to effective cybersecurity practices.

2. The Importance of Leadership in Cybersecurity

Cybersecurity is not simply a technical challenge; it is a cultural imperative. Technical tools and firewalls play a crucial role, but they are ultimately only as effective as the human element. Leaders set the tone from the top, influencing the behavior and attitudes of staff and students towards cybersecurity.

2.1 Setting the Tone

Strong leadership communication is essential for establishing cybersecurity as a core organizational value. When leaders clearly articulate the importance of cybersecurity and demonstrate a personal commitment to its success, it sends a powerful message throughout the organization.

This leadership commitment can be demonstrated through:

01. Public statements: Leaders can emphasize the importance of cybersecurity in public pronouncements, such as company town halls, student orientations, or annual reports.
02. Active participation: Leaders can demonstrate their commitment by actively participating in cybersecurity initiatives, such as attending training sessions or championing security awareness campaigns.
03. Resource allocation: Leaders can prioritize cybersecurity by allocating adequate financial and human resources towards security programs and personnel.

2.2 Building a Culture of Shared Responsibility

By setting the tone, leaders can foster a culture of shared responsibility for cybersecurity. This approach acknowledges that everyone in the organization, regardless of their role, plays a part in maintaining a secure environment.

3. Key Solutions for Leadership in Cybersecurity

This report explores ten key solutions that leaders can implement to foster a strong cybersecurity program:

Establishing Policies and Procedures: Comprehensive cybersecurity policies outline expectations for user behavior and system access. These policies should address data protection, access controls, incident response, and compliance with relevant regulations such as GDPR, HIPAA, or industry-specific standards. Regular reviews ensure policies remain current with evolving threats and regulations.

01. **Allocating Resources:** Sufficient budgetary allocations, dedicated personnel, and investments in security technologies are crucial for effective cybersecurity. This includes funding for tools, hiring security professionals, and training programs.
02. **Promoting a Culture of Awareness and Security:** Regular training sessions, awareness campaigns, and communication efforts educate staff and students about cyber threats and best practices for staying secure online. This ongoing process fosters a shared responsibility for cybersecurity.
03. **Ethical Standards:** Leadership establishes clear ethical guidelines for cybersecurity practices. This emphasizes integrity, confidentiality, and respect for privacy, ensuring appropriate handling of sensitive data and incident response.
04. **Risk Assessment and Management:** Regular risk assessments identify potential vulnerabilities and threats to the organization's digital infrastructure. Leadership oversees the development and implementation of risk management strategies to mitigate these risks effectively.
05. **Incident Response Planning:** Comprehensive incident response plans guide the organization's response to a cybersecurity breach. These plans define protocols for detection, containment, mitigation, reporting, and communication with stakeholders in the event of an incident.
06. **Education and Training:** Providing ongoing education and training programs equips staff and students with the knowledge and skills to fulfill their cybersecurity roles. Training should cover password security, phishing awareness, safe browsing habits, and incident reporting procedures.
07. **Investment in Technology:** Adequate resources are allocated to acquire and maintain essential cybersecurity technologies. These tools may include intrusion detection systems, antivirus software, firewalls, encryption tools, and security analytics platforms.
08. **Continuous Improvement:** Cybersecurity is a continuous process. Leadership fosters a culture of continuous improvement by regularly reviewing and updating policies,

procedures, and technologies. This ensures adaptation to emerging threats, evolving technologies, and lessons learned from past incidents.

09. **Accountability:** Leadership establishes clear lines of responsibility and accountability for cybersecurity practices. This ensures that individuals understand their roles and are held accountable for their actions in maintaining the institution's cybersecurity posture.

5. Recommendations

This report provides a foundation for leaders to build a robust cybersecurity program. However, it is important to acknowledge that every organization has unique needs and risk profiles. Leaders should consider the following recommendations for tailoring these solutions

01. **Conduct a Cybersecurity Maturity Assessment:** Before implementing specific solutions, an assessment can identify the organization's current cybersecurity posture. This assessment will help prioritize areas for improvement and tailor solutions to address the most critical needs.
02. **Develop a Cybersecurity Strategy:** Based on the assessment findings, leadership can develop a comprehensive cybersecurity strategy that outlines specific goals, objectives, and action plans. This strategy should align with the organization's overall goals and risk tolerance.
03. **Establish a Cybersecurity Team:** Dedicated cybersecurity personnel are essential for developing, implementing, and maintaining a strong cybersecurity program. This team may consist of in-house professionals, outsourced services, or a combination of both.
04. **Promote Collaboration:** Cybersecurity is not solely the responsibility of the IT department. Leaders should encourage collaboration between IT, security personnel, management teams, and staff to ensure everyone plays a role in maintaining security.
05. **Measure and Monitor Performance:** Effective cybersecurity requires continuous monitoring and analysis. Leaders should establish metrics to track the effectiveness of cybersecurity controls and identify areas for improvement. This may involve key performance indicators (KPIs) related to security incidents, user behavior, and system vulnerabilities.
06. **Stay Informed:** The cybersecurity landscape is constantly evolving. Leaders and security teams should remain current on emerging threats, best practices, and regulatory changes. This can be achieved through participation in industry conferences, workshops, and professional development opportunities.
07. **Embrace a Culture of Learning:** Building a strong cybersecurity posture requires a commitment to continuous learning. Leaders should encourage staff and students to participate in ongoing security awareness training and educational programs. This fosters a proactive approach to cybersecurity across the organization.

6. Conclusion

By implementing these recommendations and solutions, leaders can play a critical role in fostering a culture of cybersecurity accountability. A leadership commitment to building a strong cybersecurity program empowers staff and students to contribute to a secure environment. This collaborative approach is essential for protecting valuable assets, minimizing risks, and ensuring the organization's continued success in the digital age.

GV.RR-02 (Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced)

1. Introduction

The digital age presents immense opportunities for universities, facilitating research, education, and collaboration on a global scale. However, this growing reliance on technology also exposes universities to a significant risk: cyber threats. Data breaches, malware attacks, and unauthorized access can have devastating consequences, causing financial losses, reputational damage, and disruption of critical operations.

Mitigating these risks requires a comprehensive cybersecurity strategy that extends beyond technical solutions. A critical element in building a robust cybersecurity posture is establishing a well-defined cybersecurity governance framework. This framework outlines clear roles, responsibilities, and authorities (GV.RR-02) for various stakeholders within the university. This report examines the case study of VIT University (VIT), showcasing how a well-defined framework fosters a culture of accountability in information security management.

2. Importance of Defined Roles and Responsibilities

In the absence of clear roles and responsibilities, cybersecurity efforts can become fragmented and ineffective. When everyone understands their specific duties and ownership in information security, several key benefits are realized:

01. **Clarity and Ownership:** Clearly defined roles eliminate confusion about who is accountable for what aspect of cybersecurity. This empowers individuals to take ownership of their security duties, fostering a sense of personal responsibility for protecting university data and systems.
02. **Accountability:** Defined responsibilities ensure everyone is held accountable for their actions related to information security. This promotes a culture of security awareness and diligence, encouraging individuals to prioritize secure practices.
03. **Collaboration:** A well-defined framework helps break down silos between IT and non-IT personnel. When everyone understands their roles and how they contribute to the overall security posture, collaboration improves. Collaborative efforts lead to more comprehensive security measures being implemented across the university.
04. **Risk Management:** By assigning specific responsibilities for risk assessment, the framework encourages proactive identification and mitigation of potential security threats. This allows the university to prioritize resources effectively and address vulnerabilities before they can be exploited.
05. **Compliance:** Clearly defined roles help ensure compliance with relevant laws, regulations, and university policies related to information security. This helps the university maintain a defensible legal position in the event of a security incident.

3. VIT's Cybersecurity Governance Structure

VIT's approach to cybersecurity governance outlines distinct roles and responsibilities for both IT and non-IT personnel. This fosters shared responsibility and ensures everyone contributes to creating a secure environment.

3.1 IT Roles

01. **Vice President and Chief Information Officer (CIO):** The CIO holds the highest level of authority and responsibility for the university's IT infrastructure, security, and service provision. They are responsible for:
    a. Coordinating the information security program to ensure risk management within the university's acceptable tolerance levels.
    b. Acting as the executive sponsor for the university's IT governance process, which includes information security.
    c. Allocating resources necessary to effectively execute the information security program.
    d. Overseeing the implementation of IT systems that support information security goals and processes.
    e. Maintaining a list of key university leadership personnel responsible for information security.
02. **Chief Information Security Officer (CISO):** The CISO leads the university's information security program and reports directly to the CIO. They are also designated as the Information Security Manager (ISM) and are responsible for administering the information security program, policies, and procedures. Key responsibilities of the CISO include:
    a. Creation, maintenance, and oversight of the university's information security program, encompassing information security policies, a robust security awareness program, an information security risk management program, incident detection and response protocols, and compliance with relevant laws, regulations, and contracts regarding information security.
03. **Director/Manager of IT:** These individuals serve as senior IT leaders for their respective colleges or major university units. They report to the CIO and are responsible for:
    a. Management, oversight, and security of all IT activities within their scope.
    b. Coordinating the use and provision of IT services and infrastructure with the Office of the Vice President and Chief Information Officer. This includes ensuring alignment with university-wide policies, even for services and infrastructure not managed by the enterprise or directly contracted by the university.
    c. Supervising Information Security Managers within their unit to ensure effective implementation of the risk management program.
    d. Designating staff within their unit to carry out IT and information security responsibilities within sub-units of the college or administrative unit.
    e. Providing reports on Key Performance Indicators (KPIs) to the College Dean/Administrative Unit Vice President and other leadership personnel. These

reports facilitate understanding of the effectiveness of the information security program within the unit and identify areas for improvement.

04. **Information Security Manager (ISM):** ISMs typically hold technical leadership positions within their units and report to the Director/Manager of IT. They are responsible for
    a. Assessing and mitigating risks using the university-approved process. This involves identifying potential vulnerabilities, analyzing the likelihood and impact of threats, and implementing appropriate controls to address them.
    b. Immediately notifying the UF Computer Security Incident Response Team (CSIRT) of high-severity incidents and responding appropriately to low-severity incidents. This ensures a timely and coordinated response to security breaches.
    c. Verifying that information systems under their control, and those intended for acquisition or development by their unit, comply with authentication management requirements. Strong authentication controls are essential for preventing unauthorized access to university systems.
    d. Implementing information systems such that account authorizations are promptly enforced. This ensures that only authorized users have access to specific systems and data.
    e. Implementing backup systems and processes to ensure that Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) can be met for all data collected, stored, or maintained on unit information systems. RTO and RPO define the acceptable timeframes for restoring access and data in the event of an outage or incident.
    f. Documenting backup system operations and testing recovery capabilities. This ensures the university can restore critical systems and data efficiently in the event of a disruption.
    g. Documenting and implementing controls for all remote access methods implemented within their unit. ISMs are also responsible for monitoring these methods for unauthorized use and taking appropriate action upon discovery, which may include notification of the UF CSIRT.
    h. Monitoring and reviewing audit logs to identify and respond to inappropriate or unusual activity. Audit logs record user activity within systems, providing valuable insights into potential security incidents.
    i. Creating and maintaining procedures and documentation to secure data centers, server rooms, and telecommunication facilities. Physical security of IT infrastructure is crucial for protecting against unauthorized access.
    j. Overseeing system security within their unit. This includes implementing technical controls such as firewalls, intrusion detection systems, and data encryption to protect university data and systems.
    k. Establishing unit procedures to document and control configurations and maintenance. This ensures that system configurations are documented and changes are controlled to minimize the risk of introducing vulnerabilities.

3.2 Non-IT Roles

01. **UF Senior Leadership:** This position refers to the senior leader of a college or university administrative unit, such as deans, vice presidents, or directors reporting directly to the Provost. They are responsible for:
    a. Designating a Director/Manager of IT, Information Security Manager (ISM), and Information Security Administrator (ISA) within their unit. They are also responsible for informing the Office of the Vice President and Chief Information Officer of these designations.
    b. Reviewing Key Performance Indicators (KPIs) of the unit's information security program. This helps assess the effectiveness of security controls and identify areas for improvement.
    c. Providing guidance to the Director/Manager of IT, ISM, and ISA on how the unit's security posture aligns with both the unit's and the university's risk tolerance levels. This ensures alignment between individual units and the overall cybersecurity strategy.
    d. Providing direction to the Director/Manager of IT on the unit's IT needs. This ensures that IT resources are allocated to support the unit's operations while maintaining security considerations.
    e. Providing direction to the ISM and ISA on the unit's risk management strategy and tolerance. This allows for tailored risk management approaches within each unit while adhering to university-wide risk tolerance levels.
    f. Making final decisions on risk treatment. This involves selecting appropriate mitigation strategies for identified security risks.
02. **Information Security Administrator (ISA):** These individuals typically hold administrative leadership positions within their units. They are responsible for ensuring that the ISM and IT staff have
    a. Appropriate support and resources to properly secure data and information systems, and
    b. Implement university information security policies.

