International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-8, Issue-5, May 2022
ISSN: 2395-3470
www.ijseas.com

Information Security Analysis of VIT Vellore University

Vadiraj Rao

Department of Computer Science and Engineering Vellore Institute of Technology,Vellore

Janhavi Talhar

Department of Computer Science and Engineering Vellore Institute of Technology,Vellore

Atharva Ramgirkar

Department of Computer Science and Engineering Vellore Institute of Technology,Vellore

Abstract

Stephani Nappo quoted that 'It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it'. Cyber security, often known as network security, is an important topic to research in any system. All devices and networks are vulnerable to intrusion, which must be identified and avoided as quickly as practicable. In other circumstances, data loss can be calamitous, with serious ramifications, such as losing personal information or account information. An audit report can assist us in understanding network vulnerabilities and security features that have been conveyed. Auditing is essential for every organization, whether it is a global corporation, a non-governmental organization, or a university. The authors want to undertake a network security audit at the university level in order to assess each component of network security using NIST 800. The audit provides a detailed survey of the information and data security aspect and evaluates the security level of the organization.

Introduction

To understand the data and network security of any organization, one must understand the concept of information security. Non-repudiation, authentication, and permission are techniques that system designers employ to ensure system security in terms of the CIA trinity (confidentiality, integrity, and availability). Anyone defending information systems and understanding information security must grasp these three fundamental principles [1]. Organizational information security includes employee behaviors and attitudes regarding engagement with information systems, as well as the confidentiality, integrity, and availability of organizational information and information assets [2].

Information security is the protection of information's confidentiality, availability, and integrity. With the increased use of information technology, the risks to information security are becoming more prevalent. Risk is defined as the influence of uncertainty on objectives. Risk management has the ability to control risk. Risk management is a concerted effort to regulate and guide an organization's risk exposure [3] Audio, messages, and objects exchanged and processed by communication networks are forms of information. In broadly, it relates to all aspects of human

communication. There is no such thing as information. It cannot be converted into meaningful items until it is delivered in various ways by humans, such as voices, symbols, signs, and words. Once formed, information does not vanish [4]. Information security policies are documents that provide fundamental standards to secure information security based on top management's vision connected to major strategic business objectives within the scope of management goals. To safeguard information assets, information security policies incorporate rules, guidelines, and controls [5].

The main aim of the paper is to understand and analyze the information security of a university and evaluate if data stored by the institute is secure. Securing university data is extremely crucial and mandatory. With increasing technological advancements, Data has become the most important asset. Data drives most of the business processes and decisions. This is evident from the fact that 2.5 quintillion bytes of data is generated per day. Every business and most of the organizations are finding new ways to collect data and leverage it to drive business decisions. In educational institutions like schools and universities, data collection has become an important part of management. Institutes collect data from students like their permanent address, age, gender, family income, parents' professional jobs and a lot of other data points. Once this data is collected, the university can use the data to advertise its programs to specific areas or specific segments of students and even their parents. Some universities also have integrated payment gateways in their own portals thus credit card and debit card data of the students and their parents is also available with the universities. Thus, a university holds a lot of sensitive personal data about a student and also his/her parents. This makes universities a target for attackers to hack and get access to this sensitive data.

Prior Work

Alvita Izana Kusumarini and Henki Bayu Seta[1] analyzed server security vulnerability by using Penetration Testing Execution Standard (PTES) method on employee data of VWX University. They found the following vulnerabilities ; Cross-Site Tracing (CST) attacks, Sensitive Data Exposure, Password Guessing, DDoS Attack, and Sniffing activities and discussed their effects and how critical they are. Pius Tangeni SHAMBABI1, Stanford Musarurwa2 and Fungai BHUNU SHAVA1[2] assessed organizational information security culture among the workforce in Namibian universities. They conducted surveys with employees of the university regarding information security and discussed the major points like Information security policy awareness, password sharing etc. in detail. Made Martadi Putra and Kusprasapta Mutijarsa[3] designed an Information Security Risk Management on Bali regional police command center. They have integrated two standards ISO 27005: 2018 and NIST SP 800-30 to identify risks, control risks and give recommendations for mitigation. Wang di[4] has summarized the connotations and main work of information security in universities. She has analyzed information security based on the

following four aspects: resistance capacity, overall environment of security protection system, working mode of information construction and security awareness of all personnel and suggested countermeasures. Angraini, Alinda Alias, Okfalisa, Johor[5] have analyzed the need for compliance with Information security policies in universities. A questionnaire was handed to manager level at a university and an appropriate model for evaluation was suggested.

