A Secure Approach to Academic Websites and their Services

Hao Shu, Francois Van Laer, Matthew Cowell, Kartikeya Shukla
Department of Computer Science, NYU Tandon
Brooklyn, NY
USA

Abstract – This paper is intended to provide useful information to IT professionals and school administrators who are interested in designing a security system for an higher level educational institution. The security framework provided below is a set of guidelines with a comprehensive set of security ideas. We emphasize important strategies for consideration when implementing a higher education system. Professionals, who do not have experience in information security, will be able to use our guidelines to fortify their infrastructure and assets. Since each educational institution is unique, customized security systems should be implemented in each individual university. Therefore, there is no single optimal solution. Instead, this paper emphasizes typical factors to consider, such as analyzing common practices that are currently in use and recommend outreach in aspects that require optimization. Similarly, since absolute protection is not possible, the recommendations made are offered as general guidance to help educational institutions make informed security decisions. The primary goal of these recommendations is to help protect the data of users and employees of a generalized university setting by providing guidelines to build a secure system, in which active threats and potential danger can be mitigated.

Keywords **–** Academics, Analysis, Governance, Policy, Risk, Security, Services, System, Threats, Vulnerabilities

I. Introduction

Nowadays, educational institutions face a myriad of challenging hazards and threats. In addition to natural and technological threats, they now have to prepare for human-caused cyber threats. These incidents can be accidental or deliberate, and in turn cause disruption for the education of the students and critical operations of the university. Data collection and management have become a vital resource for schools across the world with the rise of technology and digitized information. These records, which can include a student's personal information to test scores and behavioral assessments to financial data, are highly sensitive in nature. Though some universities continue to collect student data on paper, stashing it away in filing cabinets or off-site facilities, many more are now collecting and storing this information digitally on local networks and databases. The most modern of these higher education institutions store their information on cloud systems. This shift mirrors what is happening inside the classroom, as many schools have adopted new technology and learning systems into their curricula. The shift to modern data collection, while integral to the student and institutions, also invites incredible risks considering the sheer amount of personal data that is being aggregated on networks. Taken as a whole, a student's personal record can offer malicious entities a look into a the student's life. These files can contain more public information, such as the location of their home, to more private details, such as personal health and financial data. These records can also contain information critical to the institution, such as the student's attendance, instructor assessments, administrative observations, etc.

Alarmingly, out of 17 industries in the U.S., education comes last in terms of total cybersecurity. This should be a cause for serious concern among students, parents, school boards, and the education industry as a whole. Nonetheless, despite the

ubiquity of data collection and the ever increasing number of schools nationwide storing data digitally, many higher education institutions are not doing their part to protect its students, employees, and the institutions themselves from such risks. SecurityScorecard analyzed 2393 companies with a footprint of 100 IP addresses or more in the education industry, from April 2018 to October 2018, and found the following: [1]

- "The education industry was the lowest performer in terms of cybersecurity compared to all other major industries.
- The education industry performed poorly in patching cadence, application security, and network security.
- There are several regulatory requirements for cybersecurity performance to improve in the education industry"

As the previous research showed, academic institutions are far behind in terms of system security. Moreover, not only do education institutions often fail to protect the privacy of its community members, they also often overlook the importance of keeping a system secure. This situation is exacerbated with the fact that usual secure engineering is customized for one particular institute, and the fact that the majority of users are unaware of the situation. To combat the problem stated above, we decided to redefine a specific secure engineering methodology, and create our own generalized security approach, that can be implemented by any general higher educational institution. Our research concentrates on the progresses and procedures an education institute can follow to satisfy general industry security standards. To achieve our objectives, our examination lays out generalized secure system requirements, from privilege level to risk analysis. Then, our research continues to explore the specifics around the particular institution, such as the system structure and classification process. This system, its guidelines, and the reasoning behind them are explained below.

II. Background

When anyone looks into the security of an information system, they are bound to come across the CIA triad, and our research was no different. This triad focuses on the ideas of confidentiality, integrity, and availability. All three of these are key to any system, in order to provide these three services to our users and their data. Confidentiality is used to protect the data of users from the prying eyes of unwanted or unprivileged observers. This is usually done by implementing a data privilege hierarchy that runs on the concept of least privilege, and then uses identification, authentication, and authorization to determine the privileges an individual may have. When looking at the data an institution will be controlling and maintaining, we can see that there are many categories of data with varying levels of restrictions and access controls to be implemented. Integrity of the data should also be ensured while it is within the institution's control, such as on host devices, servers, and on the university's network itself. By providing this integrity, we can ensure that only privileged changes are made to user data. This ensures that only users can change their own data, and that the systems that manage the data do not have unauthorized changes added into data that might affect the system itself. The way one provides integrity can be done in many ways. The two most common ways are access controls allowing write privileges to designated individuals and checksums, which occur in data transfers and encryption methods. Availability is key for any organization to maintain, and higher education institutions are no different. The need for students and employees to access their data and the university's data is key. For this reason, this service must be protected by providing only approved network access and prevent

threats that exploit availability, such as denial of service attacks. [2]

The CIA triad is a critical and general approach to ensure the protection of higher educational institutions and, as a result, our guidelines will start with the individual university analyzing its own data and systems with respect to the CIA triad of confidentiality, integrity, and availability.

The next step in our background research was to analyze higher education websites and their information security policies. To do this, we looked at the universities of LIU, NYU, and Columbia University. We chose NYU because we wanted to analyze the information security policies of our home university in more depth. However, we felt that basing our reasoning off one university did not produce enough substantial material, that we needed additional evidence to fully grasp the scope of this project. For this reason, we decided to compare NYU's policies with the policies of two other universities in the area: LIU and Columbia University.

LIU has a very general and short information security policy. It covers the ideas of access to the university's computers, terms of use for systems and data, email responsibilities, copyrighting, and respecting the right of other users and data. These are not very well defined, so we felt that many readers and users would have questions about each one of these sections. Also, this lack of definition would most likely lead to misconfigured, inadequately maintained, and poorly documented system. [3]

On the other hand, Columbia and NYU have extremely organized documents that cover various parts of their information security policies. When compared with LIU, our research showed that these two universities provide new categories for information policies, such as risk management policies and breach notification policies. One significant area that both universities also delve into is the management and classification of data. Columbia and NYU have many policies in the previously mentioned area, which outline the specifics behind the types of data being stored on their systems, how the data is protected, the retention rate of data, and the disposal of data. [4] NYU even gives simple instructions and advice about ways to implement better security for students on their mobile devices, laptops, and peer-to-peer connections. [5] Thus, the information security policies of Columbia and NYU directed parts of our research, especially the classification of our system's data.

Most systems also focus on a series of very well-defined guidelines that come from a set of security standards. While our system will implement a generalized version of a scheme for any university, we realized that we would also need to base some of our research on an already built set of standards. This would lead to our identification of areas of significance within a secure information infrastructure.

ISO, International Organization for Standardization, model for information security and systems, is very in-depth and well researched. The breadth of materials contained within ISO 27000, from the 2018 updates, covers material from information processing to life cycle management to wireless subnetworks. However, with all of this information, we found it hard to analyze ISO's standards because of the expansiveness of the material. Indeed, about fifty or so guideline papers are relevant to our system. We felt that, given the massive amount of subject matter, many institutions and their employees were not likely to read these papers, implement every policy, and maintain all the documentations of their system, with respect to the ISO model. It would take the IT and Infosec teams away from general maintenance and issues on a day-

to-day basis. This would not be because of a lack of caring or security awareness, but rather due to time constraints generated by the process. [6]

NIST, National Institute of Standards and Technology, has its own set of standards and framework. We studied their cybersecurity framework and found that its specifications focused heavily on the business operations and executive side of the organization in question. An example of such rules can be observed by the way NIST approaches governance, and the categorization of functions and unique identifiers for a cybersecurity environment. While these standards would be helpful for any organization to follow, they would not effectively help our research on the technical side. [7]