The scope of the ISA's responsibility encompasses information systems managed by the unit as well as third-party services procured by the unit. Specific responsibilities include, but are not limited to

Ensuring processes are in place to facilitate:

01. Risk assessments on information systems using the university-approved process.
02. Procedures to properly authorize, modify, or terminate accounts and permissions. This ensures that only authorized individuals have access to specific systems and data.
03. Establishment of RTO and RPO in conjunction with data users and owners for all data used within the unit. Verification that appropriate backup plans are implemented. This ensures timely recovery of critical data in the event of an incident.

04. Procedures to respond to inappropriate or unusual activity on unit information systems. This allows for swift detection and response to potential security breaches.
05. Procedures to protect electronic media. This includes measures such as data encryption and secure.
06. Procedures for training users to recognize and report information security incidents. Educating users about potential threats and how to report suspicious activity is crucial for early detection and response to security breaches.
07. Procedures for the protection of unit workplaces and computing devices. This may involve physical security measures, such as locking down workstations, and data security measures, such as enforcing strong password policies.
08. Provision of appropriate facilities for unit servers, network, and telecommunications equipment. This ensures a secure environment for critical IT infrastructure.
09. Development, maintenance, exercise, and training of unit contingency plans. Contingency plans outline procedures for responding to various disruptive events, including cyberattacks.
10. Ensuring appropriate resources are maintained to uphold system security. This encompasses both technical resources, such as security software, and human resources with the necessary skills to manage security effectively.
11. All Members of the University Community: All faculty, staff, students, volunteers, and other affiliates have a responsibility to participate in the university's information security program. This includes:
12. Working collaboratively with unit IT staff and Information Security Leadership (ISM and ISA) to address information security concerns. This fosters a culture of open communication and shared responsibility for security.
13. Participating in the risk assessment process if needed, before implementing or upgrading information technology. This allows users to provide valuable insights into potential security risks associated with new technologies.
14. Faculty and staff should make accommodations to use pre-vetted applications and systems whenever possible. This reduces the risk of introducing vulnerabilities through the use of unauthorized or unapproved software.

Responsibilities of all members of the university community include:

01. Completing the annual security awareness training and understanding their role in securing university data and information systems. This ongoing education is essential for keeping users informed about the latest threats and best practices for secure behavior.
02. Complying with the Acceptable Use Policy (AUP). The AUP outlines acceptable and unacceptable uses of university IT resources and helps promote responsible behavior among users.
03. Using university-approved applications and systems to perform university work. This ensures that users are working within a secure environment with appropriate security controls in place.

4. Benefits of Defined Roles and Responsibilities

VIT's approach to cybersecurity governance offers a number of benefits that contribute to a more secure environment:

01. **Clarity and Ownership:** Clear roles and responsibilities eliminate confusion about who is accountable for what aspect of cybersecurity. This empowers individuals to take ownership of their security duties and fosters a sense of personal responsibility.
02. **Accountability:** Defined responsibilities ensure everyone is held accountable for their actions related to information security. This promotes a culture of security awareness and diligence, encouraging individuals to prioritize secure practices.
03. **Collaboration:** The framework fosters collaboration between IT and non-IT personnel. When everyone understands their roles and how they contribute to the overall security posture, collaboration improves. Collaborative efforts lead to more comprehensive security measures being implemented across the university.
04. **Risk Management:** By assigning specific responsibilities for risk assessment, the framework encourages proactive identification and mitigation of potential security threats. This allows the university to prioritize resources effectively and address vulnerabilities before they can be exploited.
05. **Compliance:** Clearly defined roles help ensure compliance with relevant laws, regulations, and university policies related to information security. This helps the university maintain a defensible legal position in the event of a security incident.

5. Recommendations for Further Improvement

While VIT's approach provides a strong foundation, continuous improvement is essential in cybersecurity. Here are some recommendations for further enhancement:

01. **Regular communication:** Regular communication between IT leadership, security personnel, and university members can ensure everyone remains informed about evolving threats and security protocols. This can be achieved through various channels, such as email newsletters, security awareness campaigns, and town hall meetings.
02. **Performance measurement:** Implementing metrics to track the effectiveness of security controls and user behavior can identify areas needing improvement. These metrics may include the number of security incidents reported, the percentage of users who complete security awareness training, and the time it takes to resolve security incidents.
03. **Ongoing training:** Regular security awareness training programs can educate the university community about emerging threats and best practices for secure behavior. These programs should be tailored to different user groups, such as faculty, staff, and students, to ensure that These programs should be tailored to different user groups, such as faculty, staff, and students, to ensure the information is relevant and engaging. Additionally, incorporating phishing simulations and other interactive exercises can help users develop practical skills for identifying and responding to security threats.
04. **Incident response testing:** Regularly testing incident response plans ensures the university is prepared to effectively respond to security breaches. These tests can identify

gaps in the plan, communication breakdowns, and areas where response times can be improved.

05. **Penetration testing:** Periodic penetration testing by qualified security professionals can help identify vulnerabilities in university systems and networks that attackers may exploit. These tests should be conducted on a regular basis and address evolving security threats.
06. **Sharing best practices:** VIT can share its experiences and best practices with other universities. This can be achieved through participation in industry conferences, workshops, and collaboration with other institutions facing similar challenges.
07. **Investing in security awareness tools:** Implementing user-friendly tools can simplify security practices for the university community. These tools may include password managers, multi-factor authentication systems, and data encryption tools. By providing user-friendly options, the university can encourage adoption of secure practices without hindering productivity.
08. **Empowering security champions:** Identifying and empowering security champions within different units can promote a culture of security at the grassroots level. These champions can act as liaisons between users and IT security teams, helping to raise awareness, answer questions, and provide feedback on security initiatives.

6. Conclusion

In today's digital age, a robust cybersecurity posture is essential for universities to protect their valuable data, systems, and reputation. By fostering a culture of accountability through clearly defined roles and responsibilities, VIT University demonstrates a successful approach to information security management. By continuously refining their framework and incorporating best practices, VIT can ensure a secure environment for the university community well into the future.

GV.RR-03 (Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies)

1. Introduction

The digital landscape presents immense opportunities for universities, facilitating research, education, and collaboration on a global scale. However, this growing reliance on technology exposes universities to a significant risk: cyber threats. Data breaches, malware attacks, and unauthorized access can have devastating consequences, causing financial losses, reputational damage, and disruption of critical operations.

Effectively mitigating these risks requires a comprehensive cybersecurity strategy that extends beyond technical solutions. A critical element is ensuring adequate resources are allocated commensurate with the cybersecurity risk strategy, roles and responsibilities, and policies (GV.RR-03). This report examines the case study of VIT University (VIT), showcasing how strategic resource allocation strengthens the university's cybersecurity posture.

2. Importance of Strategic Resource Allocation

Cybersecurity is an ongoing process, requiring continuous investment in personnel, technology, training, and compliance measures. Strategic resource allocation ensures that VIT can:

01. **Address Identified Risks:** By aligning budget allocation with the risk assessment findings, the university can prioritize resources to mitigate the most critical vulnerabilities.
02. **Empower Personnel:** Adequate staffing with skilled cybersecurity professionals allows VIT to effectively manage and implement security measures.
03. **Leverage Technology:** Investing in appropriate cybersecurity technologies provides essential tools for threat detection, prevention, and response.
04. **Maintain Compliance:** Allocating resources for compliance audits and certifications ensures VIT adheres to relevant regulations and best practices.
05. **Foster a Culture of Security:** Investing in training and awareness programs educates the university community about cybersecurity, promoting responsible behavior.

3. VIT's Approach to Resource Allocation

VIT's approach to cybersecurity resource allocation encompasses several key areas:

01. **Budget Allocation:** A dedicated cybersecurity budget is established based on the university's risk assessment. This budget considers not only initial investments but also ongoing maintenance costs for personnel, technology, and training. The budget is flexible to accommodate emerging threats and technological advancements.
02. **Personnel Resources:** VIT employs skilled cybersecurity professionals with clearly defined roles and responsibilities. This team may include cybersecurity analysts, incident

responders, network security specialists, and compliance officers. Regular training ensures the team stays updated with the latest trends and technologies.

03. **Technology Investments:** VIT invests in cybersecurity technologies aligned with its risk assessment and security strategy. Firewalls, intrusion detection and prevention systems (IDPS), endpoint security solutions, encryption technologies, and Security Information and Event Management (SIEM) systems are examples of technologies that may be employed. Regular updates and patches are applied to maintain their effectiveness.
04. **Training and Education:** VIT offers cybersecurity awareness training programs, workshops, seminars, and professional development opportunities for staff and students. This education empowers individuals to understand their roles in maintaining a secure environment and identify and respond to potential threats.
05. **Compliance and Audit Costs:** Resources are allocated for compliance assessments, audits, and certifications. This ensures VIT remains compliant with relevant cybersecurity regulations, standards, and best practices. Regular audits identify areas for improvement and validate the effectiveness of implemented security measures.

4. Benefits of Strategic Resource Allocation

VIT's strategic resource allocation approach offers several benefits:

01. **Enhanced Security Posture:** By allocating resources to address identified risks, VIT strengthens its overall security posture and reduces the likelihood of successful cyberattacks.
02. **Improved Efficiency:** Strategic allocation ensures resources are directed towards the most critical areas, maximizing their impact and avoiding unnecessary expenditures.
03. **Compliance Adherence:** Allocating resources for compliance activities helps VIT maintain adherence to relevant regulations and industry best practices.
04. **Empowered Workforce:** Investing in training empowers staff and students to contribute to the university's cybersecurity efforts through informed decision-making and secure practices.
05. **Proactive Approach:** Strategic resource allocation allows VIT to take a proactive approach to cybersecurity, addressing threats before they can cause harm.

6. Recommendations for Further Improvement

While VIT's approach provides a strong foundation, continuous improvement is essential in cybersecurity. Here are some recommendations for further enhancement:

01. **Cost-benefit analysis:** Implementing cost-benefit analyses for potential cybersecurity investments can help prioritize resource allocation decisions.
02. **Metrics and measurement:** Developing metrics to track the effectiveness of cybersecurity controls and resource utilization can provide valuable insights for future resource allocation strategies.
03. **Collaboration with stakeholders:** Collaborating with university leadership to communicate cybersecurity risks and resource needs can garner broader support for ongoing investment.

04. **Sharing best practices:** VIT can share its experiences and best practices with other universities through industry conferences and collaboration initiatives.

By continuously refining their resource allocation approach, VIT can ensure optimal utilization of resources and maintain a robust cybersecurity posture in the face of evolving threats.

7. Conclusion

In today's digital age, a strategic approach to resource allocation is essential for universities to effectively manage cybersecurity risks. VIT University's commitment to allocating resources commensurate with its cybersecurity strategy, roles and responsibilities, and policies serves as a model for other institutions. By continuously improving their approach and fostering collaboration with stakeholders, VIT can ensure a secure environment for its academic and research endeavors well into the future.

8. Appendix: Potential Cost Considerations for Cybersecurity Resource Allocation

This section provides a non-exhaustive list of potential cost considerations for universities like VIT when allocating resources for cybersecurity:

01. **Personnel:** Salaries and benefits for cybersecurity professionals, including analysts, incident responders, network security specialists, and compliance officers.
02. **Technology:** Acquisition costs for firewalls, IDPS systems, endpoint security solutions, encryption software, SIEM systems, and vulnerability management tools. Additionally, ongoing maintenance and licensing fees for these technologies.
03. **Training and Education:** Development and delivery of cybersecurity awareness training programs, workshops, and professional development opportunities for staff and students.
04. **Compliance and Audits:** Costs associated with external audits, penetration testing, and certifications for compliance with relevant cybersecurity regulations and standards.
05. **Security Awareness Tools:** Implementing user-friendly tools such as password managers, multi-factor authentication systems, and data encryption tools can incur costs associated with licensing or development.

9. Call to Action

Universities face an ever-growing challenge in protecting their digital assets from cyber threats. VIT University's approach to resource allocation offers valuable insights for other institutions seeking to strengthen their cybersecurity posture. By adopting a strategic approach that aligns resource allocation with risk assessments, roles, and responsibilities, universities can create a more secure and resilient learning environment for the digital age.

GV.RR-04 (Cybersecurity is included in human resources practices)

1. Introduction

The digital landscape presents universities with a double-edged sword. On one hand, technology fuels innovation, facilitates research collaboration, and enhances the learning experience. On the other hand, it exposes universities to a growing threat: cyberattacks. Data breaches, malware infections, and unauthorized access can have devastating consequences, causing financial losses, reputational damage, and disruption of critical operations.