Wenhua Sun and Lifeng Wu[6] make an in-depth discussion and analysis of network technology means and security prevention strategies, and state the preventive measures and suggestions for the network and information security problems in universities. Chanchala Joshi and Umesh Kumar Singh[7] have designed a quantitative information security risk assessment model for Vikram University Ujjains computing environment and results showed that this proposed model enhances the security level of the campus network. Jing Nie and Xue Ling Dai[8] have discussed the information security issue in the information construction process of universities. They have focused on issues of domestic universities' informatization process and have analyzed the problems of information security management and provided reasonable solutions. Xian Weiquan,Wang Houkui, He haoyi and Zheng Donghong[9] have performed analysis of university network information security systems based on level protection models starting from level protection models to explore network information safety system, analyze the university. They aim atproviding more attention, network information safety for university teachers and students. Ho- Yeol Kwon[10] has briefly discussed IT governance with security engineering and information systems of a university. The researcher has also proposed a strategic approach of IT governance for university information systems with new performance criteria.

Chanchala Joshi and Umesh Kumar Singh[11] have proposed a framework that reduces the risk of security breach by supporting three phase activities; assessing the threats and vulnerabilities, focus on highest risk and creating actionable remediation plans,and recognizing the vulnerability management compliance requirement. The results showed enhancement in security. Victoria Stanciu and Andrei Tinca[12] have carried out an empirical study on students' awareness on information security. Their study revealed that the students' computing knowledge is more technical and less addressed to information security issues. The research concludes by emphasizing on the need for improving the universities curriculum in regard with information security issues and students' training using programs. Jake Weidman and Jens Grossklags[13] have assessed the current state of information security policies in academic organizations. They assessed the current state of information security policies by analyzing in-use policies from 200 universities and colleges in the USA and identified important features and general attributes of these documents. Nashrawan Taha and Laila Dahabiyeh[14] provide an empirical comparison in the level of information security awareness

and behavior. They have discussed the importance of smart phone security knowledge in students and have suggested conducting training camps for increasing security awareness

.

Kathryn Parsons , Dragana Calic , Malcolm Pattinson , Marcus Butavicius , Agata McCormac and Tara Zwaans[15] have worked to establish the validity of the Human Aspects of Information Security Questionnaire (HAIS-Q), as an effective instrument for measuring ISA. 112 university students completed the questionnaire and also took part in an empirical lab-based phishing experiment. They found out that participants who scored graeter had better performance in the experiment. Ali Daneshmandnia[16] has studied the influence of organizational culture on information governance effectiveness. The researcher employed Cameron and Quinn's 2011 competing value framework. It was found organizational culture may influence IG effectiveness positively whereas presence of information silos was a challenge to IG effectiveness. M. Elizabeth Haywood[17] has used COBIT to study computer crime at Bucks County community college in Pennsylvania. The aspects of COBIT were highlighted for evaluating information technology governance and management and many suggestions for minimizing risks and vulnerabilities were mentioned.

Audit Process

The auditing process is divided into five stages. The scope and objective of the audit are initially defined during the pre-audit process. In this case, the objective is to determine how safe the institute's network and data security is. The audit's selected location and organization are examined, as well as any financial factors. An agreement is generated on the creation of an audit. The external auditor, who is recruited by the organization for legal or obligatory reasons, is required to sign an officially established confidentiality agreement. The audit team then handles the planning and initiation in the second phase. The fundamental risk assessment is put forth, and legal restrictions are considered. Initial audit team meetings are held, as well as an overall timeline is established.

The most essential step in establishing an audit is gathering data. There are various techniques for gathering evidence and testing the facts. The network security department within the institute was contacted as part of this research to acquire all information on the audit questions. Information gathering can be conducted using network survey, identification of OS as TCP/IP fingerprint, port scanning and identification of services provided. The amount of confidentiality and accessibility in the displayed audit determines these parameters. The audit team draws insights and findings after interpreting the obtained material. This is the auditing's analysis step. The evidence obtained is examined, and inferences are drawn based on it. Finally, the audit is drafted and the organization's overall security level is assessed.