We decided to concentrate on the standards set forth by OWASP ASVS, which is the Open Web Application Security Project that addresses an Application Security Verification Standard. ASVS has many ideas about the security of websites, software, and hardware, as well as data management techniques, which we wanted to integrate into our design. When looking into OWASP ASVS in more detail, these guidelines discuss many checklists that can be helpful to the average IT employee or even non-tech-savvy executives. Many checklists could prove to be helpful for these individuals, such as: access control architectural requirements, data protection and privacy architectural requirements, single- and multi-factor one time verifier requirements. These are only a few of the checklists that we looked into. However, these were the ones supporting us in the development of guidelines for our system. Access controls architectural requirements helped us understand how we should distribute privileges within our system, thus protecting data confidentiality. Data protection and privacy architectural requirements enabled us to categorize the data for any higher education institutions. Lastly, single- and multi-factor one time verifier requirements assisted up into pinpointing more in-depth access controls, such as two-factor authentication, that can be used in our system. [8]

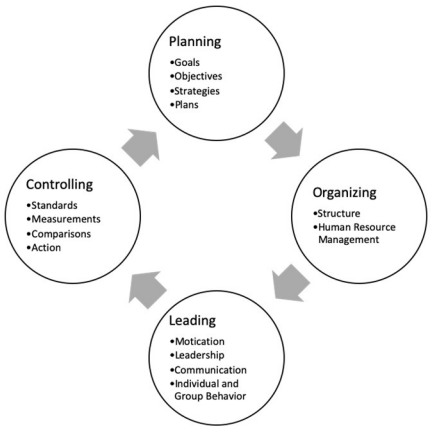

Figure 1: Old life cycle for implementing a secure system

Figure 2: Revamped life cycle for implementing our guidelines for a secure system

Once we established the standards required for the system, we proposed guidelines on how a university could implement our system. This required a cross-examination of different system components, which was accomplished through a life cycle chart. In Figure 1, we can see the life cycle chart is made up of four categories. These categories are used to help managers deal with the creation of systems and tasks**.** [9] However, this life cycle is beyond the scope of our project given that it also focuses on the organization and leadership within the company, which we do not necessarily have access

to. Thus, this life cycle is impractical for us to use, since our system focuses on a generalized model for any university, and not one specific university.

This lead us to the development of a new life cycle that our system would follow. This life cycle needed to suit our specific needs for a secure system implementation, while also providing a broad sense of malleability in order to allow any university to implement it. For this reason, we created a life cycle that focuses on planning, implementing, and updating. This life cycle can be seen in Figure 2. Planning allows any university to analyze their own business goals that they want to achieve with our secure system. This will require planning on the administrators part, in order to determine how to best to incorporate security with other core technological ideas, such as usability and availability. This will also require the analysis and classification of assets, threats, etc. to ensure that all aspects of the university and its security needs are accounted for. Once this process is completed, the university can implement the system we are outlining in this paper, which will guide the security side of the university's infrastructure. This implementation is done through various avenues, such as information storage methods, access controls, incident response, etc. Finally, our system guidelines define the steps needed for these higher education administrators to maintain and update their own secure version of our system.

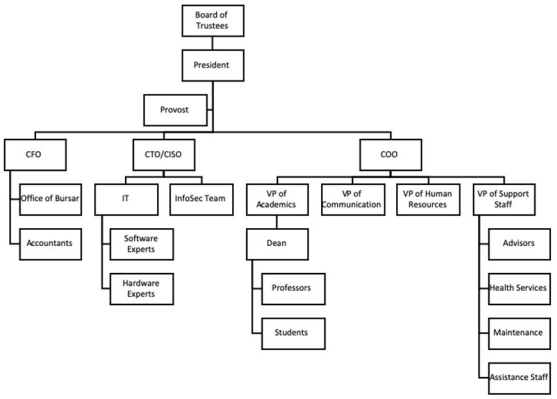

Figure 3: Governance hierarchy of higher education institutions

Although leadership and governance were less practical to apply to our system design and life cycle because we did not focus on a specific university, both principles are essential for any organization. In Figure 3, we conceptualized the most common governance hierarchy that could be seen in a generalized university infrastructure. Here, we can see the hierarchy starts at the board of trustees then leads to the president and provost. [10] Beneath them, C-level executives control the management of a specific area. The key area of focus is the information side of the university that would be controlled by a CTO. Most likely, he would also be the CISO given the size of the university and the lack of funding and experience required. This executive would thus control all information assets, software and hardware, as well as managing the specialized InfoSec team for the university.

III. Development

After analyzing the CIA triad and OWASP standards, we began to form the base concepts of the actual system itself.

Entity Classification

Subsequently, we determined all of the users that would operate, and have access to, some part of

the university's system. Overall, we determined that there are seven groups of users called entities. The entities within our system are: students, instructors, advisors, registrar, office of bursar, IT, and system admins. Each of these entities would have some kind of access to numerous actions, which we termed as capabilities, on the various subsystems. The type of access would be full access, limited time access, or viewing only access. This access would determine privilege in the system in order to dictate how the user would interact with each of the capabilities. We have seven capabilities, which are the data forms each entity can have access to. These capabilities are: financial, grades, credential access, registration, change in permission level, academic records, and system controls.

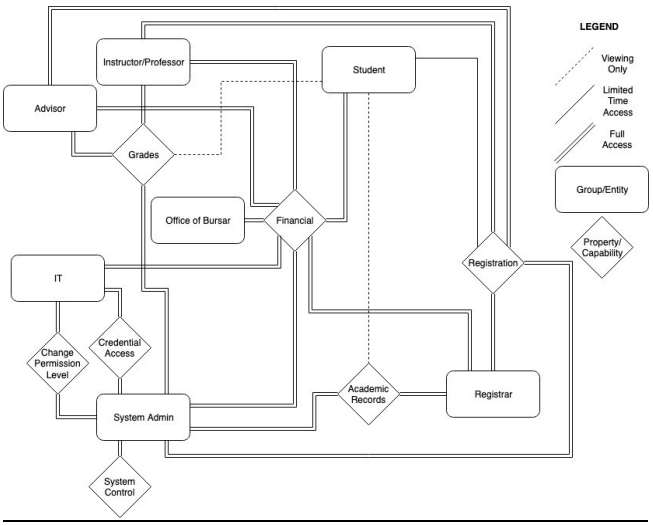

Figure 4: Entity diagram

It can be inferred from Figure 4, that there is a multitude of capabilities for each entity, therefore demonstrating the need for access control in a generalized university's system. These access controls should isolate both users and systems. Isolation will allow for users to only access the data and systems that they are privileged to access. For instance, students should only have access to the systems that revolve around financial data, grades, registration, and academic records. However, regarding financials, grades, and academic records, they should only be allowed to access their own. As for registration, students have access to the registration system for a specific amount of time, which occurs during the registration period of the university.

Property / Capability	Student	Instructor	Advisor (Instructor)	Registrar	Office of Bursar	IT	System Admins
Financial	X (own)	X (own)	X (own)	X (own)	X (all)	X (own)	X (all)
Grades	X (view their own grades only)	X (view and edit grades of multiple students)	X (view all grades)				X
Credential Access						X	X
Registration	X (Limited)	X	X	X			X
Change permission level						X (can change permission lvl down and up to their level)	X (can provide higher levels of access)
Academic Records (SSN, etc.)	X (own)			X			X
System Control							X

Figure 5: Chain of command

Figure 5 is the chain of command, which shows the tabular representation of the entity diagram in Figure 4. With this table, one can better observe the relationship between the entities and their capabilities. The entities have varying levels of capabilities, from the Office of Bursar, which only has access to the financial data of all of the employees and students at the university, to the system administrators, who have access to all data on all systems in the university's information infrastructure. On the capability side, only a select few entities have access to the system's control and credential data, albeit all entities should have some form of access right to financial data.

Data Classification

Information Assets	Data Classification	Impact if Compromised
Financial	Restricted	High
Grades	Confidential	Low
Credentials	Restricted	High
Registration Information	Internal	Medium
Academic Records	Restricted	Medium
Personal Public Information	Public	Low
University Website Information	Public	Low

Figure 6: Data classification

After creating the entity diagram, and establishing relationships between users, data, and the subsystems, we analyzed the data that our system would be handling. Afterwards, we narrowed down all of that data to only what a university would be managing. Much of these data categories come from the entity diagram categories. However, a few more are data categories mentioned here. The reasoning behind this is that our system focuses around keeping information private within the university's network. However, most universities and companies contain a public server with accessible data, outside of their network.