Effectively mitigating these risks requires a comprehensive cybersecurity strategy that extends beyond technical solutions. A crucial element is integrating cybersecurity into human resources (HR) practices, as outlined in NIST Special Publication 800-161 Revision 1 (GV.RR-04). This report examines Vellore Institute of Technology's (VIT) approach to integrating cybersecurity into HR practices, showcasing how this fosters a culture of security awareness and empowers personnel to contribute to safeguarding the university's digital assets.

2. The Cybersecurity Threat Landscape for Universities

Universities house a wealth of sensitive information, including student records, research data, intellectual property, and financial data. This makes them prime targets for cybercriminals seeking financial gain, sensitive information, or to disrupt academic activities. Here's a closer look at some of the most common cybersecurity threats universities face:

01. **Phishing Attacks:** These deceptive emails or messages attempt to trick recipients into revealing personal information, clicking on malicious links, or downloading malware. Phishing attacks are a major threat because they exploit human error and can bypass even the most sophisticated technical controls.
02. **Malware Attacks:** Malicious software, such as viruses, ransomware, and spyware, can infect university systems, disrupt operations, steal data, or hold it hostage for ransom.
03. **Data Breaches:** Unauthorized access to university systems can result in the exposure of sensitive data. Data breaches can have severe legal and financial ramifications, erode trust with students, faculty, and staff, and damage the university's reputation.
04. **Denial-of-Service (DoS) Attacks:** These attacks overwhelm university systems with traffic, rendering them unavailable to legitimate users. DoS attacks can disrupt critical services such as online registration, course delivery, and administrative functions.
05. **Advanced Persistent Threats (APTs):** These sophisticated attacks involve attackers gaining long-term, unauthorized access to a university's network to steal data or disrupt operations. APTs are often targeted and difficult to detect.

3. The Importance of Integrating Cybersecurity into HR Practices

Integrating cybersecurity into HR practices offers several key benefits for universities like VIT:

01. **Enhanced Security Posture:** By educating and empowering employees, human error becomes a less significant contributor to cybersecurity incidents. This reduces the university's overall vulnerability.
02. **Culture of Security Awareness:** Integrating cybersecurity into HR practices fosters a culture where security is seen as a shared responsibility. Employees become more vigilant and understand their role in protecting university data and systems.
03. **Reduced Risk of Incidents:** Security-conscious employees are less likely to fall victim to phishing attacks or engage in risky behaviors that could compromise the university's security.
04. **Compliance Adherence:** Integrating cybersecurity into HR practices helps ensure that the university adheres to relevant regulations and best practices regarding information security.
05. **Proactive Approach:** By emphasizing cybersecurity from the outset, VIT can instill secure habits in employees early on, reducing the need for corrective actions later.

4. VIT's Comprehensive Approach to Integrating Cybersecurity into HR Practices

VIT implements a multi-faceted approach to integrate cybersecurity into its HR practices, fostering a culture of security awareness and empowering its workforce:

4.1 Cybersecurity Awareness Training:

VIT collaborates with IT and cybersecurity departments to develop comprehensive training programs tailored to different employee groups. These programs address evolving threats, best practices for:

01. Password management (using strong passwords, avoiding password reuse, and employing multi-factor authentication)
02. Data classification and handling (identifying sensitive data, understanding appropriate storage and access controls)
03. Responsible technology use (avoiding unauthorized software downloads, being cautious about opening attachments and clicking on links in emails)
04. Recognizing and reporting phishing attempts (identifying suspicious emails, verifying sender addresses, reporting suspicious activity)
05. Training is provided to all staff, including new hires and existing employees. Cybersecurity training is a mandatory component of the onboarding process for new employees. Regular refresher training sessions ensure that everyone remains informed about the latest threats and best practices.

4.2 Security Policies and Procedures:

VIT maintains a well-defined set of cybersecurity policies and procedures that all employees are expected to understand and follow. These policies cover essential aspects such as:

01. Acceptable Use Policy (AUP) outlining authorized and prohibited uses of university IT resources

02. Password policy mandating strong password creation and regular password changes
03. Data classification and handling procedures specifying how sensitive data should be stored, accessed, and transmitted
04. Incident reporting protocols outlining procedures for reporting suspected security incidents
05. BYOD (Bring Your Own Device) policy, if applicable, addressing security considerations for personal devices used on the university network VIT ensures that all employees are familiar with these policies through various means, such as incorporating them into the onboarding process, making them readily available on the university intranet, and organizing awareness campaigns.

4.3 Role-based Access Controls (RBAC):

VIT collaborates with the IT department to implement RBAC. This ensures that employees only have access to the systems, data, and applications necessary for their job roles. The principle of least privilege is followed, granting the minimum level of access required for employees to perform their duties effectively. Regular reviews and updates of access permissions are conducted to ensure alignment with changes in employee roles or departures from the organization.

4.4 Security Awareness Campaigns:

VIT recognizes that ongoing reinforcement is essential for maintaining a culture of security awareness. The university supports ongoing security awareness campaigns to keep cybersecurity at the forefront of employees' minds. These campaigns may include:

01. Distributing informative materials such as posters, flyers, and email newsletters with security tips and reminders
02. Organizing security awareness events, workshops, and webinars featuring cybersecurity experts
03. Encouraging participation in training sessions and knowledge-sharing initiatives
04. Utilizing internal communication channels to share security updates and best practices

4.5 Incident Response and Reporting:

VIT understands the importance of timely and effective response to security incidents. The university has established clear procedures for reporting security incidents or concerns. These procedures include:

01. Specifying appropriate reporting channels, such as designated IT security personnel, departmental supervisors, or a dedicated incident reporting hotline
02. Outlining investigation processes, ensuring a thorough examination of the incident to determine the root cause and identify necessary remediation steps
03. Establishing clear communication protocols to keep relevant stakeholders informed throughout the response process

04. Fostering a supportive environment where employees feel comfortable reporting incidents without fear of reprisal. This may involve offering anonymity for reporting or providing training on how to report incidents effectively.

4.6 Security-minded Recruitment and Selection:

VIT recognizes that a security-conscious workforce starts with the recruitment process. The university prioritizes cybersecurity awareness and skills during recruitment, particularly for positions with access to sensitive information or IT/data management responsibilities. Here's how VIT integrates cybersecurity into recruitment:

01. Incorporating cybersecurity-related questions into job descriptions to assess a candidate's understanding of security best practices
02. During interviews, asking questions about a candidate's experience with data security, password management, and identifying phishing attempts
03. Prioritizing candidates who demonstrate a commitment to cybersecurity and a willingness to adhere to university security policies

5. Benefits of VIT's Approach

VIT's comprehensive approach to integrating cybersecurity into HR practices offers several significant benefits:

01. **Empowered Workforce:** Employees are equipped with the knowledge and skills to make informed decisions regarding cybersecurity. This fosters a sense of ownership and shared responsibility for protecting the university's digital assets.
02. **Reduced Human Error:** By emphasizing security awareness and responsible behavior, the likelihood of human error leading to security incidents is minimized. Security-conscious employees are less likely to fall victim to phishing attacks or engage in risky behaviors that could compromise the university's security.
03. **Improved Compliance:** Integrating cybersecurity into HR practices helps VIT meet its compliance obligations regarding information security. Clearly defined policies, ongoing training, and incident reporting procedures demonstrate the university's commitment to data security and adherence to relevant regulations.
04. **Proactive Risk Management:** By fostering a culture of security awareness, VIT can proactively address potential cybersecurity threats before they escalate into incidents. Early detection and response can minimize the impact of security breaches and ensure business continuity.
05. **Enhanced Reputation:** A strong cybersecurity posture enhances VIT's reputation as a secure and trustworthy institution. This can be beneficial for attracting students, faculty, research partners, and potential donors.

6. Recommendations for Further Improvement

While VIT's approach provides a strong foundation, continuous improvement is essential in cybersecurity. Here are some recommendations for further enhancement:

01. **Gamification:** Incorporating gamification elements into cybersecurity training can make it more engaging and interactive, leading to better knowledge retention. Gamified training modules can utilize points, badges, and leaderboards Gamified training modules can utilize points, badges, and leaderboards to create a more competitive and engaging learning experience. This can be particularly effective for younger generations of employees who are accustomed to interactive learning environments.
02. **Phishing Simulations:** Regular phishing simulations can help employees identify and avoid suspicious emails, a common tactic used by cybercriminals. These simulations can be tailored to mimic real-world phishing attempts, allowing employees to practice spotting red flags and reporting them appropriately. Over time, phishing simulations can hone employees' ability to discern legitimate emails from malicious ones.
03. **Security Champions:** Identifying and empowering security champions within different departments can be a valuable strategy. Security champions can act as liaisons between employees and IT security teams. They can answer questions, provide peer-to-peer support, and promote security awareness initiatives within their departments.
04. **Metrics and Measurement:** Developing metrics and measurement frameworks can provide valuable insights into the effectiveness of cybersecurity awareness programs. Tracking metrics such as employee participation in training, phishing simulation results, and reported security incidents can help identify areas for improvement and demonstrate the return on investment (ROI) of cybersecurity awareness initiatives.
05. **Continuous Monitoring and Awareness Campaigns:** The cybersecurity threat landscape is constantly evolving. Therefore, ongoing monitoring of emerging threats and tailoring awareness campaigns to address them is crucial. VIT can leverage threat intelligence feeds, industry reports, and security conferences to stay informed about the latest cyber threats and vulnerabilities. By keeping employees updated on these evolving threats, VIT can ensure they remain vigilant and prepared.

7. Conclusion

VIT University's approach to integrating cybersecurity into HR practices serves as a model for other institutions seeking to strengthen their cybersecurity posture. By prioritizing security awareness, empowering employees, and fostering a culture of shared responsibility, VIT creates a more secure learning and research environment. This comprehensive approach not only mitigates cybersecurity risks but also fosters trust and transparency within the university community.

8. Call to Action

In the digital age, cybersecurity is no longer an IT concern; it's a shared responsibility. Universities like VIT that prioritize integrating cybersecurity into HR practices demonstrate a proactive commitment to safeguarding their digital assets and fostering a culture of security awareness. By adopting similar strategies, universities can empower their workforce to become active participants in protecting their institutions from cyber threats.

GV.PO-01 (Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced)

Introduction

The VIT IT Policy - 2023 serves as a cornerstone for maintaining a secure and responsible Information Technology (IT) environment within the VIT community. This report delves into the intricacies of the policy, outlining its key components, procedures, and best practices for cybersecurity. By adhering to these guidelines, faculty, students, staff, and administrators can ensure the safe and ethical use of VIT's IT resources.

Applicability

The VIT IT Policy encompasses all technology administered by the institution, including:

01. Centrally managed systems like servers, network infrastructure, and core applications.
02. Departmental IT resources specific to individual departments or colleges.
03. Personally owned devices connected to the VIT network, ensuring responsible use within the network environment.
04. Information services provided by VIT administration, encompassing various online resources and portals.
05. Resources administered by central departments like libraries, computer centers, laboratories, offices, hostels, and guest houses, where network access is facilitated by VIT.

This comprehensive scope emphasizes the importance of responsible IT practices across all facets of the VIT community.

Policy Framework

The VIT IT Policy is structured around several key policy groups, each addressing a specific aspect of IT usage:

01. **Acceptable Use Policy (AUP):** Defines appropriate and ethical use of VIT's IT resources. This includes restrictions on illegal activities, copyright infringement, and activities that could compromise network security.
02. **Hardware and Software Procurement Policy:** Establishes guidelines for acquiring hardware and software. This policy might outline approval processes, vendor selection criteria, minimum security standards for procured equipment, and proper licensing requirements.

03. **IT Hardware Installation Policy:** Defines procedures for installing new hardware on the VIT network. This includes compatibility checks, configuration guidelines, documentation requirements, and proper disposal procedures for old equipment.
04. **Software Installation and Licensing Policy:** Regulates the installation of software on VIT systems. This policy emphasizes the use of authorized and licensed software only, outlining procedures for requesting software installation, software updates, and maintaining proper licenses.
05. **Network (Intranet & Internet) Use Policy:** Defines acceptable use of the VIT network, including limitations on bandwidth usage, restrictions on peer-to-peer file sharing, guidelines for using online resources responsibly, and acceptable online communication practices.
06. **E-mail Account Use Policy:** Regulates the use of VIT email accounts. This policy might define appropriate email etiquette, email security practices, password complexity requirements, and responsible use of email attachments.
07. **Web Site Hosting Policy:** Establishes guidelines for hosting websites on VIT servers. This might include an approval process, website content restrictions, security protocols for website maintenance, and responsibilities of website owners.
08. **VIT Database Use Policy:** Defines access rights and usage guidelines for VIT databases. This policy might specify authorized users for accessing specific databases, the type of data permitted for retrieval, procedures for data export, and reporting requirements for database usage.