Auditor roles and responsibilities

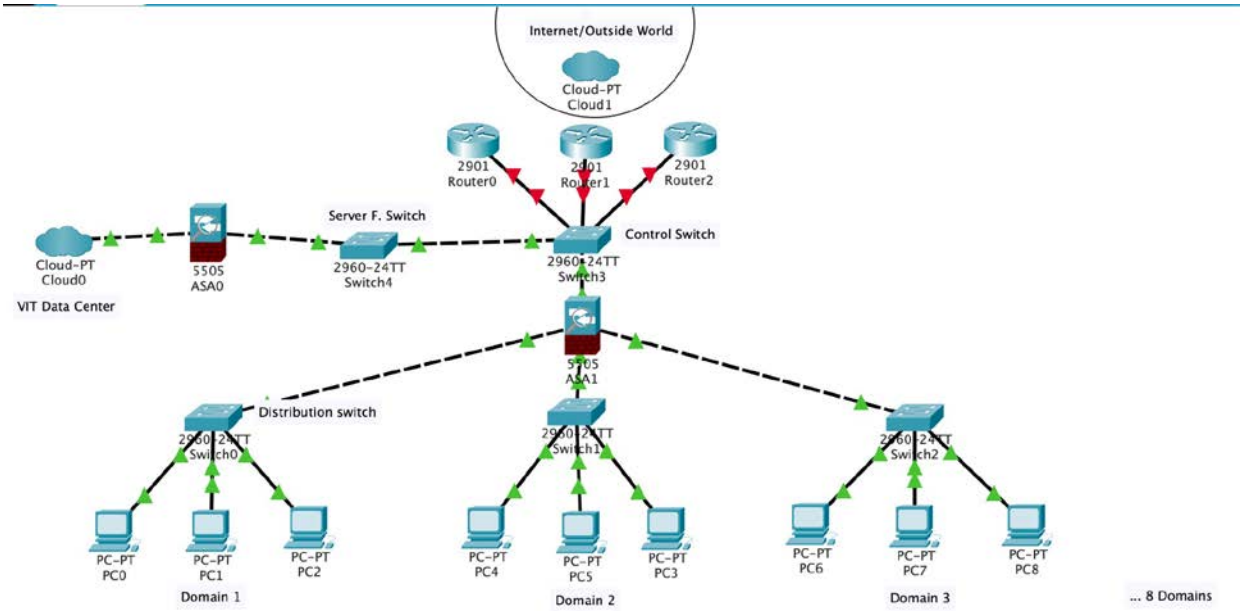
An information security auditor examines the safety and efficacy of computer systems and their

security components. An auditor asks security related questions and develops insights based on received facts. They test control and security efficiency of the network system. Any organization storing big data and executing large amounts of transactions on daily basis is prone to computer attacks and malwares. An auditor checks the security weaknesses and inspects all related factors. They develop and administer all the risks and vulnerabilities in the organization as a whole. The entire system effectiveness, efficiency and compliances are thoroughly studied and analyzed. Then the auditor drafts the details, including the review or interview of all the considered parameters. Once this procedure is completed, the auditor will summarize the draft and produce a thorough report indicating if the network system is operating efficiently and effectively. The derived audit is further delivered to the organization's management or infosec department, who study any essential modifications that must be done to improve the system's integrity.

University description

Vellore Institute of Technology was established under Section 3 of the UGC Act, 1956 and founded in 1984. It is located in Vellore, a district in Tamil Nadu, India. There are 3 other campuses under VIT located in Andhra Pradesh, Chennai and Bhopal. The university is one of the top institutes in the country and offers around 64 Undergraduate, 35 Postgraduate, 16 Integrated, 2 Research and 2 MTech Industrial Programs. The study proposed by the authors of this research focused on the Vellore Campus. This campus has more than 20,000 students every year. Thus, there is a lot of data that is available of all the students, its faculty members and the staff members as well. This research project was conducted in coordination with the VIT Vellore Center of Technical Support Department. The Centre for Technical Support (CTS) is responsible for the policies that regulate the usage of VIT computing and IT communication resources. The IT Policy applies to administrative department resources such as the Library, Computer Laboratories, Institutional Offices, Hostels and Guest Houses when the Institution provides network access. VIT's IT system is extensively distributed, linking 56 buildings over a very high-speed, durable network backbone. The computer network is currently developed on a CISCO switching platform with a 10Gig backbone. This fast network is home to over 12000 IP-enabled devices. Understanding the need for academics and students to use digital media in their research, teaching, and learning, three major Internet service providers, BSNL, JIO, and AIRTEL, have made 10Gbps of internet bandwidth accessible. An average annual budget of Rs.17.87 Crore spent on developing the university demonstrates the management's dedication to establishing a world-class IT facility on the campus. (Comprising the Vellore and Chennai campuses' capital and operational budgets) The complete infrastructure comprises 68 physical servers with 366TB of storage for Private Cloud, 220+ Virtual Machines, and 500 Virtual Desktop Infrastructure (VDI) deployed enabling students to work with engineering software from any device at anytime, anywhere.