Figure 6 presents all seven data categories: financial data, grades, credentials, registration information, academic records, personal public information, and university website information. Each of these data types can have one of four types of classifications. These classifications were dependent upon how private the information is to either the user or the university. These classifications are: public, internal, confidential, and restricted. Public information is classified by information the university has on their servers. However, given that data can be found elsewhere, more lenient security measures can be introduced. On the other side, restricted data should be protected at all times by the university with the use of access controls and encryption. This is because this information is very private and could have a major impact on the users or university if this data were to be compromised (the rightmost column of Figure 6). The repercussions that can occur can be financial, legal, reputational, etc.

In Figure 6, we can see that the data that needs to be protected the most needs to be financial and credential data. This is because both of these data types have restricted access and are likely to have a high impact if either of them were to be compromised. Personal public information, such as home address, as well as university website information, such as degrees offered, are not as vital to protect because of their low repercussions and their abundant access across the Internet.

Asset Classification

High Tolerance	Moderate Tolerance	Low Tolerance
1. The unauthorized use, access to the asset would not have impact on our system's operation.	1. The unauthorized use, access to the asset would impact some of our system's operation. 2. The risk associated with the asset is transferred, well-estimated, mitigated, controlled.	1. The unauthorized use, alteration, access to the asset would bring disastrous consequences to our system's operation. 2. The exploits of an asset can greatly undermine the overall security of our system. 3. The misuse, or unauthorized operation of an asset can break the governance guidelines and legal regulations.

Figure 7: Asset risk tolerance level

Assets	Example	Value	Risk Tolerance
People	Internal or external personnel	3	Moderate
Procedure	Business-sensitive procedure and policy	2	Moderate
Data	Network traffic and database records	5	Low
Software	Applications, OS, and software security measures	4	Low
Hardware	Equipment and hardware security measures	4	Low
Networking	LAN components Internet components Network security measures	4	Low

Figure 8: Asset classification

"An information asset is defined as any resource that collects, stores, processes, or transmits information, or any collection, set, or database of information that is of value to our system." [9] It is not easy to precisely identify all the assets within an organization. Our methods to identify and classify information assets are primarily based on the information asset model in "Management of Information Security" [9]

In "*Information Asset Value Quantification Expanded"*, it is stated that "Valuation of information as an asset relies upon both tangible and intangible valuation measures to create a linkage between the organizational mission and the supporting Information asset". [11] Indeed, asset valuation involves many calculations and can be complex to determine. Asset valuation can also be surprisingly subjective, let alone some assets' value is infeasible to define. For instance, it is impractical to define the value of a small paper file. The small file is an asset, albeit it doesn't have a meaningful monetary value or significance. Moreover, it is not feasible to assign value to every asset. The operation is too time-consuming and less cost-efficient. Hence, we classified our assets into groups, and each group was assigned a value.

Our people assets consist of internal personnel and external personnel. Internal personnel includes our staffs, IT administrators, etc., while external personnel includes trusted vendors, external auditing personnel, etc. Our procedure assets are information that creates value for our system's operation. For instance, IT sensitive procedures mandate the secure handling of data of our system. Procedure assets also include our business policies that direct university personnel, and other policies that are open to the public for transparency. Our data assets include information in all states: transmission, processing, and storage. For instance, network traffic in transmission, student payment data in processing, student records in storage, are all confidential or restricted data assets of our system. Software assets are applications such as operating system running on our servers, security measures on servers, etc. Software assets provide our system's hardware devices with control and abstraction. Similarly, our hardware assets include hardware devices such as servers, databases, etc. Basically, hardware assets provide our system with platforms that enable our system to offer key higher education services. Our network assets consist of network devices, such as routers, switches, etc. Network assets provide our system with a path that enables the communication and interaction between other hardware devices. It is undeniable that network assets can be classified as hardware assets. However, we separated them because networks assets are often the frontline of defense, and deal with data on a software basis. We believe this separation allow us to better manage our assets.

There are many information asset valuation methods. For example, to qualify a value for an information asset in the military context, nine factors have been identified for establishing the value and metadata of an information asset. These nine factors are: [11]

- Accessibility: the ability to use the information asset
- Availability: the reliability and timely use of an information asset
- Confidentiality: the secrecy, and disclosure prevention, of information traversing within the information asset
- Contextual: the association of asset information to the consumer
- Essentiality: the importance of the information asset to the consumer
- Integrity: the accuracy, reliability, and unauthorized modification prevention of information traversing the information asset
- Non-repudiation: the assurance the information is from the information asset
- Substitution: the ability to replace the information asset with an equal information asset
- Temporal: the effect of the change in time on the information asset information.

Our system aims to offer service to general, higher level institutes, so applying the entire military level valuation method seems less cost-efficient. However, these military valuation criteria did provide some insights. Our top focus is that the most valuable assets are given the highest priority when managing risks. Our determination of asset values are based on the overall importance of that asset group to our system's operation, and we applied some of the above military asset valuation criteria to our asset valuation, specifically: availability, confidentiality, essentiality, and integrity.

As shown in Figure 8, data assets are valued 5 as the most critical assets. Specifically, the availability, confidentiality, essentiality, integrity are all 5. Thus, with all values receiving a 5 we can classify the data assets as 5. Data, such as students' records, SSN, or identity information, is our top priority to protect and are most critical. Hardware, software, and network assets are valued 4, not because they are less critical or less important than data assets, but because we perceive data asset as the top priority to protect. On the contrary, procedure assets is valued 2. Specifically, the availability and confidentiality of the procedure assets are a 2, since many policies are meant to be public, such as the privacy policy. Finally, the essentiality is a 1 and the integrity is 3, which creates an overall value of 2 for the procedure assets. However, although procedure assets are valued as 2, IT sensitive procedure and policy can be more critical than normal business procedure and policy. This valuation is general in order to demonstrate our priority on data, software, hardware and network assets.

IV. Analysis

Risks are always involved with businesses. No matter what type of business it is, there is always an amount of various risks involved. Risks can have different levels of impact on different organizations, and they are especially appreciated by those who rely heavily on technology. However, some risks can be assessed and controlled, whereas some risks are unexpected and disastrous enough to put an organization out of business. No matter how diligent an organization attempts to predict risks, the unforeseeable nature of some risks still allow them to find their ways into the organization's operation. As a result, it is every organization's priority to assess risks, to predict possible outcomes, and to maintain a business contingency plan as well as a disaster recovery plan in case risks interrupt business operation.

There are many risk analysis methodologies. Some famous ones can date back to the last century, when information security was a relatively new subject. As early as 1975, the United States of America National Bureau of Standards proposed Annual Loss Expectancy as a criterion for measuring computer-related risks. When calculating Annual Loss Expectancy, product of impact and frequency of harmful outcomes are usually taken into the equation. However, this risk assessment methodology is flawed because it fails to distinguish between highly frequent, low-impact events and rare, high-impact events. Consequently, the United States of America National Bureau of Standards made significant efforts to improve the risk management field. [12]

Years later, many approaches were revised and improved, which would offer additional steps, processes, and calculations to measure risks. These approaches were still solely based on the ones created back in 1980s. [12] According to "Current Challenges in Information Security Risk Management," "advances in security methods lag behind the general systems development methods and more general methods fail to consider security specifications." [12] In order to protect the confidentiality, integrity, and availability of the

system, we considered advanced, and newly-developed risk analysis methodologies.

Newly-developed risk analysis methodologies often share commonalities. For example, the CCTA Risk Analysis and Management Method and ISO 27005 share some processes that are analogous to each other. In fact, almost all methodologies require that the inventory and security classification of infrastructure elements and the understanding of the organization's missions and objectives in a first phase. The following phase requires the identification of threats and potential vulnerabilities, which is needed in combination with the results of the impact analysis to determine the actual risks. [12] Due to the shared commonalities between many risk analysis methodologies, we completed our risk analysis by following a generic risk analysis technique, which consists of common risk assessment procedures, and processes that are cost-efficient and fit our system's needs.