User Groups and Compliance

The VIT IT Policy applies to two distinct user groups:

01. **End Users:** This group encompasses faculty, students, senior administrators, officers, staff, and other authorized personnel within the VIT community.
02. **Network Administrators:** These individuals are responsible for managing and maintaining the VIT network infrastructure, ensuring its security and smooth operation.

Compliance with the VIT IT Policy is mandatory for all users. Violations of the policy may result in disciplinary action by VIT authorities, ranging from warnings to suspension of IT privileges. In cases of illegal activities, law enforcement agencies may become involved.

Procedures: Access Authorization

The policy outlines specific procedures for granting access to sensitive areas like the VIT Data Center:

01. **Pre-approval:** Access requires pre-approval via email from a dean, director, or department head who can vouch for the legitimacy of the access request.

02. **Review and Approval:** The Assistant Director, Systems, will review and approve the request.
03. **Access Granting:** Authorized staff/vendors will be allowed entry by a Data Center employee but will then have unescorted access within the facility.
04. **Logging:** Authorized personnel are responsible for logging in and out upon entering and exiting the Data Center.
05. **Visitor Policy:** Anyone who is not a Data Center employee, authorized staff member, or authorized vendor is considered a visitor. Visitors must be accompanied by a Data Center employee or authorized staff member at all times.

These procedures ensure controlled access to sensitive IT infrastructure, minimizing security risks.

Fig:1 GV.PO-01 FlowDiagram

Best Practices

The VIT IT Policy emphasizes various best practices for cybersecurity across different aspects of IT usage:

01. **User Accounts and Administration:** This section highlights the importance of unique and secure user accounts. Users are encouraged to maintain strong passwords, report any misconfigurations, and promptly inform the IT department about any suspicious activity

related to their accounts. Additionally, faculty members are expected to uphold the same standards for their accounts.

02. **General User Accounts:** This section defines acceptable use for general-purpose accounts assigned to faculty, students, and staff. Some key best practices include:
    a. Accessing accounts only for authorized purposes and following instructions from faculty or IT personnel.
    b. Refraining from installing unauthorized software or programs without prior permission from the IT department.
    c. Accepting and adhering to periodic policy updates and security protocols implemented by the IT department.
    d. Strictly avoiding using these accounts for social media or personal purposes that fall outside the scope of academic or professional activities at VIT.
    e. Abstaining from saving unauthorized or inappropriate images, files, or data on these accounts.
    f. Refraining from accessing unauthorized data using these accounts.
03. **Special User Accounts:** This section focuses on accounts with elevated privileges, typically granted for specific tasks or lab environments. Here are some best practices:
    a. Accessing these accounts only with prior permission from faculty or lab in-charges.
    b. Maintaining the utmost care and security for these accounts, as any misuse can have serious consequences.
    c. Keeping the credentials of these accounts secure by storing them with the lab in-charge and not sharing them with unauthorized individuals.
    d. Regularly changing passwords for these accounts to minimize the risk of unauthorized access.
04. **Physical Security:** This section emphasizes the importance of safeguarding IT equipment and resources from physical threats. Best practices include:
    a. Users and lab assistants actively monitoring the lab environment and its premises to deter potential security breaches.
    b. Maintaining functional CCTV cameras within labs and other critical IT areas for surveillance purposes.
    c. Lab in-charges ensuring proper security measures at the entrance and exit points of lab premises to control access.
    d. Lab in-charges keeping meticulous records of lab timings, equipment inventory, and access logs to identify any discrepancies or suspicious activities.
05. **Password Handling:** Strong and secure passwords are crucial for protecting user accounts and sensitive information. The policy recommends the following best practices:
    a. Maintaining a record of passwords for all accounts used within the VIT network. This record should be kept in a secure and confidential location.
    b. Implementing a policy of changing passwords for all accounts at regular intervals, following the specific guidelines outlined by the IT department.

    c. Avoiding the use of easily guessable passwords or personal information within passwords. Ideally, passwords should be a combination of uppercase and lowercase letters, numbers, and special characters.
    d. Refraining from sharing passwords with anyone, including colleagues or friends.
06. **User and Access Rights Assignment:** This section defines the roles and responsibilities related to user account management and access controls. Key points include:
    a. Administrator accounts are to be maintained solely by the IT department. These accounts should have the highest level of security protocols in place.
    b. IT administrators are responsible for implementing and enforcing security policies across the VIT network infrastructure.
    c. Administrators must conduct regular audits of all computers on the network to identify and address any potential security vulnerabilities.
    d. Access to information and information processing facilities should be granted based on the principle of least privilege and "need-to-know" basis. This means users will only be granted access to the information and systems they require to perform their designated tasks.
    e. Access rights for users should be reviewed and updated periodically to ensure continued compliance with the least privilege principle.
    f. The IT department should document clear procedures for user access management and communicate these procedures effectively to all users within the VIT community.
07. **Unauthorized Data:** This section prohibits the storage of unauthorized data on official VIT systems or websites. This includes:
    a. Personal documents unrelated to academic or professional activities at VIT.
    b. Presentations containing sensitive or confidential information not approved for public access.
    c. Multimedia files like music, movies, or games that are not relevant to authorized activities.
    d. By adhering to these best practices, users can significantly contribute to a more secure IT environment for the entire VIT community.

Conclusion

The VIT IT Policy - 2023 serves as a comprehensive framework for safeguarding the institution's IT infrastructure and protecting the data of its users. By outlining clear policies, procedures, and best practices, the policy empowers all members of the VIT community to take responsibility for cybersecurity. Through a collective effort of adhering to these guidelines and fostering a culture of cyber awareness, VIT can ensure a secure and reliable IT environment that supports academic excellence and innovation.

GV.PO-02 (Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission)

Introduction

The digital landscape of higher education institutions is constantly evolving, offering unparalleled opportunities for learning and collaboration. However, this interconnectedness also presents significant challenges in the realm of cybersecurity. As cyber threats become more sophisticated and prevalent, universities like VIT must prioritize data security and user privacy.

This report provides a detailed examination of VIT University's cybersecurity policies and procedures. It outlines the framework established to manage cybersecurity risks, the various mitigation strategies employed, and the communication channels adopted to foster stakeholder awareness.

Cybersecurity Threat Landscape

Understanding the ever-changing nature of cyber threats is crucial for establishing effective defense mechanisms. This report explores some of the most common threats encountered in the digital world:

01. **Denial-of-Service (DoS) Attacks:** These attacks overwhelm a network with excessive traffic, disrupting access to vital systems like online learning platforms, administrative portals, or email servers. Students and faculty may be unable to access critical resources, hindering academic activities.
02. **Malware:** Malicious software, often disguised as legitimate applications, can be installed on devices through various means. This can compromise data integrity, disrupt system functionality, and potentially lead to data breaches.
03. **Phishing and Spear Phishing:** Phishing attacks attempt to deceive users into revealing personal information or clicking on malicious links, often through fraudulent emails. Spear phishing attacks target specific individuals or groups within a university, making them more believable and potentially compromising sensitive information.
04. **Ransomware:** This type of malware encrypts a user's data, rendering it inaccessible. Attackers then demand a ransom payment in exchange for decryption, potentially jeopardizing critical academic or administrative data.
05. **SQL Injection (SQLI) Vulnerabilities:** Exploiting weaknesses in database security protocols, attackers can inject malicious code to gain unauthorized access to sensitive information stored within databases. This can lead to data breaches and compromise of student records, financial data, or intellectual property.
06. **Password Attacks:** These attacks attempt to gain unauthorized access to accounts by trying various password combinations. Weak or easily guessable passwords leave users vulnerable to brute-force attacks or dictionary attacks that systematically attempt different combinations.
07. **Eavesdropping Attacks:** Malicious actors intercept network traffic to steal sensitive information transmitted between users or devices. This can compromise login credentials, financial information, or confidential academic work.
08. **Birthday Attacks:** Based on the mathematical concept of the birthday paradox, this attack exploits the probability of collisions in hashing algorithms. While seemingly theoretical, it highlights the importance of using strong hashing techniques and complex passwords to mitigate risks.
09. **Dictionary and Brute-Force Attacks:** These attacks rely on automated tools to systematically attempt a large number of password combinations. Strong password policies with minimum length requirements and the use of special characters make these attacks significantly more difficult.
10. **Insider Threats:** Individuals with authorized access to university systems and data can pose a significant threat if they choose to misuse their privileges. Implementing access control measures and fostering a culture of cybersecurity awareness are crucial in mitigating this risk.
11. **Man-in-the-Middle (MITM) Attacks:** These attacks involve an attacker intercepting communication between two parties, allowing them to potentially steal information or

manipulate data in transit. Unsecured Wi-Fi networks often make users vulnerable to such attacks.

VIT's Cybersecurity Framework

Recognizing these threats, VIT University has adopted a comprehensive cybersecurity framework. This framework establishes a multi-pronged approach, encompassing the following key elements:

01. **Risk Assessment and Review Process:** An ongoing process of identifying, analyzing, and prioritizing potential cybersecurity risks based on the evolving threat landscape. This ensures that policies and procedures remain relevant and effective.
02. **Policy and Procedure Updates:** Regular reviews and updates of cybersecurity policies and procedures to reflect changes in technology, emerging threats, and best practices. This ensures the university stays abreast of the latest security measures.
03. **Prevention, Protection, and Mitigation Strategies:** A proactive approach that focuses on preventing attacks, minimizing vulnerabilities, and having effective plans in place to mitigate any potential damage caused by successful attacks. This includes:
04. **Secure Data Storage:** Implementing robust data storage practices with regular backups ensures vital information is protected even if a cyberattack occurs. Data encryption adds an extra layer of security.
05. **Access Control Lists and Firewalls:** These tools effectively limit access to authorized users and provide a crucial first line of defense against unauthorized intrusions into university networks.
06. **Policies for Secure Deployment, Maintenance, and Responsible Use:** Clearly defined policies outline proper procedures for deploying and maintaining university systems, as well as establishing standards for responsible use of technology resources by faculty, staff, and students.
07. **Communication Strategy:** A comprehensive strategy to ensure all stakeholders within the university community are aware of cybersecurity policies, procedures, and best practices. This includes:
08. **Internal Newsletters:** Disseminating regular newsletters with relevant articles, updates on the latest threats, advice on cybersecurity best practices, These newsletters can highlight successful security measures implemented or showcase case studies to illustrate the real-world consequences of cyberattacks. This helps raise awareness and encourage responsible behavior.
09. **Targeted Email Communications:** Sending targeted emails to specific stakeholder groups with urgent updates, reminders about password changes, or notifications of potential phishing attempts. This ensures timely communication of critical information.
10. **Regular Training Sessions:** Conducting customized training sessions for faculty, staff, and students. Faculty training might focus on identifying phishing attempts and securing online learning platforms, while staff training could address data handling procedures and secure access controls. Student training sessions can emphasize responsible password

management and safe online practices. Offering both in-person and online training options caters to diverse learning preferences and schedules.

11. **Dedicated Online Portals:** Establishing a dedicated section on the university website or intranet portal that serves as a central repository for cybersecurity resources.

This portal can house:

01. Links to relevant cybersecurity policies and procedures documents.
02. Educational materials and guides on best practices for securing passwords, avoiding phishing attacks, and using university technology responsibly.
03. Frequently Asked Questions (FAQs) to address common cybersecurity concerns.
04. Interactive features like forums or chat rooms to encourage open communication and knowledge sharing among stakeholders.
05. Enforcement Measures: Implementing mechanisms to ensure adherence to cybersecurity policies and procedures. These measures could include:
06. Mandatory cybersecurity training for all new faculty, staff, and students.
07. Periodic audits and reviews of user activity and access controls.
08. Disciplinary actions for violations of cybersecurity policies, depending on the severity of the offense.

Best Practices and User Awareness

VIT University recognizes that user awareness and adherence to best practices are crucial components of a robust cybersecurity posture. The report emphasizes the following key practices:

01. **Password Management:** Using strong passwords with a combination of uppercase and lowercase letters, numbers, and special characters is essential. Implementing two-factor authentication provides an additional layer of security. Regularly changing passwords and avoiding reuse across different accounts minimizes risks.
02. **Email Security:** Being cautious about opening attachments or clicking on links in unsolicited emails, especially those that appear suspicious or out of the ordinary. Verifying sender legitimacy and hovering over links before clicking helps identify potential phishing attempts.
03. **Software Updates:** Regularly updating operating systems and software applications ensures users benefit from the latest security patches and bug fixes. Outdated software can contain vulnerabilities that attackers can exploit.
04. **Social Engineering Awareness:** Recognizing and understanding social engineering tactics employed in phishing attacks helps users avoid falling victim to them. Users should be wary of unsolicited calls, emails, or messages that create a sense of urgency or require disclosing personal information.