Fig 1 Network Architecture within domain



Data collection and inferences

In order to properly audit the information security system and network architecture, team leads and director of CTS (Center of Technical Support) were approached. As the data that we are dealing with is sensitive, it was important for us to keep the questionnaire to a certain level. Any kind of sensitive information is not revealed which can be used to identify the vulnerabilities/risks in the network and system architecture of the organization. VIT has implemented some of the best practices to enhance student data security and safeguard all the assets in VIT. There anr multiple layers of security, a strong backup system and an alternative to all failure mechanisms. The data center in VIT is one of the best data centers located in India. Some of the mentioned questions and information

FUNCTION	CATEGORY	QUESTION	SOLUTION
IDENTIFICATION OF THREAT/ RISK	Asset Management: The data, staff, tools, systems, and facilities that enable the	How many devices can be connected to one given network?	There is no limit to devices connected. On average one domain connects to 3000 devices.

	company to execute its goals are recognized and managed in accordance with their relative relevance to the organization's goals and risk management plan.	What is the limit for software platforms accessible on devices?	There is no limit to platforms accessible. On average, there are 200 applications accessible on network desktops. Even though the number is not limited, .exe files can only be downloaded with right permissions.
		How does internal communication take place?	Internal communication within the security department is conveyed from employees to team leads and then to higher authorities.
		How is complexity defined within a domain?	The systems in the various domains are complex due to the huge number of users and connected devices.
		How are roles and responsibilities distributed?	Network security department handles risks and threats regarding network security.
	Business Environment: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities,	What are the major threats possible in university?	General threats like Phishing, email-spamming, Malware, etc. are possible in the University system
		How is the priority of the security threat determined?	The server detecting vulnerabilities provides top 20 problems from each domain and it is then manually checked to confirm if any threat is severe. It is a fully automated process

	and risk management decisions.		and corrected by the server. Only the top 5 critical issues are checked manually.
		What are the critical services provided to permit certain requirements?	Multiple firewalls are implemented at each communication to implement access lists at each point. There are redundant devices as well.
	Governance: The policies, procedures, and processes used to monitor and manage the institution's regulatory, legal, risk, environmental, and operational requirements are recognized and used to advise cybersecurity risk management.	How are the organizational cybersecurity policies established and communicated?	A committee is set to create new frameworks and policies. It is communicated inter-domain via the team leads.
		How are the cybersecurity roles and responsibilities coordinated and aligned with internal roles and external partners	Team leads are responsible for communicating across domains and to registrar and Director.
		How are cybersecurity legal and regulatory responsibilities, including privacy and civil liberties duties, are recognized and managed.	Legal and regulatory knowledge is shared from Registrar to group of Lawyers. The CTS department is not involved in the legal activities.
		How are cybersecurity risks governed?	Details of cyber activities are managed by the network security department.
	Risk Assessment: How the institute handles cybersecurity risk to organizational operations (such as mission, functions, image, or reputation),	How are the vulnerabilities in the system identified and documented	The vulnerabilities are scanned automatically by a server regularly to show any minor/major threat to the system.
		How are risk responses identified?	Soon after the risk is conveyed by the server, the top 20 are manually checked to identify the severity and impact.