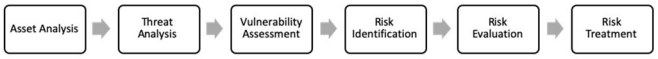

Figure 9: Risk analysis Process

Our risk analysis process, which is shown in Figure 9, started with an understanding of what our assets are, and what assets are potentially at risk. Then, our risk analysis involved threat identification and assessment. In order to model all the threats facing our system, we frequently referred back to our asset assessment throughout the process. Threat assessment criteria are the following:

- Possible threat agents: entities or events that can harm our system's operation. For instance, an attacker who runs malicious code against our system.
- Motivations: what drives threat agents to harm our system. For example, a hired attacker DDoS against our system so the hirer gains competitive advantage.
- Capabilities: what a threat agent is capable of. For example, a fire is capable of destroying all servers.
- Costs: the costs of outcomes. For example, a huge financial loss.
- Likelihood: likelihood defined by the frequency and probability of a threat's occurrence.

With sufficient insights into the threats facing our system, we then were able to rank threats based on our assessment so we address the threat with highest priority first.

The third phase of our risk analysis involved vulnerability identification and assessment. The vulnerability identification was achieved by comparing our threat assessment against our asset assessment, which allowed us to discover potential vulnerabilities in the forms of flaw within our system's boundary. These weaknesses can originate from how our system is designed, implemented and configured. With this knowledge, we could better understand what we must do to reduce the likelihood that a particular threat takes advantage of a vulnerability. In order to better secure our system, we also identified vulnerabilities that can exist outside of our system's boundary.

The last two steps in the risk analysis process were risk assessment and risk management. During this process, we derived and identified all risks associated with our system, according to the combination of previous asset assessment, threat assessment, and vulnerability assessment.

To conclude our risk analysis, we proposed our risk treatment strategies, management plans, and technical solutions. The risk treatment strategies are based upon the four general risk treatment strategies: risk avoidance, risk mitigation, risk transfer, and risk acceptance. However, our risk treatment strategies also synthesize our own guidelines and approaches,

creating a harmony between the general strategies and our own. As a result, we obtain an abstract security framework which could be fitted to any educational institution with a few modifications.

Threat and Vulnerability Analysis

In our process, we identified possible threats which our system could face. In our case, a threat is defined as "any event or circumstance that has the potential to adversely affect operations and assets". [9] Identifying threats can be quite burdensome as the task can become quickly endless. The deeper you look into the hidden dangers one asset could encounter, the more you realize the process could be interminable, as additional hazards surface. After all, the motto "no system is ever completely secure" is one of the first principles taught in cybersecurity. Nevertheless, we classified our threats into three distinct groups: physical, hardware, and software.

These threats were ranked using multiple criteria (both qualitative and quantitative). First, we determined the probability or likelihood of that particular threat occurring. Then, it was essential to establish the cost it could generate for our organization if the threat occurred. Finally, the frequency of each threat was considered. Those three criteria allowed us to sort each threat, in each different group, according to a priority to address and solidify our system to make sure that threat could not transpire.

Threat	Vulnerability	Loss	Likelihood	Priority to address
Forces of Nature	Poor architecture, safety procedures and equipment, or insufficient backups	Equipment, data, and personnel	1	Low
Theft	Insufficient security, or human error	Hardware and intellectual property	4	High
Unauthorized Access	Poor security policy	Hardware and intellectual property	3	High
Human Error	Insufficient security, awareness education, or poor procedures	Equipment, data, and personnel	5	High
Undermined Quality of Service (power outage, ISP down, etc.)	Third-party policies	Service loss and competitive advantage loss	2	Moderate

Figure 10: Physical threats and vulnerabilities

Within the physical category, which can be seen in Figure 10, we can find threats that could lead to loss or damage of our information assets, whether it relates to our actual data, equipment, or even in some cases, personnel. The primary threat affecting our system is forces of nature. These present probably some of the most dangerous threats that one could encounter, ranging from more common incidents such as fires or floods, to rarer catastrophes, such as earthquakes. Evidently, those often disrupt many people's' lives, but they can also have a devastating effect on businesses. Infrastructure could be destroyed, data could be lost, and the cost engendered could very quickly reach vertiginous sums. Nonetheless, in our case, forces of nature was not our top priority to address as the chosen location of our facilities (the Northeastern U.S.) was not reputed as risky regarding natural disasters, thus explaining the score of 1 on our likelihood scale. Additionally, other threats were considered more critical as they were more likely to affect us more quickly. Therefore, a low priority to address was preferred.

The secondary physical threat is theft. Unfortunately, theft remains a fixed factor, regardless of the industry. It is almost certain that it will occur throughout the operation of an organization. This is the reason why theft received a

4 on our likelihood scale. Additionally, we made it one of our high priorities to address. Indeed, when an asset is essential to the correct functioning of an organization, its theft could be discovered rather quickly. On the other hand, if the importance of the stolen object or data is minimal, it could possibly go unnoticed for quite some time. Nevertheless, serious consequences could arise later on, potentially jeopardizing the company's future.

The tertiary physical threat is unauthorized access. Unauthorized access could lead to severe breach of confidentiality, and conceivably physical theft of data and/or equipment. This explains as to why unauthorized access also received a high priority to address. It is vital to properly draft security policies that will be implemented, to make sure that only permitted personnel access restricted premises. However, only a 3 was given to that particular threat on our likelihood scale, as a physical attempt appeared somewhat improbable, especially knowing that other methods, notably online, would be more effective.

The quaternary physical threat is human error. A human error can be defined as "a failure to perform a prescribed task or the performance of a forbidden action". [13] The act is generally performed "without intent or malicious purpose or in ignorance". [9] Nonetheless, despite the innocuousness of a mistake, consequences can be disastrous and have maximal impact on an organization. The most problematic threat to a company is its own employees as they are the ones closest to our information assets. Additionally, it is a known fact that human beings make mistakes. There are many reasons why such mistakes occur. From stress to fatigue, or even due to a simple distraction, the possibilities are unlimited, which is why a 5 (the highest grade) was chosen on our likelihood scale. A high priority was also attributed. The training of our staff needs to be thoroughly incorporated within our organizational culture, to ensure a proper error-contained continuity of our operations.

Finally, our quinary threat is undermined quality of service. From a power outage to an Internet disturbance, the proper functioning of our organization can suddenly be disrupted by issues that we have no control over. It is fundamental that we arrange agreements with our various providers to limit the impact of such matters on our own services. Additionally, alternative solutions need to be considered beforehand, in case such crisis were to arise. The grade the threat received on our likelihood scale is a 2, as we thought it was not very likely to occur. Also, given that the cause of such a threat is out of our hands, we believe the threat is of moderate priority to address.

Threat	Vulnerability	Loss	Likelihood	Priority to address
Sabotage	Weak physical security	Data storage and data	1	Moderate
Hardware Failure	Design flaw or insufficient maintenance	Data	3	Moderate
Hardware Vulnerability	Design flaw	Data stolen	3	High
Network Error	Poor configuration	Connectivity	3	Moderate

Figure 11: Hardware threats and vulnerabilities

In Figure 11, hardware-related threats that could undermine our system are listed. While some of these threats could be seen as physical threats, they were not considered as such, given that they had a direct effect on our hardware equipment.

The primary threat listed is sabotage. Sabotage is defined as "a deliberate and malicious act that results in the disruption of the normal processes and functions or the destruction or damage of equipment or information". [14] However, given that an attacker would need to physically introduce himself within our organization, we believed that this threat would be rather unlikely to occur, which is why a 1 was given on our likelihood scale. On the other hand, we felt that the priority to address the

threat was moderate, as there was not much mitigation that we could made on our part.

Our secondary hardware-related threat is hardware failure. Throughout the years, many manufacturers have problems with products and supply chains. Whether it is from a flaw in the device or from inappropriate maintenance, hardware failure could halt the university's operations and thus, disturb its proper functioning. However, some issues could be out of our control, as we might not even be aware of such problems. With those factors taken into consideration, we gave the threat a 3 on our likelihood scale and a moderate priority to address.

Then, an additional hardware-related threat takes advantage of a hardware vulnerability. This is the only threat in this category that we believed needed to be a high priority to address. The consequences of an attack exploiting such vulnerability could be critical to our system, as it would not only affect the proper running of our organization, but could also alter the data itself. Additionally, we gave it a 3 on our likelihood scale, as we did for most threats in this category. As indispensable the mitigation of those threats is, software-related threats seemed more imperative to take care of.