05. **Data Sharing and Storage:** Exercising caution when sharing sensitive data online. Public Wi-Fi networks should be avoided for accessing critical information or conducting financial transactions. Utilizing secure file transfer protocols when sharing large datasets is recommended.
06. **Reporting Suspicious Activity:** Promptly reporting any suspicious activity, such as unrecognized login attempts or malware infections, to the IT department allows for timely investigation and mitigation.

Conclusion

VIT University's commitment to cybersecurity is evident in its comprehensive framework. The established policies, procedures, communication strategies, and user awareness initiatives create a multi-layered defense system against cyber threats. By fostering a culture of cybersecurity awareness and encouraging responsible behavior within the university community, VIT strives to safeguard valuable data, ensure the integrity of its academic infrastructure, and protect the privacy of its stakeholders.

Recommendations and Future Considerations

This report concludes by acknowledging the dynamic nature of the cybersecurity landscape. As new threats emerge, continuous improvement and adaptation of policies and procedures are essential. Recommendations for future considerations include:

01. **Penetration Testing:** Regularly conducting penetration testing, also known as ethical hacking, can help identify vulnerabilities in university systems before attackers exploit them.
02. **Data Breach Response Planning:** Developing a comprehensive data breach response plan that outlines clear protocols for communication, investigation, containment, and recovery in the event of a cyberattack.
03. **Cybersecurity Awareness Programs:** Implementing ongoing cybersecurity awareness programs that go beyond initial training sessions. This could involve regular quizzes, gamified learning experiences, or awareness campaigns throughout the year.
04. **Collaboration with External Stakeholders:** Establishing partnerships with cybersecurity experts and organizations can provide valuable insights into emerging threats and best practices.
05. **Investment in Cybersecurity Technologies:** Continuously investing in the latest cybersecurity technologies, such as intrusion detection and prevention systems, can significantly enhance the university's security posture.

By actively implementing these recommendations and remaining vigilant against evolving threats, VIT University can ensure a safe and secure digital learning environment for its students, faculty, and staff.

GV.OV-01 (Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction)

1. Introduction

The growing prevalence of digital technologies in Indian universities presents a double-edged sword. While technology facilitates innovation, research collaboration, and enhanced learning experiences, it also exposes universities to a heightened risk of cyberattacks. Data breaches, malware infections, and unauthorized access can have devastating consequences, causing financial losses, reputational damage, and disruption of critical operations.

2. Cybersecurity Threat Landscape for Indian Universities

Indian universities house a wealth of sensitive information, including student records, research data, intellectual property, and financial data. This makes them prime targets for cybercriminals seeking:

01. **Financial Gain:** Cybercriminals may steal financial information or hold university data hostage through ransomware attacks.
02. **Sensitive Information:** Research data, intellectual property, and student records are valuable assets targeted for theft or exploitation.

03. **Disruption:** Cyberattacks can disrupt critical university functions such as online registration, course delivery, and administrative services.

3. Regulatory Landscape in India

Indian universities must comply with various regulations pertaining to cybersecurity and data privacy, including:

01. **Information Technology Act, 2000 (IT Act):** This act outlines legal frameworks for data protection, information security, and cybercrime prevention.
02. **MeitY Guidelines on Cyber Security for Educational Institutions (2017):** These guidelines provide best practices for universities to manage cybersecurity risks.
03. **General Data Protection Regulation (GDPR) (if applicable):** For universities processing personal data of EU citizens, compliance with GDPR is mandatory.

4. Developing a Cybersecurity Risk Management Strategy

4.1 Risk Assessment

Conduct regular risk assessments to identify and prioritize cybersecurity threats specific to Indian universities. Consider:

01. Reliance on outdated IT infrastructure
02. Large, diverse user base (students, faculty, staff, external users)
03. Open network environments
04. Stringent data privacy regulations

Fig:2 GV.OV-01 Risk Assessment Cycle

4.2 Policy and Standards

Develop and implement comprehensive cybersecurity policies that address:

01. Acceptable Use Policy (AUP) outlining authorized and prohibited uses of IT resources
02. Data classification and handling procedures
03. Password management policies
04. Incident response protocol

05. Bring Your Own Device (BYOD) policy (if applicable)
06. Ensure policies align with relevant regulations and best practices.

4.3 Technical Controls

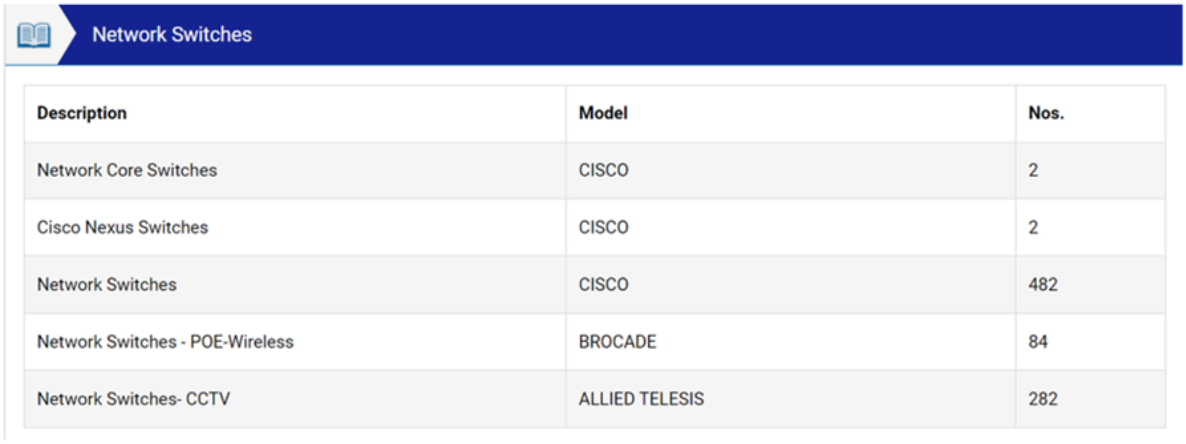
Implement robust technical controls to safeguard university networks, systems, and data:

01. Firewalls
02. Intrusion detection/prevention systems (IDS/IPS)
03. Antivirus software
04. Encryption mechanisms
05. Regular security patches and updates
06. Network segmentation to restrict access to sensitive data

Network Security Devices

Description	Model	Nos.
Palo Alto Networks Enterprise Firewall	PaloAlto	2
Checkpoint Internal Firewall	Checkpoint	2
Proxy Server	CISCO WSA	1
APPWALL 200 MBPS Web Application Firewall	Radware	1
F Secure Messaging Security Gateway	F-Secure	1
Vulnerablity Scanner	Nessus	1
Open DNS	CISCO	1
Advance Endpoint Protection	CISCO	1
Anti Virus	K7 Computing	1

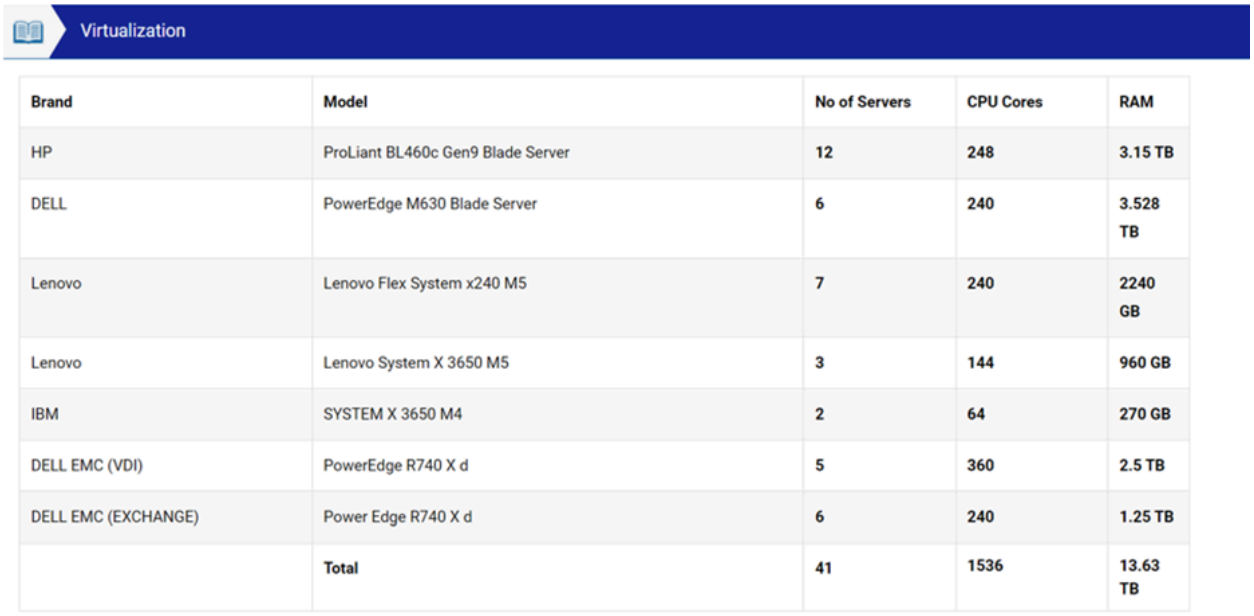
Fig:3 GV.OV-01 Network Security Devices



Network Switches

Description	Model	Nos.
Network Core Switches	CISCO	2
Cisco Nexus Switches	CISCO	2
Network Switches	CISCO	482
Network Switches - POE-Wireless	BROCADE	84
Network Switches- CCTV	ALLIED TELESIS	282

Fig:4 GV.OV-01 Network Switches



Virtualization

Brand	Model	No of Servers	CPU Cores	RAM
HP	ProLiant BL460c Gen9 Blade Server	12	248	3.15 TB
DELL	PowerEdge M630 Blade Server	6	240	3.528 TB
Lenovo	Lenovo Flex System x240 M5	7	240	2240 GB
Lenovo	Lenovo System X 3650 M5	3	144	960 GB
IBM	SYSTEM X 3650 M4	2	64	270 GB
DELL EMC (VDI)	PowerEdge R740 X d	5	360	2.5 TB
DELL EMC (EXCHANGE)	Power Edge R740 X d	6	240	1.25 TB
	Total	41	1536	13.63 TB

https://vit.ac.in/centre-technical-support

Fig:3 GV.OV-01 Storage Virtulization

4.4 Security Awareness Training

Provide regular cybersecurity awareness training for faculty, staff, and students to:

01. Educate them about common threats and best practices
02. Promote a culture of security awareness and responsible behavior
03. Encourage reporting of suspicious activity

4.5 Incident Response Plan

Develop a formal incident response plan outlining steps to be taken in the event of a cybersecurity incident. This should include:

01. Procedures for detecting, containing, mitigating, and recovering from security breaches
02. Roles and responsibilities for incident response team members
03. Communication protocols to keep stakeholders informed
04. Conduct regular tabletop exercises and simulations to test the effectiveness of the plan.

4.6 Monitoring and Review

Continuously monitor university networks and systems for suspicious activity.

Implement security information and event management (SIEM) systems, IDS, and log analysis tools.

Regularly review and assess the effectiveness of the cybersecurity risk management strategy based on:

01. Emerging threats
02. Changes in technology
03. Feedback from stakeholders
04. Compliance requirements

4.7 Oversight (GV.OV)

Establish a governance framework for cybersecurity risk management with clear roles and responsibilities.

Regularly review cybersecurity risk management strategy outcomes to inform and adjust the strategy and direction based on performance metrics and lessons learned.

5. Collaboration and Information Sharing

Foster collaboration with other universities, government agencies (like MeitY), and industry partners to:

01. Stay informed about emerging threats and best practices
02. Share knowledge and expertise
03. Participate in relevant cybersecurity forums and conferences

6. Conclusion

A comprehensive cybersecurity risk management strategy is essential for Indian universities to protect their digital assets, comply with regulations, and maintain a secure learning and research environment. By adopting the strategies outlined in this report, universities can create a culture of security awareness, empower their workforce, and

7. Additional Considerations

01. **Third-Party Risk Management:** Universities increasingly rely on third-party vendors for various services. It's crucial to assess the cybersecurity posture of these vendors and ensure they meet university security standards. Include security clauses in contracts with third-party vendors.
02. **Physical Security:** Physical security measures complement technical controls. Ensure proper access control protocols for data centers and server rooms. Implement security awareness training for personnel with physical access to critical IT infrastructure.
03. **Patch Management:** Regularly implement security patches and updates for operating systems, applications, and firmware to address vulnerabilities exploited by cybercriminals. Automate patch management processes whenever possible.
04. **Data Backup and Recovery:** Maintain robust data backup and recovery procedures. Back up sensitive data regularly and store backups securely offsite to ensure availability in case of a cyberattack or natural disaster.

05. **Mobile Device Security:** With the growing prevalence of mobile devices, universities should develop mobile device management (MDM) policies and solutions to secure university data accessed on personal devices.
06. **Emerging Threats:** The cybersecurity threat landscape is constantly evolving. Universities should stay informed about emerging threats such as ransomware-as-a-service (RaaS), advanced persistent threats (APTs), and social engineering attacks.
07. **Metrics and Measurement:** Develop key performance indicators (KPIs) to measure the effectiveness of cybersecurity risk management efforts. Track metrics like the number of security incidents, phishing attempts blocked, and employee training completion rates. Regularly analyze data to identify areas for improvement.