	assets, and people.		
	Risk Management Strategy: Priorities, limits, risk tolerances, and assumptions for the organization are defined and utilized to support operational risk choices.	How is the sensitive data identified and managed?	Almost all the data regarding students and transitions is sensitive. These use strict authentication methods to restrict access to unauthorized personnel.
		How is the organizational risk tolerance determined and expressed	The university has low tolerance for any kinds of risks. Once an incident is noted, actions are taken within minutes.
		How is data protected from 3rd parties like banks or other organizations?	No third party has access within the system under any circumstances. They require an authorized device and double verification to do so.
PROTECTION	Identity Management, Authentication and Access Control: Access to physical and logical assets, as well as related facilities, is restricted to authorized people, processes, and devices, and is controlled in accordance with the risk of unauthorized access to approved activities and transactions.	How are identities and credentials of authorized individuals issued, managed, verified, revoked, and audited?	The university implements its own authentication system.
		How is network integrity protected in the system?	Network is monitored efficiently with network segmentation. Each domain has a set of rules to follow.
		How are network permissions handled?	Framework to permit authorized users are applied throughout the organization. Access is managed on the basis of separation of duties.
		How are physical devices protected/ authenticated?	Each device within the network requires valid credentials to login. To access WIFI networks/ other network

			settings, further authentication is required.
	Awareness and Training: Personnel and partners of the business get cybersecurity awareness education and are educated to fulfill their cybersecurity-related activities and obligations in accordance with associated rules, procedures, and agreements.	How are all users informed and trained of protocols?	The users are made aware of their login credentials to access the networks. Unauthorized users have no access to any device or network.
		Who are the privileged users? What are their roles and responsibilities?	The team leads can access the settings inside the network. The director and registrar can also access these settings.
		Who are the third-party stakeholders?	No other than team leads can access the network security settings. Third party is provided with a separate university device with predefined settings.
		How are cybersecurity roles and responsibilities distributed?	The entire security is divided into 3 teams. One handles network security, the other handles infrastructure and the other handles hardware.
	Data Security: To ensure the confidentiality, integrity, and availability of information, information and records are handled in accordance with the organization's risk plan.	How is the data-at-rest protected?	Data is stored in various different locations including the university's Private cloud.
		How is the data-in-transit protected?	Traveling data is protected by firewalls and Anti-malware software.
		How are the assets managed throughout removal, transfers, and disposition?	Data assets are managed using authentication and firewalls. There is also cyber-insurance to protect the overall

			security. Physical assets are protected with CCTV security systems.
		What is the asset capacity? How is it protected?	There is no upper limit to devices or data that can be connected to a domain. They are all connected via VLAN in the system.
		How are protections against data leaks implemented?	Data leaks are managed by the software development department?
		Integrity checking mechanisms are used to verify software, firmware, and information integrity?	There is a separate automated server dedicated to check the logs of top 20 activities
		How is the development and testing environment protected?	There are periodic checks conducted by the CTS staff and any anomaly is reported to the Team Leads
	Information Protection Processes and Procedures: To manage the protection of information systems and assets, security policies (that address the objective, scope, roles, duties, management commitment, and coordination across organizational entities), protocols, and procedures are	What is the general procedure to protect the control systems and the management systems in the university?	Any attacks from the outside have to pass through two layers of firewall. There are 8 security checks at every level.
		How are the data backups maintained?	Data is backed up every day automatically by the servers.
		Are there any configuration change control protocols?	Yes, there are protocols to support all the functions.
		Are the response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) analyzed and tested?	The plans are well laid out and are tested periodically. There are annual maintenance checkers and other activities to audit the response plans.

	maintained and used.	Are there policies and regulations regarding the physical operating environment for organizational assets. How are they managed?	There are well laid out policies in every aspect of network security and systems security. The CTS manages these policies.
		How is the removable data/ data that is required temporarily managed?	The VIT Data center is the main data center which has all the data views. The temporary data is deleted.
		How are protection processes improved? How often does the process take place?	VIT software patches are conducted in coordination with OEMs. Updating and improvement occurs with every update and annually.
		How is the effectiveness of protection technologies analyzed?	Several parameters are analyzed like server downtime, number of detected anomalies, etc.
		How are vulnerabilities detected in the system? How is vulnerability management plan developed and implemented?	Event logs of all the activities are analyzed by an automated server.
	Maintenance: Industrial control as well as information system components are maintained and repaired in accordance with rules and procedures.	How is the maintenance and repair of organizational assets performed and logged? Who approves the operations?	Internal maintenance and repair are taken care of by CTS, if any complicated issue occurs, OEM is contacted. The approval is done by CTS team leads, director and registrar
		How is the remote maintenance of organizational assets approved, logged, and performed? For university's remote branches, where is all the functioning managed?	Each domain has its team and officials who manage the assets, logs and performance. VIT has 4 branches; each branch has its own CTS department which manages their respective branch.