Finally, our last hardware-related threat is network error. Communication is key in every organization, regardless of the industry it operates in. We need our services to be fully running and available for all of our users. Therefore, we cannot afford to have our network poorly configured. As the other factors, a 3 was given on our likelihood scale, and its priority to address was considered moderate.

Threat	Vulnerability	Loss	Likelihood	Priority to address
DDoS	Lack of firewall security, or filtering procedures	Availability (bandwidth)	5	High
MITM or ARP Poisoning	Poor encryption standards	Confidentiality compromised	4	Moderate
Malware	Poor IDS configuration, bad security layer, insecure coding practices, or social engineering	Data stolen/altered or system affected	5	High
Data Referential Integrity	Human error or poor security policy	Inconsistency in access to systems/services	1	Low
Social Engineering	Lack of security awareness	Unauthorized access (passwords), credentials	5	High
Web Attacks (XSRF, XSS, SQL injection, etc.)	Bad coding practices leading to unauthorized privilege escalation	Confidentiality, Integrity, and Availability of data	5	High

Figure 12: Software threats and vulnerabilities

In our last group, we listed all potential software-related threats. These software-related threats can be seen in Figure 12. Most of them are actual attacks that could harm our system in various ways. We believe that this category is of utmost importance regarding the implementation of our system and should be considered as such. It is critical to keep the number of these potential threats to a minimum, as they are the easiest for a malicious entity to design, and the most impactful on the objectives of our system.

The first software-related threat is Distributed Denial of Service (DDoS). A DDoS attack is an "attempt to make an online service unavailable by overwhelming it with traffic from multiple sources". [15] Our services need to be fully available for our organization to properly operate. A firewall and proper filtering procedures must be implemented in order to ensure our system functions to the best of its abilities. Therefore, a 5 was given on our likelihood scale as well as a high priority to address.

The second software-related threat is man in the middle or ARP poisoning. We need to use reliable encryption standards, which will satisfy our organization's needs. We cannot afford any malicious entity intercepting our data. The likelihood

for that threat occurring is a 4 on our likelihood scale. However, we only gave it a moderate priority to address given that the solution for that threat is relatively straightforward. Our traffic must constantly be encrypted.

The third software-related threat is malware. Any malicious software "seeking to invade, damage, or disable devices, often by taking partial control over the device's operations" [16] can be classified as malware. In 2017, 13 new malware specimens were discovered every minute. [17] Therefore, the likelihood the threat received on our scale is a 5. Our system must possess the appropriate defenses against it as soon as possible. From having an Intrusion Detection and Prevention System (IDPS) to training our staff, the priority to address this threat is high.

The fourth software-related threat is Data Referential Integrity. When data is being updated throughout our system, we have to make sure that multiple entities are not incompatibly altering the same information. We gave a 1 on our likelihood scale as well as a low priority to address, as it is quite easy to achieve a solution. First, we must have all of our subsystems synchronized. When a change is made, all subsystems should reflect that change. Additionally, a privilege infrastructure should be built to determine the data every user is allowed to access or not.

The fifth software-related threat is social engineering. Attackers are finding more ingenious ways to steal people's information, whether it is a password of a social media platform or the bank account number. Social engineering consist of "manipulating individuals in order to get them to give up confidential information". [18] It is a known fact that human beings tend to trust others easily. Our employees across all departments must to be properly trained, so they can detect any attempt to maliciously obtain confidential data from them. We gave social engineering a 5 on our likelihood scale as it is the most common type of attack nowadays. Additionally, we must make a high priority of ours to address the propagation of that threat and the possible defenses to counter it.

Finally, our last software-related threat is web attacks. These attacks include:

- Cross-Site Request Forgery (XSRF): attack that "forces an end user to execute unwanted actions on a web application in which they are currently authenticated", [19]
- Cross-Site Scripting (XSS): attack that "uses a web application to send malicious code, generally in the form of a browser side script", [20]
- SQL injection: attack that exploits "SQL query via the input data from the client to the application". [21]

We gave web attacks a 5 on our likelihood scale, given the ease of feasibility of such attacks. Additionally, they were considered to be of high priority to address, as those attacks would exploit vulnerabilities present on our public services.

Risk Matrix and Analysis

Consequence - Severity	Legal	Financial	Information Technology	Environmental	Safety	Quality of Service	Reputational
Severe	- Unauthorized Access - MITM - Web Attacks	- Unauthorized Access - Sabotage - DDoS - MITM - Malware - Web Attacks	- Sabotage - Hardware Failure - Hardware Vulnerability - Malware - Web Attacks		- Forces of Nature	- Sabotage - Network Error - DDoS - Malware - Web Attacks	- Unauthorized Access - MITM - Web Attacks
Major	- Human Error - Malware	- Forces of Nature - Hardware Failure - Hardware Vulnerability - Social Engineering	- Unauthorized Access - Data Referential Integrity		- Sabotage	-Undermined Quality of Service - Hardware Failure - Hardware Vulnerability	- Network Error - DDoS - Malware
Moderate	- Hardware Vulnerability	- Data Referential Integrity	- Forces of Nature - Social Engineering		- Human Error	- Forces of Nature - Human Error	- Sabotage - Hardware Vulnerability
Minor or Insignificant		- Theft		- Hardware Failure			

Figure 13: Risk analysis matrix

From our threat and vulnerability analysis, a risk analysis matrix was created. Three distinct

criteria were adopted to classify each threat. The first criterion is the consequence of that threat: legal, financial, information technology, environmental, safety, quality of service, and reputational. The second criterion is the severity that a threat could have on our system. In our matrix, severe represents the most impactful threat, while minor or insignificant portrays the lowest one. Finally, our last criterion is a color code, to evidently highlight the priority of each solution/strategy. Red depicts the most important threats to take care of while green represents the least critical ones. The red blocks and their subsequent threats should be addressed first with the strategies implemented through our system. To establish that color code, several elements were taken into consideration:

- Likelihood of a threat
- Impact a threat could have on our system
- The relationship a threat could potentially have with other threats

For example, as it can be seen in Figure 13, web attacks were sorted into five categories: legal, financial, information technology, quality of service, and reputational. Additionally, web attacks were considered severe in each of those categories, given that they could have catastrophic repercussions on our system, if there were to be exploited. Finally, all of these cells were coded red, as it would become critically hard to protect the system, if those attacks were to be launched simultaneously.

V. Strategies

Our strategies are based on the four general risk treatment strategies: risk avoidance, risk mitigation, risk transfer and risk acceptance. However, we also combined our own guidelines and approaches with the general treatment strategies. This process allowed us to create a customized lists of strategies that best fit our system. These six secure coding strategies are:

- Secure coding principles
- Secure data handling
- System logging
- Isolation of users and systems
- Auditing
- Comprehensive maintenance practices

By applying proper coding guidelines, we can defend our system against potential software threats, as well as avoiding counterproductive procedures in the future. For example, the KISS ("Keep It Simple Stupid") principle should be followed. Complex code makes it more arduous to read, debug, and ultimately modify. Additionally, the DRY ("Don't Repeat Yourself") principle should also be observed. Editing later on will become easier if the code is written coherently. [22] Finally, a last example would be to sanitize our code to be protected against attacks by using coding analyzers. These can help fix coding issues that may lead to exploits by attackers, such as SQL injections. One such fix could be the restriction of particular characters in certain inputs, such as letters when requiring a phone number.

Through encryption and access controls, we can better defend our data across our systems, and protect it against potential attacks, such as eavesdropping in MITM scenarios. For instance, by implementing TLS protocol, the user traffic when accessing our web service will be encrypted using AES. With respect to data integrity, we can hash our data such as passwords, so that even if our system's database was breached, all the passwords would be in unreadable random strings. Therefore, attackers will not obtain the actual passwords.

Servers, firewalls and other IT equipment must keep log files to record important events and transactions. This information can provide important clues regarding hostile activity affecting networking services. Log data can also allow us to find and troubleshoot equipment problems including configuration problems and hardware failures.

Reviewing logs frequently could help us identify malicious activities occurring within the system. Given the large amount of log data generated by our system, it is impractical to review all logs manually every day. Instead, we can use a log monitoring software to automate this task and point out questioning events, such as potential threats. This process can be accomplished through implementing using real-time reporting systems. Alerts can be sent to the system administrator via email or text as soon as a suspicious activity is detected.