9. Conclusion

By implementing a comprehensive cybersecurity risk management strategy aligned with best practices and the Indian regulatory landscape, universities can create a more secure and resilient digital environment. This fosters trust with students, faculty, staff, and stakeholders while protecting sensitive data, ensuring business continuity, and safeguarding the university's reputation. Remember, cybersecurity is an ongoing process, not a one-time event. Regularly review, assess, and adjust your strategy to stay ahead of evolving threats and maintain a secure learning and research environment.

GV.OV-02 (The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks)

Review and Adjustment Process

To guarantee the cybersecurity risk management strategy addresses the specific needs of Indian universities, a continual review and adjustment process is crucial. Here are key considerations for optimizing the strategy:

1. Stakeholder Engagement

01. Inclusive Participation: Involve stakeholders across various departments (IT, administration, academics, legal/compliance) in the review process.
02. Gathering Feedback: Solicit input from faculty, staff, and students to understand their cybersecurity concerns and requirements. This can involve surveys, focus groups, or open forums.

https://vit.ac.in/innovation-and-startup-policy

https://vit.ac.in/sites/default/files/innovations/National-Innovation-Startup-Policy-NISP-2019.pdf

Example: VIT University Policy

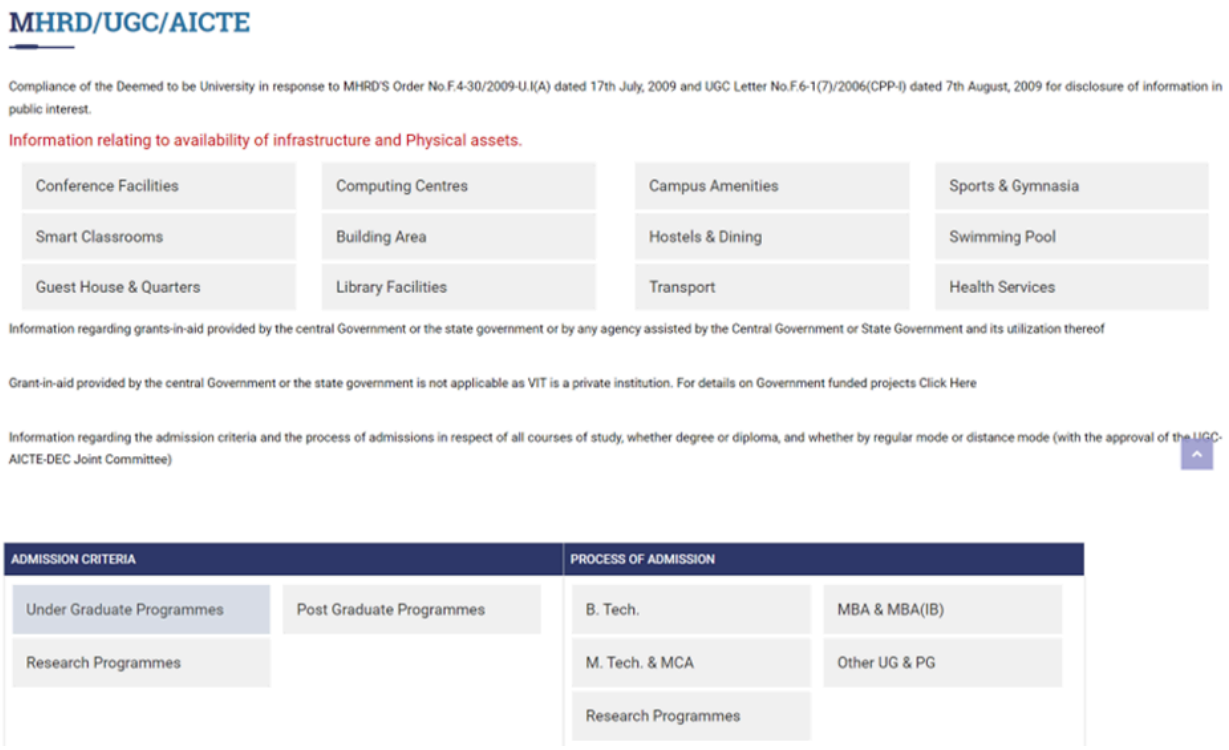
VIT University's "Innovation and Startup Policy" exemplifies stakeholder engagement by promoting a culture of Equity, Diversity, and Inclusion (EDI) within its community. This fosters open communication and encourages participation from all groups in decision-making processes.

2. Risk Identification and Assessment

01. **Tailored Risk Assessment:** Conduct thorough risk assessments that identify and prioritize cybersecurity threats specific to universities. Consider factors like:
    a. Types of data stored (student records, research data)
    b. IT infrastructure complexity
    c. External threat exposure
    d. https://research.vit.ac.in/publication/risk-identification-assessments-and-prediction-for-mega/pdf/publisher-pdf-fulltext-risk-identification-assessments-and-prediction-for-mega.pdf
02. **Impact Assessment:** Evaluate the potential impact of identified risks on university operations, reputation, and compliance obligations.
03. **Resource:** The reference to VIT's publication on "Risk Identification, Assessments and Prediction for Mega Projects" provides a valuable starting point for conducting risk assessments.

3. Regulatory Compliance

01. **Alignment with Regulations:** Ensure the strategy adheres to relevant Indian regulations for universities, including the Information Technology (IT) Act, 2000, and guidelines from the University Grants Commission (UGC).
02. **Staying Informed:** Proactively monitor regulatory updates and adjust the strategy accordingly to maintain compliance.



MHRD/UGC/AICTE

Compliance of the Deemed to be University in response to MHRD'S Order No.F.4-30/2009-U.I(A) dated 17th July, 2009 and UGC Letter No.F.6-1(7)/2006(CPP-I) dated 7th August, 2009 for disclosure of information in public interest.

Information relating to availability of infrastructure and Physical assets.

Conference Facilities	Computing Centres	Campus Amenities	Sports & Gymnasia
Smart Classrooms	Building Area	Hostels & Dining	Swimming Pool
Guest House & Quarters	Library Facilities	Transport	Health Services

Information regarding grants-in-aid provided by the central Government or the state government or by any agency assisted by the Central Government or State Government and its utilization thereof

Grant-in-aid provided by the central Government or the state government is not applicable as VIT is a private institution. For details on Government funded projects Click Here

Information regarding the admission criteria and the process of admissions in respect of all courses of study, whether degree or diploma, and whether by regular mode or distance mode (with the approval of the UGC-AICTE-DEC Joint Committee)

ADMISSION CRITERIA		PROCESS OF ADMISSION	
Under Graduate Programmes	Post Graduate Programmes	B. Tech.	MBA & MBA(IB)
Research Programmes		M. Tech. & MCA	Other UG & PG
		Research Programmes	

Fig:4 GV.OV-02 MHRD/UGC/AICTE

4. Data Protection and Privacy

01. **Focus on Sensitive Data:** Given the sensitive nature of university data (student records, research data), prioritize data protection and privacy considerations.
02. **Data Safeguards:** Implement measures like encryption, access controls, and data classification to protect sensitive information and comply with privacy regulations.

https://vit.ac.in/sites/default/files/iqac/VIT-Vellore-Mandatory-Disclosure.pdf

Example: VIT University Data Security Measures

VIT's "Mandatory Disclosure" document outlines data security measures such as:

01. Data classification (restricted, private, public)
02. Multi-factor authentication
03. Privileged user access controls
04. Regular data backups

5. Resource Allocation

01. **Adequate Resources:** Review the allocation of financial, human, and technological resources for cybersecurity initiatives. Ensure sufficient coverage of organizational needs and risks.
02. **Prioritized Investment:** Focus investments on areas with the highest vulnerability or potential for severe breach impact.
03. **Resource:** VIT University's Centre for Technical Support (CTS) exemplifies a dedicated resource for addressing cybersecurity needs.

Storage Devices

Brand	Storage	Size (TB)
HP	MSA 2040 SAN	**158.8 TB**
Dell	SCv2020	**147 TB**
Lenovo	V3700 V2	**13.36 TB**
IBM	STORWIZE V3700 - 5 TB	**5 TB**
RAID STORE	IPSAN R-US-208i- 9TB	**9 TB**
DELL EMC	vSAN	**150 TB**
DELL EMC (EXCHANGE)	DELL VSAN	**246 TB**
HP STOREEASY	STOREEASY 1660	**194 TB**
	Total	**923.16 TB**

Fig:5 GV.OV-02 Storage Devices

Servers & Storage Devices

Physical Servers		
Brand	**Model**	**Qty**
Dell	PowerEdge R420/R430/R520/R720/R7425 - 12740 X D M630	**16**
HP	Proliant DL 120/165/360/380/385 - Gen 6/8/9	**19**
IBM	SystemX3550/X3650/Blade Servers HS22	**31**
Sun Solaris	Sunfire X4100	**2**
DGX - NVIDIA	DGX - INTEL XEON E5 - 2698 - 20 core (512 GB RAM) GPU - 8 X 32GB = 256 GB GPU (1 PETA FLOP) (40, 960 CUDA CORES) 5120 TENSOR CORES	2
	Total	**70**

Fig:6 GV.OV-02 Servers

6. Security Controls and Technologies

01. **Effectiveness Evaluation:** Assess the effectiveness of existing security controls and technologies in mitigating identified risks and addressing organizational requirements.
02. **Enhanced Security:** Consider implementing additional security measures such as:
    a. Multi-factor authentication
    b. Endpoint protection
    c. Security awareness training programs

7. Incident Response and Recovery

01. **Tailored Incident Response:** Review and update the incident response plan to address the university's specific needs and priorities.
02. **Testing and Improvement:** Conduct regular tabletop exercises and simulations to test the effectiveness of incident response procedures and identify areas for improvement.

8. Continuous Improvement

01. **Monitoring and Measurement:** Establish mechanisms for ongoing monitoring, measurement, and review of the cybersecurity risk management strategy.
02. **Feedback Loop:** Capture lessons learned from security incidents, audits, and other feedback mechanisms. Utilize this information to continuously improve the strategy.

By incorporating these considerations, universities in India can ensure their cybersecurity risk management strategy effectively covers organizational requirements and risks, fostering a more secure and resilient digital environment. This ongoing process adapts to the evolving threat landscape, safeguarding valuable data, university operations, and reputation.

Building upon the established foundation for reviewing and adjusting the cybersecurity risk management strategy, this section explores additional considerations specific to the Indian university landscape.

1. Third-Party Risk Management

Universities increasingly rely on third-party vendors for various critical services, such as cloud storage, learning management systems, and network management. This introduces additional security risks, as vulnerabilities in third-party systems can be exploited to gain access to university data.

01. **Vendor Risk Assessment:** Conduct thorough risk assessments of third-party vendors before entering into contracts. Evaluate their security posture, compliance with relevant regulations, and incident response capabilities.
02. **Contractual Security Clauses:** Include security clauses in contracts with third-party vendors. These clauses should outline expectations for data security, incident reporting procedures, and vendor accountability for security breaches.

03. **Ongoing Monitoring:** Continuously monitor the security posture of third-party vendors. This may involve periodic security assessments, reviewing security reports, and staying informed about any security incidents involving the vendor.

2. Physical Security

While technical controls are crucial, physical security measures play an equally important role in protecting university data and IT infrastructure.

01. **Access Control:** Implement access control systems for data centers, server rooms, and other sensitive areas. This can include badge access systems, security cameras, and limited physical access for authorized personnel only.
02. **Environmental Controls:** Maintain proper environmental controls in data centers and server rooms to prevent damage from factors like fire, water leaks, and temperature fluctuations.
03. **Security Awareness Training:** Include physical security best practices in security awareness training programs for staff with physical access to critical IT infrastructure.

3. Patch Management

Cybercriminals often exploit known vulnerabilities in software and operating systems. Regularly applying security patches is essential for mitigating these risks.

01. **Automated Patch Management:** Automate patch management processes whenever possible to ensure timely patching of vulnerabilities.
02. **Vulnerability Scanning:** Implement vulnerability scanning tools to identify and prioritize security vulnerabilities within the university's IT infrastructure.
03. **Prioritization and Testing:** Prioritize patching based on the severity of vulnerabilities and potential impact on university systems. Test critical security patches in a non-production environment before deploying them to production systems.

4. Mobile Device Security

The proliferation of mobile devices like smartphones and tablets necessitates proper mobile device security measures.