	Protective Technology: Technical security solutions are handled in accordance with applicable policies, procedures, and agreements to strengthen the safety and robustness of systems and assets.	How are the logs and records determined, documented, implemented, and reviewed?	There are well laid policies for documenting and logging the events. Most of the work is automated and handled by the server.
		The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The Principle of Least functionality is incorporated in the end devices but servers and switches don't implement it.
		How are the communications and control networks protected?	There is 8 points of security including two firewalls, endpoint security, DNS security, VLAN security and others.
		What mechanisms are implemented to safeguard the system when it needs resilience in both regular and unfavorable conditions	Hot swapping and load balancing is implemented. Thus, in any kind of unfavorable conditions backup and alternative is available.
DETECTION	Anomalies and Events: Unusual activity is recognized, and the possible significance of occurrences are comprehended.	Who analyses vulnerabilities and anomalous events?	A dedicated server is responsible for analyzing system vulnerabilities and anomalous events.
		How are detected events analyzed to understand attack targets and methods?	Once the server logs the critical activities, they are manually reviewed by CTS team to check for attacks and possible methods of attacks
		How is the occurred event data collected and how is it correlated to multiple sources and sensors?	Every event is logged in detail. From the most inactive endpoint device to the most active switch. Every log is backed up and kept for a specified

			time duration and eventually deleted.
		How is the severity/ impact of the occurred event analyzed?	Policy document lists the threat level and impact level of all the events. Action is taken based on the policies.
		How are alerts given out to staff regarding an occurred event? Does a threshold exist for the alerts?	Alerts are given through phone notifications and email-based notifications. Yes, threshold based on event critical level and occurrence frequency.
	Security Continuous Monitoring: The security framework as well as resources are monitored in order to detect cybersecurity incidents and ensure that defensive measures are effective.	How is the network monitored to detect any potential cybersecurity events?	Everything is automated and very little manual intervention is required. If a potential threat is detected, it's notification is sent to the team for review and necessary action is taken.
		How is the physical environment monitored?	Every domain has staff members assigned to monitor the physical environment.
		How is Malicious code, Malware, unauthorized access, threats detected?	VIT follows a strict policy on which files are allowed to enter the network and download to the end devices. If a file consists of .exe format, it becomes a serious potential threat.
		In case external service provider activity is implemented, how is it monitored?	In the case of an external service provider, VIT will make sure all the connected devices

			from the eternal service are safe. VIT never allows any external device to get connected to their network. They implement external services through their own devices.
		How frequently vulnerability scans are performed?	VIT has annual vulnerability scans. Apart from that, a server is always checking and reporting anomalies.
	Detection Processes: To guarantee knowledge of anomalous events, detection systems and procedures are established and evaluated.	How are roles and responsibility divided in order to maintain and look out for procedures ensuring protocols regarding detection of threats.	Threat detection is automated. As for the roles, CTS has team members, team leads, assistant directors, directors. The approval also comes from the registrar.
		How often are the detection processes tested and verified?	Detection and testing occur periodically. Depending on the situation, it may happen on a weekly or monthly basis.
		Are the detection processes continuously improved based on past events?	In case any event is detected, it is logged and marked critical. After the incident response, the framework is improved to mitigate similar attacks.
RESPONSE	Response Planning: Response methodologies are implemented and maintained to guarantee that identified cybersecurity issues are addressed.	When is the response plan executed? Is this response plan executed during or after an incident?	Response plan has its phases. Depending on the severity of the event. If immediate action is needed, it is taken to avoid further damage. Soon after the event occurs, incident response policy is also carried out.