One of the key strategies to implement in a university's system is to isolate users and systems. To do this, a VPN should be implemented into the university's infrastructure to not only allow secure site-to-site communications within a university's network, but also provide host-to-host security to allow remote access to the university's internal network. The VPN serves as a layer that isolates public and user traffic. The VPN could be customized to the university's needs and should be audited by VPN experts, such as ExpressVPN or NordVPN.

A second method of isolation between systems would be to have a bastion server established to protect the internal network. An intrusion detection and prevention system could also be deployed on the external side of the network, to help with filtering. On the other hand, a firewall should be installed on the inside of the bastion system.

The implementation could be done with free software, such as Cisco's Snort IDS and Linux IPtables firewall. A more effective, modern, and more expensive way of providing this bastion server would be to use SolarWinds' Log and Event Management IDS system and a FortiGate firewall from Fortinet.

Auditing is the fifth strategy necessary for any organization. It can be done internally by a committee or externally by a third-party auditing service. By creating an internal assessment committee, we can better mitigate legal, financial, and reputational risks from within the company. This would also lessen the threats posed by malicious, external, third-party companies and employees. However, this could lead to unfollowed policies implemented by the university or even the government. External third-parties would help the IT and InfoSec teams follow these policies and secure previously unseen vulnerabilities. Thus, annual audits should consist of both compliance audits, for government regulations, and information system audits, for securing the university's infrastructure. [23]

By following strict maintenance guidelines, we can always proactively plan ahead, and be prepared for any unforeseen or unorthodox incidents. An educational institution should avoid overconfidence after implementation of its security profile. Since organizational changes may occur, such as acquisition of new assets or emergence of new vulnerabilities, it might be necessary to adapt and thus alter our system development life cycle. For example, patches should be properly installed on all systems on a regular basis. The four types of maintenance should be applied. Firstly, corrective maintenance includes updates in order to correct a problem. Secondly, adaptive maintenance proactively keeps software updates. Thirdly, perfective maintenance refines the software, by including new features or new user requirements. Lastly, preventive maintenance attempts to address problems before they occur. Also, non-maintenance and diagnostic tasks must be documented and reviewed on a monthly basis. [24]

Layer	Solutions	Tool
Application layer	Secure coding, security layer (reference monitor), anti-malware, DNSSEC, hash	Malwarebytes and Coding analyzer (Sonar, etc.)
Transport layer	Encryption through cryptography	TLS/SSL protocol
Network layer	Firewall, VPN, IDPS	Iptables, Fortigate, Snort, SolarWinds Log and Event Management, Cisco routers with built-in secure functions.
Link layer	Port security	Cisco switches with built-in secure functions
Physical layer	Access control, monitors	Token, fingerprint scanner, camera

Figure 14: Layered security

Figure 14 shows a more visually appealing way of looking at our solutions, with respect to the TCP/IP layers. The proposal of our hardware and software solutions is derived from the idea of defense in depth. Defense in depth is a concept where multiple security layers are deployed throughout one system. For instance, on the hardware level, specifically on the link and network layers, we recommend implementing latest switches and routers from Cisco. Cisco's routers and switches offer built-in secure functions such as secure boot, which ensures the executables have not been modified before booting. Runtime defense is also effective against injection of malicious code into running processes, etc. On the software level, specifically on the transport layer, we can protect the confidentiality and the integrity of data in transit by implementing TLS protocol. On the application layer, we suggest implementing anti-malware software and security layer. For instance, a security layer that prevents an unauthorized process from modifying memory.

By implementing this hardware and software services, we can apply the six strategies we set out to reinforce with our system and guidelines with multiple layers of security.

VI. Further Work

As our research demonstrates, a secure scheme can be developed for any higher education institution. The next step in our research would be to implement our system and follow the guidelines we set forth in our strategies, as well as the CIA triad and OWASP ASVS. Through the execution of a practical version of our system, we would be able to conduct studies to show the viability and success rate of the ideas we discussed throughout this paper.

VII. Conclusion

Through our analysis, we determined the security goals that a university needs to achieve in order to offer a secure environment for its community. We also outlined the respective guidelines necessary to reach that objective. Additionally, this document is not intended to be prescriptive. It is neither a specification nor is it a comprehensive set of requirements to be followed. It only provides a framework and outlines the main strategies to create a secure system from the bottom up. This more secure system can work for any educational institution because of its generalized methodology.

Guidelines to a secure system tailored to a university's needs:

- Understand the mission and objectives of the university
- Frame the system architecture to satisfy the functional requirements through the modeling of an entity diagram
- Determine a user privilege hierarchy, necessary subsystems, and fundamental services through a chain of commands
- Prioritize information through data and assets classification
- Specify security requirements through quantifying the probability and impact of identified risks
- Fulfill security specifications through the combination of security strategies we define, as well as those define customized for the institution
- Further analyze new threats and update the system to secure these issues
- Maintain infrastructure and documentation on policies

In conclusion, throughout our paper, we formulated instructions, allowing any organization in the higher education field to conceive its own information security management system, in a protected and safe fashion to the best of its abilities.

IX. References

[1] SecurityScorecard. "SecurityScorecard Report Finds U.S. Education System Ranks Last for Cybersecurity among 17 U.S. Industries." *Report Finds U.S. Education System Ranks Last for Cybersecurity*, securityscorecard.com/press-releases/securityscorecard-report-finds-u-s-education-system-ranks-last-for-cybersecurity-among-17-u-s-industries.

[2] Ninja, Security. "CIA Triad." *Infosec Resources*, Infosec Institute, 21 May 2018, resources.infosecinstitute.com/cia-triad/#gref.

[3]"Information Technology Policies." LIU, www.liu.edu/About-LIU/University-Policies/Information-Technology-Policies.

[4] "Columbia University IT Policies and Strategies." Columbia University Information Technology, cuit.columbia.edu/columbia-it-policies-strategies.

[5] "IT Security and Policy." NYU, www.nyu.edu/life/information-technology/it-security-and-policies.html.

[6] Iso, and International Organization for Standardization. *Publicly Available Standards*, International Organization for Standardization, standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[7] "Framework for Improving Critical Infrastructure Cybersecurity." NIST, NIST, 12 Feb. 2014, www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[8] Cuthbert, Daniel, et al. "OWASP Application Security Verification Standards." *OWASP*, OWASP, 1 Mar. 2019, github.com/OWASP/ASVS/raw/master/4.0/OWASP Application Security Verification Standard 4.0-en.pdf.

[9] Whitman, Michael E., and Herbert J. Mattord. Management of Information Security. Cengage, 2019.

[10] Seraphin, Catherine. "The College Administration Hierarchy." *CollegeXpress*, www.collegexpress.com/articles-and-advice/student-life/articles/living-campus/college-administration-hierarchy/.

[11] Hellesen, Denzil, and Michael Grimaila. "Information Asset Value Quantification Expanded." Proceedings of the International Conference on Information Warfare & Security, Jan. 2010, pp. 138–147.

[12] Fenz, Stefan, et al. "Current Challenges in Information Security Risk Management."Information Management & Computer Security, vol. 22, no. 5, 2014, pp. 410-430.

[13] Dhillon, Balbir S., and Subramanyam N. Rayapati. "Human Performance Reliability Modelling." Microelectronics Reliability, vol. 28, no. 4, 1988, pp. 573–580., doi:10.1016/0026-2714(88)90143-6.

[14] "Cyber Sabotage." Military.com, 6 Feb. 2008, www.military.com/defensetech/2008/02/06/cyber-sabotage.

[15] "What Is a DDoS Attack?" Digital Attack Map, www.digitalattackmap.com/understanding-ddos/.

[16] "Malware Definition – What Is It and How to Remove It." Malwarebytes, www.malwarebytes.com/malware/.

[17] Benzmüller, Ralf. "Malware Numbers 2017." SECURITY BLOG, 27 Mar. 2018, www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017.

[18] "What Is Social Engineering? Examples And."