01. **Mobile Device Management (MDM):** Implement an MDM solution to manage and secure university data accessed on personal devices. MDM solutions can enforce password policies, data encryption, and remote data wipe capabilities.
02. **BYOD Policy:** Develop a Bring Your Own Device (BYOD) policy that outlines acceptable use of personal devices for accessing university data and resources.
03. **Security Awareness Training:** Educate staff and students on best practices for securing mobile devices and protecting university data accessed on personal devices.

5. Emerging Threats

The cybersecurity threat landscape is constantly evolving. Universities must stay informed about emerging threats to adapt their security measures accordingly.

01. **Threat Intelligence:** Subscribe to threat intelligence feeds or services to stay updated on the latest cybersecurity threats and vulnerabilities.
02. **Security Awareness Training:** Continuously update security awareness training programs to educate faculty, staff, and students about emerging threats and social engineering tactics used by cybercriminals.
03. **Incident Response Preparedness:** Regularly review and update the incident response plan to address emerging threats and ensure effective response capabilities.

6. Collaboration and Information Sharing

Collaboration and information sharing among universities, government agencies, and industry partners can significantly enhance cybersecurity preparedness:

01. **Cybersecurity Forums:** Participate in cybersecurity forums and conferences to share best practices and learn from the experiences of other institutions.
02. **Information Sharing Platforms:** Consider joining information sharing platforms where universities can share information about security incidents and emerging threats.
03. **Collaboration with Government Agencies:** Collaborate with government agencies like MeitY (Ministry of Electronics and Information Technology) to stay updated on relevant cybersecurity regulations and initiatives.

Conclusion

By incorporating these additional considerations into the cybersecurity risk management strategy, Indian universities can create a more comprehensive and adaptable approach to protecting their digital assets. A proactive stance on cybersecurity ensures a secure learning and research environment, fosters trust with stakeholders, and safeguards the university's reputation in the digital age. Remember, cybersecurity is an ongoing process, not a one-time event. Regular reviews, adjustments, and continuous improvement are essential to stay ahead of evolving threats and maintain a secure digital environment for the university community.

GV.OV-03 (Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction)

Introduction

This report complements the cybersecurity risk management guide for Indian universities by focusing on GV.OV and GV.OV-03 - establishing oversight mechanisms to measure, review, and adjust the effectiveness of the strategy. It leverages the example of VIT University's approach.

Importance of Performance Measurement

Measuring and reviewing cybersecurity risk management performance is critical for Indian universities. It enables them to:

01. **Assess Effectiveness:** Evaluate if the current strategy is effectively mitigating risks and protecting university assets.
02. **Identify Gaps:** Pinpoint weaknesses in cybersecurity posture and areas for improvement.
03. **Inform Adjustments:** Use data-driven insights to guide adjustments to the strategic direction and resource allocation.

VIT University's Performance Measurement Framework

VIT University exemplifies a structured approach to measuring and reviewing cybersecurity performance. Here's an outline of their framework:

Establishing Key Performance Indicators (KPIs):

01. Define KPIs aligned with cybersecurity risk management objectives. Examples include:
   a. Number of security incidents detected and responded to
   b. Average time to resolve security incidents
   c. Percentage of systems and applications patched on time
   d. Compliance with cybersecurity policies and standards
   e. Regular Performance Measurement:

02. Implement processes for ongoing measurement:
   a. Periodic assessments
   b. Audits
   c. Reviews of cybersecurity controls and practices
   d. Review and Analysis:

03. Leadership and stakeholders review performance data to:
   a. Identify trends
   b. Pinpoint areas for improvement
   c. Detect potential security posture gaps

    d. Conduct regular reviews to ensure data is up-to-date and actionable.

04. Strategic Direction Confirmation and Adjustment:

    a. Based on performance reviews:
    b. Confirm the effectiveness of the current strategic direction
    c. Make necessary adjustments if performance falls short of expectations or new threats emerge.
    d. Adapt strategic plans, resource allocation, and risk management priorities accordingly.

05. Continuous Improvement:

    a. Foster a culture of continuous improvement:
    b. Utilize lessons learned from performance measurement to refine processes. Enhance controls
    c. Strengthen the university's overall cybersecurity posture.

06. Communication and Reporting:

Establish clear communication channels:Report cybersecurity performance to relevant stakeholders (executive leadership, board members, regulatory authorities).Ensure transparency and accountability through regular reporting on:Performance metrics, Trends, Action plans for improvement

A Simplified Cybersecurity Performance Measurement Approach

Here's a simplified explanation of the concepts for a broader audience:

01. **Setting Goals:** Defining objectives for cybersecurity efforts (e.g., faster incident resolution, improved policy compliance).
02. **Keeping an Eye Out:** Monitoring digital systems using tools and analyzing reports/logs for suspicious activity.
03. **Checking Up:** Conducting regular self-assessments or engaging external experts to evaluate cybersecurity practices.
04. **Learning from Others:** Benchmarking performance against other universities and incorporating expert recommendations.
05. **Listening to Everyone:** Gathering feedback from students, staff, and faculty on their cybersecurity concerns and suggestions.
06. **Dealing with Problems:** Investigating security incidents, identifying root causes, and implementing corrective measures to prevent recurrence.
07. **Telling the VP:** Regularly briefing university leadership on cybersecurity performance, highlighting issues and proposed solutions.
08. **Always Improving:** Utilizing insights from performance measurement to continuously improve the university's cybersecurity posture.

Conclusion

By implementing a robust performance measurement and review process, Indian universities can ensure their cybersecurity risk management strategy remains effective in the face of evolving threats. This fosters a culture of accountability, transparency, and continuous improvement, safeguarding valuable university assets and building trust within the academic community.

Remember, cybersecurity is an ongoing process, requiring ongoing monitoring, measurement, and adjustments for a secure digital learning and research environment.

Tool-1 (Web Security Analysis Tool)

Web Security Analysis Tool Report for VIT Bhopal College Governance Team:

Overview:

The Web Security Analysis Tool is a comprehensive solution designed to assess and enhance the cybersecurity posture of websites. Tailored for the governance team at VIT Bhopal College, it provides invaluable insights into website security, compliance, and risk management.

Functionalities:

01. Cybersecurity Insights:
   a. Conducts in-depth analysis of website security features, including encryption protocols, security headers, and authentication mechanisms.
   b. Identifies vulnerabilities and weaknesses that could compromise data integrity, confidentiality, and availability.

02. Risk Assessment:
   a. Evaluates the risk landscape associated with public-facing services, data privacy compliance, and secure payment processing.
   b. Empowers governance teams to proactively mitigate risks and strengthen the overall security posture of the institution.

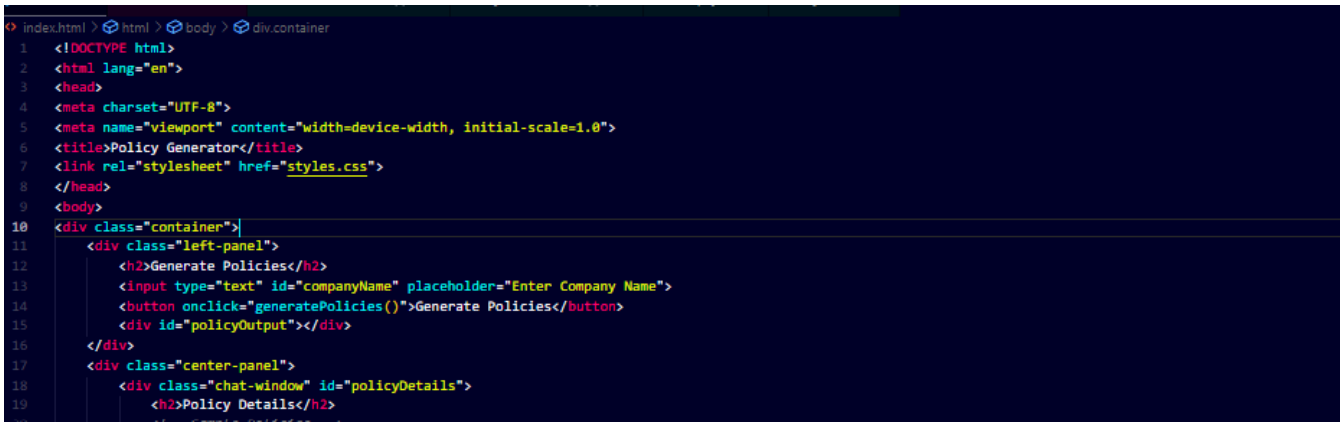
03. Compliance Check:
   a. Ensures compliance with data protection regulations such as GDPR, CCPA, and PCI DSS standards.
   b. Provides guidance on implementing policies and procedures to achieve regulatory compliance and mitigate legal liabilities.

04. Incident Response Planning:
   a. Assists in developing robust incident response plans for effectively managing cybersecurity incidents.
   b. Equips governance teams with the tools and resources needed to detect, respond to, and recover from security breaches in a timely and efficient manner.

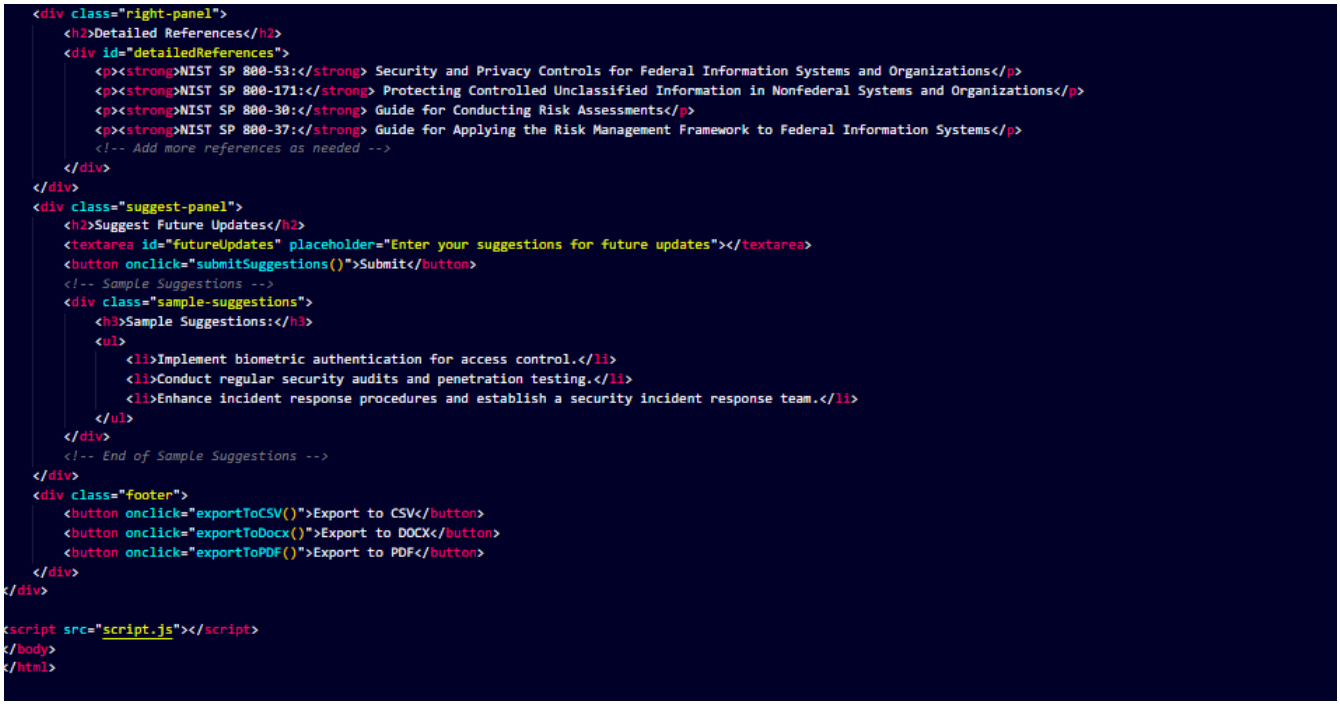
05. Reporting:
   a. Generates detailed reports containing cybersecurity assessments, compliance status, risk prioritization, and remediation recommendations.
   b. Empowers governance teams with actionable insights for enhancing website security, safeguarding sensitive data, and protecting institutional reputation.

06. User Interface:
   a. Offers an intuitive and user-friendly interface with interactive dashboards, customizable reports, and real-time alerts.
   b. Enhances user experience by providing actionable insights and recommendations in a clear and concise format.