	Communications: Internal and external stakeholders collaborate to coordinate response operations. For instance, external support is ensured from the law enforcement agencies.	How are roles and responsibilities distributed for the Response plan execution? Who is reported regarding the incident?	There is a separate team for incident response and management. A strict hierarchy is followed for reporting incidents. Finally, the team leads and directors take the decision.
		What are the policies regarding response plans?	Each event, threat, action and asset handling have its own set of policies.
		Is any voluntary information sharing conducted with external stakeholders to achieve broader cybersecurity situational awareness? Who is approached for the stated purpose?	Only the OEM is contacted in case of any external contact. No other third party is given data. No kind of information sharing takes place to third parties.
	Analysis: Analysis is carried out to verify that the reaction is successful and that recovery efforts are encouraged.	How are notifications from detection systems circulated and investigated?	Depending on the kind of threat/incident, notifications are sent to appropriate people. Some are sent to all. Some are not sent to all depending on the confidentiality of the notification.
		How is the impact of the response plan analyzed?	No severe incident has occurred in VIT yet. Impact is analyzed based on which data is compromised.
		Are any kinds of forensics performed to validate the response plan?	If the impact of the incident is high, only then forensics is performed, else it is usually left to the automated response software.
		How are processes conducted to respond to vulnerabilities? How are	The vulnerability testing is a completely automated process.

		they integrated into policies?	Once they are tested and analyzed, they are updated to policies based on severity level.
	Mitigation: Operations are carried out to prevent an event from escalating, to reduce its impacts, and to eventually resolve the incident.	How are the high impact incidents contained? How is any further related threat avoided?	All the endpoints and networks with the endpoints are isolated. Then the response is taken.
		How are the incidents mitigated?	Incidents are mitigated based on predefined policies. Each incident has a threat/impact segment. Based on that incident mitigation is done.
		When are the newly identified vulnerabilities that mitigated or documented as accepted risks included into the policy framework?	The newly identified risks are included once the threat is mitigated. After analyzing all the aspects of the risk are studied and then included in the policy.
	Improvements: Lessons acquired from current and historical detection/reaction actions are used to enhance organizational response operations.	Are the response plans revised? How often are the policies altered?	The response plan is updated and improved annually based on even minute risks or threats experienced.
		How are the response strategies updated?	There has been no major attack but the response strategies are updated periodically
RECOVER (RC)	Recovery Planning: To ensure the restoration of systems or assets damaged by cybersecurity events, recovery protocols and procedures are	Is the recovery plan executed during or after the cybersecurity incident has occurred?	University has a strong recovery team that reacts within minutes of incident

	implemented and maintained.		
	Improvements: Lessons acquired are incorporated into future initiatives to enhance recovery plans and processes.	How are recovery plans incorporated and updated?	Soon after the incident, new frameworks are set based on occurred incident. Updating response plans occurs annually irrespective of attacks.
	Communications: Activities for restoration are coordinated with both internal and external stakeholders (e.g., Coordinating centers, owners of attacking systems, victims, Internet Service Providers, other CSIRTs, and vendors).	How is reputation and integrity managed after an incident	The declaration of incident and incident response is managed by the network security department. The information is not leaked outside university or within other members.

Conclusion

The research conducted by the authors have focused at the VIT network security and information security architecture, as well as the regulations that govern it. VIT Vellore and its branches have established one of the most safe information security frameworks based on our research. It is an extremely sophisticated network with a complicated architecture. It features several firewalls and backups, as well as around 8 checkpoints, such as endpoint security, switch security, and firewall. VIT offers one of the most modern data centres, its own cloud data storage, as well as data management and encryption. Moreover, with such a strong commitment to information security

and rules, VIT is a highly secure university that is concerned about the data security of its students. As students of this prestigious university, the authors are bound to not release all of the material due to confidentiality concerns and time. Future work in this area has a huge scope and has a wide range of possibilities. Furthermore, several components of the audit can have an extended analysis, such as risk assessment, full network security analysis, and several other aspects.

Acknowledgement

We thank the CTS department of Vellore Institute of Technology for permitting us and guiding us through the auditing process and explaining all the aspects of the university's security system. We shall be failing in our duties if we don't record our deepest sense of gratitude to Prof. Mohan Kumar, Assistant Director System, and Mr. Paul Sir, Assistant Manager, for giving their precioustime for the survey that has been briefed in the research. Their untiring efforts to develop and studythis colossal network system of VIT inspired us much.