Webroot, www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering.
[19] “Cross-Site Request Forgery (CSRF).” OWASP, www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF).
[20] “Cross-Site Scripting (XSS).” OWASP, www.owasp.org/index.php/Cross-site_Scripting_(XSS).
[21] “SQL Injection.” OWASP, www.owasp.org/index.php/SQL_injection.
[22] Lee, Joel. “10 Basic Programming Principles Every Programmer Must Follow.” MakeUseOf, 26 Oct. 2017, www.makeuseof.com/tag/basic-programming-principles/.
[23] “Internal Audit Types - University Audit Services - Finance Division - Carnegie Mellon University.” *Internal Audit Types - University Audit Services - Finance Division - Carnegie Mellon University*, Carnegie Mellon University, www.cmu.edu/finance/audit-services/internal/types-of-audits.html.
[24] Tutorialspoint.com. “Software Maintenance Overview.” Software Maintenance Overview, Tutorialspoint, www.tutorialspoint.com/software_engineering/software_maintenance_overview.htm.
[25] “Thread modeling: 12 available methods” https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html
[26] “What Is Management? Definition, Features (Explained).” IEduNote.com, 1 Dec. 2018, iedunote.com/management.
[27] “What Is IT Security? - Information Technology Security.” Cisco, 14 Jan. 2019, www.cisco.com/c/en/us/products/security/what-is-it-security.html.
[28] Rowe, Craig. “The 5 Step Risk Management Process [Updated for 2018].” The 5 Step Risk Management Process [Updated for 2018], www.clearrisk.com/risk-management-blog/bid/47395/the-risk-management-process-in-5-steps.

X. Appendix

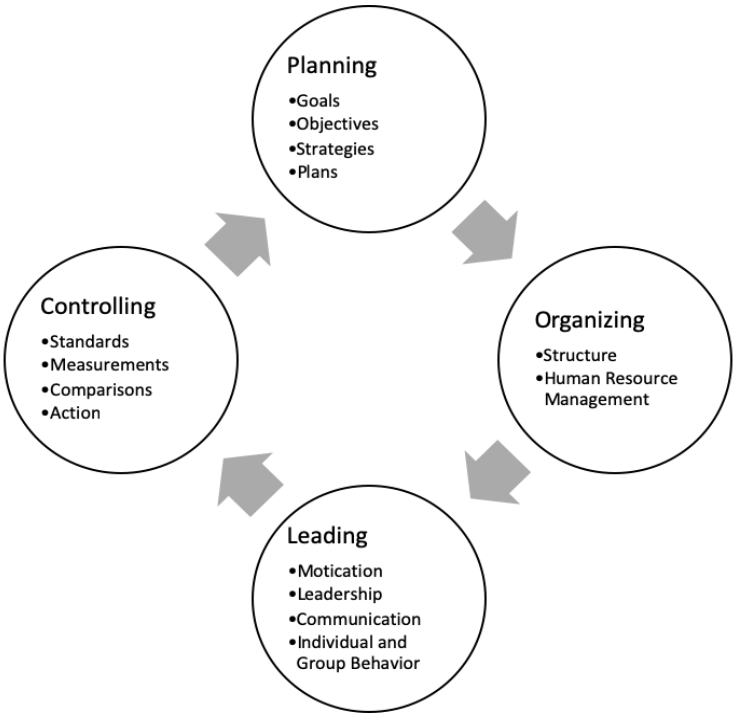

Figure 1: Old life cycle for implementing a secure system

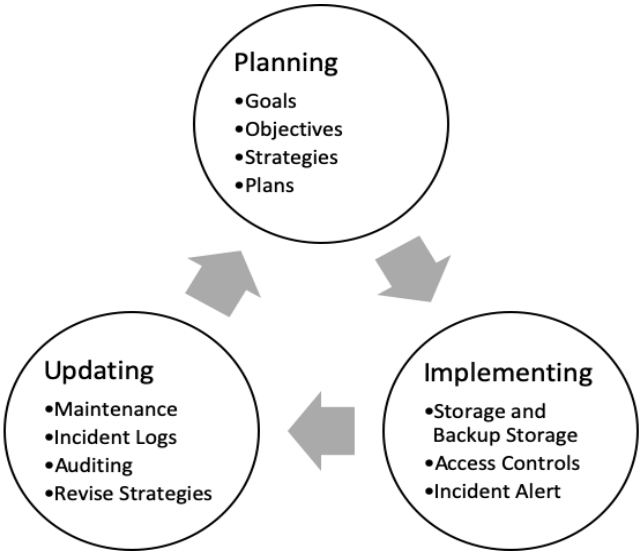

Figure 2: Revamped life cycle for implementing our guidelines for a secure system