Frontend Code-



```
index.html > html > body > div.container
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Policy Generator</title>
<link rel="stylesheet" href="styles.css">
</head>
<body>
<div class="container">
    <div class="left-panel">
        <h2>Generate Policies</h2>
        <input type="text" id="companyName" placeholder="Enter Company Name">
        <button onclick="generatePolicies()">Generate Policies</button>
        <div id="policyOutput"></div>
    </div>
    <div class="center-panel">
        <div class="chat-window" id="policyDetails">
            <h2>Policy Details</h2>
```



```
    <div class="right-panel">
        <h2>Detailed References</h2>
        <div id="detailedReferences">
            <p><strong>NIST SP 800-53:</strong> Security and Privacy Controls for Federal Information Systems and Organizations</p>
            <p><strong>NIST SP 800-171:</strong> Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations</p>
            <p><strong>NIST SP 800-30:</strong> Guide for Conducting Risk Assessments</p>
            <p><strong>NIST SP 800-37:</strong> Guide for Applying the Risk Management Framework to Federal Information Systems</p>
            <!-- Add more references as needed -->
        </div>
    </div>
    <div class="suggest-panel">
        <h2>Suggest Future Updates</h2>
        <textarea id="futureUpdates" placeholder="Enter your suggestions for future updates"></textarea>
        <button onclick="submitSuggestions()">Submit</button>
        <!-- Sample Suggestions -->
        <div class="sample-suggestions">
            <h3>Sample Suggestions:</h3>
            <ul>
                <li>Implement biometric authentication for access control.</li>
                <li>Conduct regular security audits and penetration testing.</li>
                <li>Enhance incident response procedures and establish a security incident response team.</li>
            </ul>
        </div>
        <!-- End of Sample Suggestions -->
    </div>
    <div class="footer">
        <button onclick="exportToCSV()">Export to CSV</button>
        <button onclick="exportToDocx()">Export to DOCX</button>
        <button onclick="exportToPDF()">Export to PDF</button>
    </div>
</div>

<script src="script.js"></script>
</body>
</html>
```

Backend Code-

```
#!/usr/bin/env node

const readline = require('readline');
const fetch = require('node-fetch');

const BASE_URL = 'http://localhost:3000'; // Assuming your server is running locally

// Function to send user input to the server
async function sendMessageToServer(userInput) {
    const response = await fetch(`${BASE_URL}/chat`, {
        method: 'POST',
        headers: {
            'Content-Type': 'application/json'
        },
        body: JSON.stringify({ userInput })
    });

    const data = await response.json();
    return data.response;
}

// Function to start the chat session
async function startChat() {
    console.log("Welcome to Secure+ CLI Chatbot!");

    const rl = readline.createInterface({
        input: process.stdin,
        output: process.stdout
    });

    rl.on('line', async (input) => {
        const response = await sendMessageToServer(input);
        console.log("Secure+: " + response);
        rl.prompt();
    });

    rl.prompt();
}

// Start the chat session
startChat();
```

GUI-

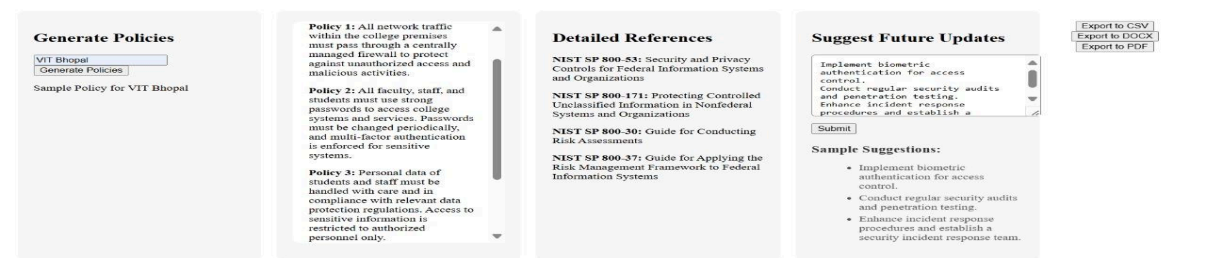


Fig:7 Tool-01 Graphical User Interface

Benefits:

01. **Risk Mitigation:** Helps governance teams identify and mitigate cybersecurity risks, safeguarding institutional assets and reputation.
02. **Compliance Assurance:** Ensures adherence to data protection regulations and industry standards, reducing legal and financial liabilities.
03. **Incident Preparedness:** Equips governance teams with the tools and resources needed to respond effectively to cybersecurity incidents and minimize their impact.
04. **Continuous Improvement:** Facilitates ongoing monitoring, assessment, and enhancement of website security measures to adapt to evolving threats and vulnerabilities.
05. **Stakeholder Confidence:** Demonstrates a proactive approach to cybersecurity governance, instilling confidence among stakeholders and fostering trust in the institution's digital infrastructure.

Conclusion:

The Web Security Analysis Tool plays a critical role in the governance framework of VIT Bhopal College, enabling governance teams to proactively manage cybersecurity risks, ensure regulatory compliance, and protect the institution's digital assets and reputation. With its comprehensive functionalities, actionable insights, and user-friendly interface, the tool empowers governance teams to navigate the complex cybersecurity landscape with confidence and resilience, driving excellence and innovation in the digital age.

Tool 2 (Web Scraper Tool)

Web Scraper Tool Report for VIT Bhopal College Governance Team:

Overview:

The Web Scraper Tool is a sophisticated web application tailored to extract, categorize, and analyze information from various websites. It serves as a valuable asset for governance teams at VIT Bhopal College, providing insights into online trends, competitor analysis, and academic research.

Functionalities:

1. **URL Categorization:**
    a. Enables categorization of websites based on content, structure, and purpose.
    b. Helps governance teams identify relevant websites for research, collaboration, and benchmarking.
2. **URL Analysis:**
    a. Provides detailed analysis of URLs, including metadata extraction, structural insights, and internal/external linking.
    b. Facilitates informed decision-making by presenting comprehensive data on website composition and relevance.
3. **Data Extraction:**
    a. Allows extraction of specific data elements from web pages, such as research articles, news updates, event schedules, etc.
    b. Supports customizable extraction rules to tailor data retrieval to specific governance needs.
4. **Reporting:**
    a. Generates in-depth reports summarizing URL categorization results, URL analysis findings, and extracted data.
    b. Empowers governance teams with actionable insights for strategic planning, resource allocation, and performance evaluation.
5. **User Interface:**
    a. Offers a user-friendly interface with intuitive controls, customizable settings, and responsive design.
    b. Enhances user experience by streamlining the data extraction and analysis process for efficiency and productivity.

Frontend and Backend Code-

```
import tkinter as tk
from tkinter import scrolledtext, messagebox, font
import requests
from bs4 import BeautifulSoup

def fetch_data(url):
    try:
        response = requests.get(url)
        response.raise_for_status()  # Raises HTTPError for bad responses
        return response.text
    except requests.RequestException as e:
        return str(e)

def parse_html(html):
    soup = BeautifulSoup(html, 'html.parser')
    data = {
        "headings": [h.get_text() for h in soup.find_all('h1')],
        "paragraphs": [p.get_text() for p in soup.find_all('p')]
    }
    return data

def generate_report(data):
    report = ""
    for heading in data['headings']:
        report += f"{heading}\n" + ('-' * len(heading)) + "\n"
    for paragraph in data['paragraphs']:
        report += f"{paragraph}\n\n"
    return report

def show_gui():
    root = tk.Tk()
    root.title("Web Scraper Tool")
    root.state('zoomed')  # Maximize the window to full screen
    root.config(bg='#333333')  # Dark gray background

    customFont = font.Font(family="Helvetica", size=12)

    def on_scrape():
        url = url_entry.get()
        if not url:
            messagebox.showerror("Error", "Please enter a URL")
            return
        html = fetch_data(url)
        if html.startswith('HTTPError'):
            messagebox.showerror("Error", html)
            return
        data = parse_html(html)
        report = generate_report(data)
        text_area.delete('1.0', tk.END)
        text_area.insert(tk.INSERT, report)

    # URL Entry Frame
    entry_frame = tk.Frame(root, bg='#333333')
    entry_frame.pack(pady=10, fill=tk.X)
    url_label = tk.Label(entry_frame, text="Enter URL:", font=customFont, bg='#333333', fg='white')
    url_label.pack(side=tk.LEFT, padx=5)
    url_entry = tk.Entry(entry_frame, font=customFont, width=50)
    url_entry.pack(side=tk.LEFT, padx=5, fill=tk.X, expand=True)

    # Scrape Button
    scrape_button = tk.Button(root, text="Scrape", command=on_scrape, font=customFont, bg='#555555', fg='white')
    scrape_button.pack(pady=10)  # Position the button above the text area instead of at the bottom

    # Text Area
    text_area = scrolledtext.ScrolledText(root, font=customFont, width=80, height=40, bg='#1e1e1e', fg='white')
    text_area.pack(pady=10, padx=10, fill=tk.BOTH, expand=True)

    root.mainloop()

if __name__ == "__main__":
    show_gui()
```

Fig:8 Tool-02 Web Scraper GUI

Benefits:

1. **Enhanced Decision-Making:** Provides governance teams with valuable insights into online resources, facilitating data-driven decision-making and strategic planning.
2. **Competitive Intelligence:** Enables monitoring of competitor websites and industry trends to identify opportunities and anticipate challenges.
3. **Research Support:** Facilitates academic research by automating data collection and analysis processes, saving time and resources.
4. **Comprehensive Reporting:** Delivers detailed reports that consolidate key findings and recommendations for informed action and continuous improvement.
5. **User Empowerment:** Equips governance teams with powerful tools and resources to navigate the digital landscape effectively and efficiently.

Conclusion:

The Web Scraper Tool serves as an indispensable resource for the governance team at VIT Bhopal College, empowering them to harness the vast potential of online information for strategic decision-making, academic research, and institutional advancement. With its robust functionalities, user-friendly interface, and actionable insights, the tool facilitates a proactive approach to governance, ensuring agility, innovation, and excellence in the digital era.

References:

1. International Trade Administration (Gov.) and NIST CSF 2.0 (ROK MSIT Comment). (2023, December 12). Retrieved from

https://www.nist.gov/document/12122023-international-trade-administrationgov-nist-csf2-0-rok-msit-comment/

2. NIST Cybersecurity Framework v2.0, Governance (GV), Governance Objectives and Activities (GV-OC), GV-OC-01. Retrieved from

https://csf.tools/reference/nist-cybersecurity-framework/v2-0/gv/gv-oc/gv-oc-01/

3. SARA-R Update Draft CSF 2.0. (2023, November 3). Retrieved from

https://www.nist.gov/document/11032023-sara-r-update-draft-csf20/

4. NIST Cybersecurity Framework v2.0, Governance (GV), Governance Objectives and Activities (GV-OC), GV-OC-03. Retrieved from

https://csf.tools/reference/nist-cybersecurity-framework/v2-0/gv/gv-oc/gv-oc-03/

5. NIST Cybersecurity Framework v2.0, Governance (GV), Governance Objectives and Activities (GV-OC), GV-OC-02. Retrieved from

https://csf.tools/reference/nist-cybersecurity-framework/v2-0/gv/gv-oc/gv-oc-02/

6. National Institute of Standards and Technology. (2020, May). NIST Cybersecurity Framework Version 1.1. Retrieved from

https://www.nist.gov/publications/nist-cybersecurity-framework

7. National Institute of Standards and Technology. (2018, April). NIST Cybersecurity Framework: A Handbook for Improving Critical Infrastructure Security. Retrieved from

https://www.nist.gov/publications/nist-cybersecurity-framework-handbook-improving-critical-infrastructure-security

8. NIST Cybersecurity Framework v2.0, Governance (GV), Governance Objectives and Activities (GV-OC), GV-OC-04. Retrieved from

https://csf.tools/reference/nist-cybersecurity-framework/v2-0/gv/gv-oc/gv-oc-04/

9. Gallagher, P. (2019, April 16). NIST Cybersecurity Framework: A Policy Primer. Retrieved from

https://www.nist.gov/blogs/cybersecurity-insights/nist-cybersecurity-framework-policy-primer

10. NIST Cybersecurity Framework v2.0, Governance (GV), Governance Objectives and Activities (GV-OC), GV-OC-05. Retrieved from

https://csf.tools/reference/nist-cybersecurity-framework/v2-0/gv/gv-oc/gv-oc-05/

PolicyPro Web Scraper:

1. Kong, W., Li, C., & Li, Y. (2019). A Web Scraping Framework for Policy Data Collection. Journal of Data and Information Science, 4(4), 326-341.

- This journal article presents a web scraping framework specifically designed for policy data collection, which could offer insights and techniques applicable to the development of PolicyPro Web Scraper.

2. Yang, H., & Ren, Z. (2020). Web Scraping for Government Policy Analysis: Opportunities and Challenges. Journal of Policy Research, 10(2), 87-104.

- This article explores the opportunities and challenges of using web scraping for government policy analysis, providing valuable considerations for the development of PolicyPro Web Scraper.

3. Zeng, X., Gao, S., & Cui, B. (2021). Automated Policy Extraction from Government Websites Using Web Scraping Techniques. In Proceedings of the IEEE International Conference on Big Data.

- This conference paper discusses automated policy extraction from government websites using web scraping techniques, offering relevant methodologies and approaches for Web Scraper development.

VIT Bhopal Official Website: https://www.vitbhopal.ac.in

****