We are highly indebted to our mentor and Professor Lavanya K, her scholastic guidance for the completion of this research work. We offer our humble thanks to the authorities of Vellore Institute of Technology, Vellore for allowing us to do research. We take this opportunity to express our thanks to all the experts and authors of the books whose references have been of immense help in our research. Once again We thank all authorities and experts, who directly or indirectly helped us in completing this elephantine task in time- bound work.

References

[1] Kusumarini, A. I., & Seta, H. B. (2021). Information System Security Analysis to DetermineServer Security Vulnerability with Penetration Testing Execution Standard (PTES) Method at VWX University. 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS, Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2021 International Conference On, 7–12. https://doi.org/10.1109/ICIMCIS53775.2021.9699285

[2] Shambabi, P. T., Musarurwa, S., & Shava, F. B. (2021). Assessing Organisational Information Security Culture Among Workforce in Universities: A Case of Namibia. 2021 IST-Africa Conference (IST-Africa), IST-Africa Conference (IST-Africa), 2021, 1–8.

Putra, I. M. M., & Mutijarsa, K. (2021). Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), Computer and InformationTechnology (EIConCIT), 2021 3rd East Indonesia Conference On, 14–19. https://doi.org/10.1109/EIConCIT50028.2021.9431865

[3] Di, W. (2020). Analysis and Countermeasure on Information Security in Universities. 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), Safe Production and Informatization (IICSPI), 2020 IEEE 3rd International Conference Of, 439–

442.https://doi.org/10.1109/IICSPI51290.2020.9332466

[4] Angraini, Alinda Alias, R., & Okfalisa, O. (2019). Need for Compliance With Information Security Policy In Universities: a Preliminary survey. 2019 Fourth International Conference on Informatics and Computing (ICIC), Informatics and Computing (ICIC), 2019 Fourth International Conference On, 1–6. https://doi.org/10.1109/ICIC47613.2019.8985949

[5] Sun, W., & Wu, L. (2019). Research on network and information security in Colleges andUniversities. 2019 International Conference on Information Technology and Computer Application (ITCA), Information Technology and Computer Application (ITCA), 2019 International Conference On, 292–295. https://doi.org/10.1109/ITCA49981.2019.00071

[6] Joshi, C., & Singh, U. K. (2016). Quantitative Information Security Risk Assessment Modelfor University Computing Environment. 2016 International Conference on Information Technology (ICIT), Information Technology (ICIT), 2016 International Conference on, ICIT, 69–74. https://doi.org/10.1109/ICIT.2016.026

[7] Nie, J., & Dai, X. (2016). On the Information Security Issue in the Information ConstructionProcess of Colleges and Universities. 2016 12th International Conference on Computational Intelligence and Security (CIS), Computational Intelligence and Security (CIS), 2016 12th International Conference on, CIS, 582–585. https://doi.org/10.1109/CIS.2016.0141

[8] Xian Weiquan, Wang Houkui, He Haoyi, & Zheng Donghong. (2012). The Analysis of University Network Information Security System Based on Level Protection Model. 2012 EighthInternational Conference on Computational Intelligence and Security, Computational Intelligence and Security (CIS), 2012 Eighth International Conference on, Computational Intelligence and Security (CIS), 2010 International Conference On, 609–614. https://doi.org/10.1109/CIS.2012.142

[9] Ho-Yeol Kwon. (2008). Security Engineering in IT Governance for University InformationSystem. 2008 International Conference on Information Security and Assurance (Isa 2008), Information Security and Assurance, 2008. ISA 2008. International Conference On, 501–504. https://doi.org/10.1109/ISA.2008.93

[10] Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

[11] Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between ownperception and reality – an empirical study. Accounting & Management Information Systems / Contabilitate Si Informatica de Gestiune, 15(1), 112–130.

[12] Jake Weidman, & Jens Grossklags. (2019). Assessing the current state of information security policies in academic organizations. Information & Computer Security, 28(3), 423–444.https://doi.org/10.1108/ICS-12-2018-0142

[13] Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. Education & Information Technologies, 26(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

[14] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017).The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

[15] Daneshmandnia, A. (2019). The influence of organizational culture on informationgovernance effectiveness. Records Management Journal, 29(1), 18–41. https://doi.org/10.1108/RMJ-09-2018-0033

[16] Haywood, M. E. (2021). Making the Grade: Using COBIT to Study Computer Crime at Bucks County Community College (Pennsylvania). Journal of Information Systems Education,32(2), 115–118.