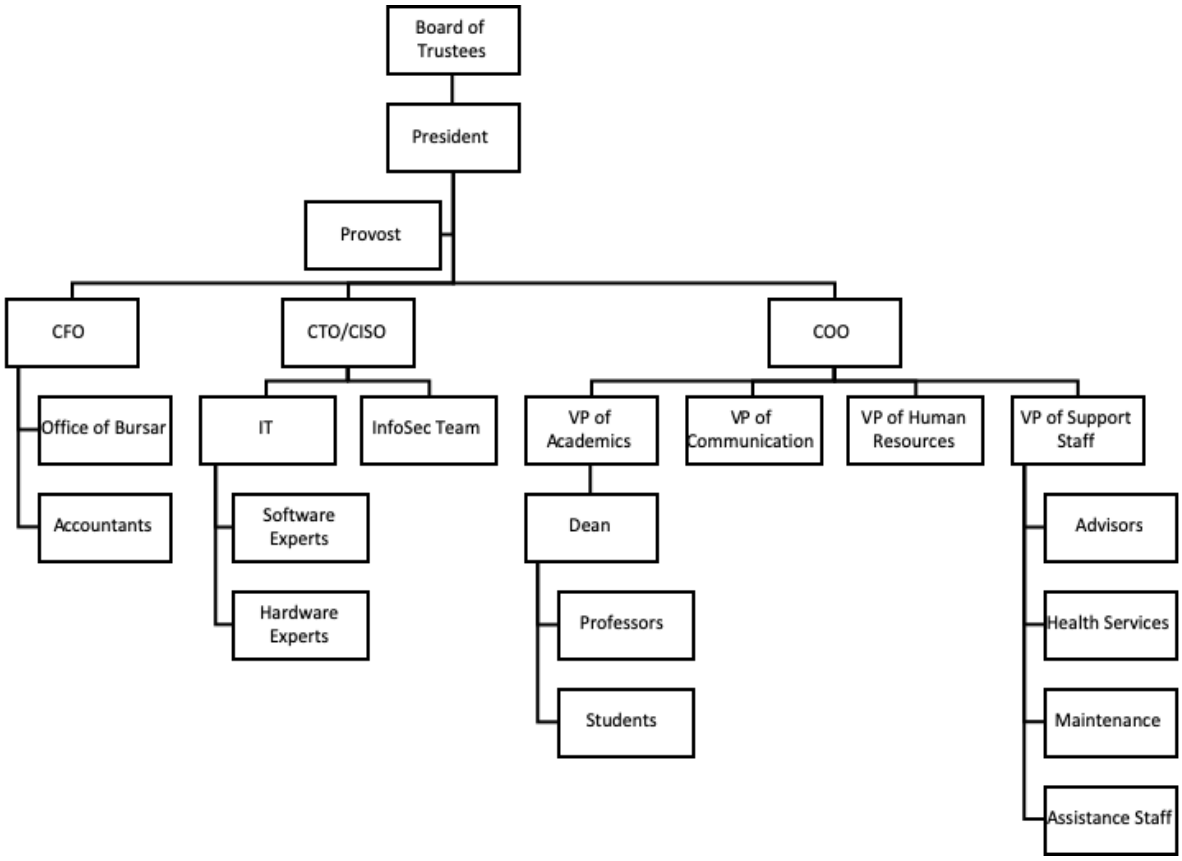

Figure 3: Governance hierarchy of higher education institutions

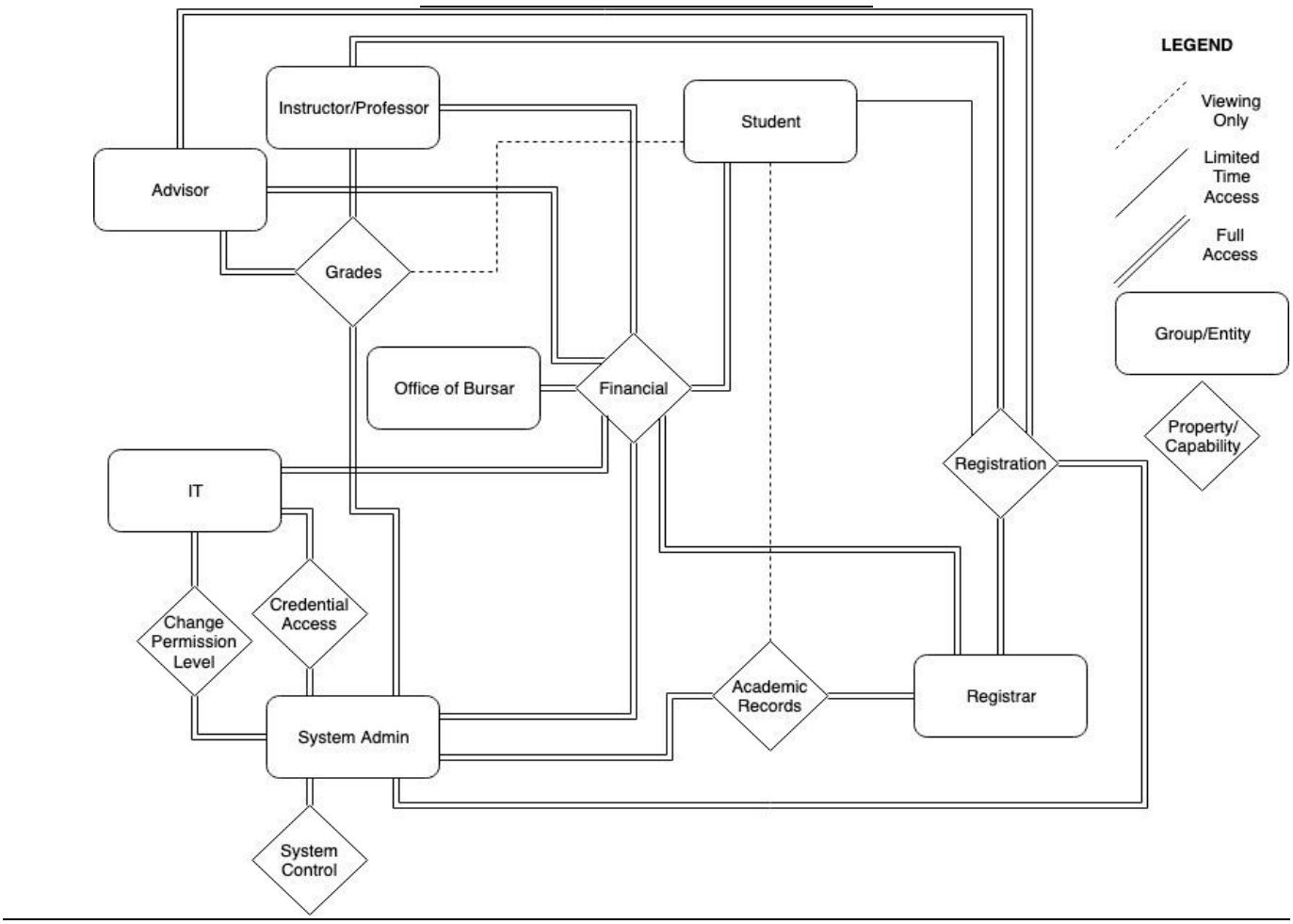

Figure 4: Entity diagram

Property / Capability	Student	Instructor	Advisor (Instructor)	Registrar	Office of Bursar	IT	System Admins
Financial	X (own)	X (own)	X (own)	X (own)	X (all)	X (own)	X (all)
Grades	X (view their own grades only)	X (view and edit grades of multiple students)	X (view all grades)				X
Credential Access						X	X
Registration	X (Limited)	X	X	X			X
Change permission level						X (can change permission lvl down and up to their level)	X (can provide higher levels of access)
Academic Records (SSN, etc.)	X (own)			X			X
System Control							X

Figure 5: Chain of command

Information Assets	Data Classification	Impact if Compromised
Financial	Restricted	High
Grades	Confidential	Low
Credentials	Restricted	High
Registration Information	Internal	Medium
Academic Records	Restricted	Medium
Personal Public Information	Public	Low
University Website Information	Public	Low

Figure 6: Data classification

High Tolerance	Moderate Tolerance	Low Tolerance
1. The unauthorized use, access to the asset would not have impact on our system's operation.	1. The unauthorized use, access to the asset would impact some of our system's operation. 2. The risk associated with the asset is transferred, well-estimated, mitigated, controlled.	1. The unauthorized use, alteration, access to the asset would bring disastrous consequences to our system's operation. 2. The exploits of an asset can greatly undermine the overall security of our system. 3. The misuse, or unauthorized operation of an asset can break the governance guidelines and legal regulations.

Figure 7: Asset risk tolerance level

Assets	Example	Value	Risk Tolerance
People	Internal or external personnel	3	Moderate
Procedure	Business-sensitive procedure and policy	2	Moderate
Data	Network traffic and database records	5	Low
Software	Applications, OS, and software security measures	4	Low
Hardware	Equipment and hardware security measures	4	Low
Networking	LAN components Internet components Network security measures	4	Low

Figure 8: Asset classification

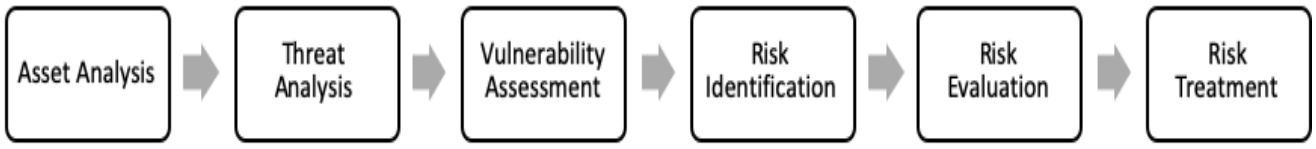

Figure 9: Risk analysis Process

Threat	Vulnerability	Loss	Likelihood	Priority to address
Forces of Nature	Poor architecture, safety procedures and equipment, or insufficient backups	Equipment, data, and personnel	1	Low
Theft	Insufficient security, or human error	Hardware and intellectual property	4	High
Unauthorized Access	Poor security policy	Hardware and intellectual property	3	High
Human Error	Insufficient security, awareness education, or poor procedures	Equipment, data, and personnel	5	High
Undermined Quality of Service (power outage, ISP down, etc.)	Third-party policies	Service loss and competitive advantage loss	2	Moderate

Figure 10: Physical threats and vulnerabilities

Threat	Vulnerability	Loss	Likelihood	Priority to address
Sabotage	Weak physical security	Data storage and data	1	Moderate
Hardware Failure	Design flaw or insufficient maintenance	Data	3	Moderate
Hardware Vulnerability	Design flaw	Data stolen	3	High
Network Error	Poor configuration	Connectivity	3	Moderate

Figure 11: Hardware threats and vulnerabilities

Threat	Vulnerability	Loss	Likelihood	Priority to address
DDoS	Lack of firewall security, or filtering procedures	Availability (bandwidth)	5	High
MITM or ARP Poisoning	Poor encryption standards	Confidentiality compromised	4	Moderate
Malware	Poor IDS configuration, bad security layer, insecure coding practices, or social engineering	Data stolen/altered or system affected	5	High
Data Referential Integrity	Human error or poor security policy	Inconsistency in access to systems/services	1	Low
Social Engineering	Lack of security awareness	Unauthorized access (passwords), credentials	5	High
Web Attacks (XSRF, XSS, SQL injection, etc.)	Bad coding practices leading to unauthorized privilege escalation	Confidentiality, Integrity, and Availability of data	5	High

Figure 12: Software threats and vulnerabilities

Consequence - Severity	Legal	Financial	Information Technology	Environmental	Safety	Quality of Service	Reputational
Severe	- Unauthorized Access - MITM - Web Attacks	- Unauthorized Access - Sabotage - DDoS - MITM - Malware - Web Attacks	- Sabotage - Hardware Failure - Hardware Vulnerability - Malware - Web Attacks		- Forces of Nature	- Sabotage - Network Error - DDoS - Malware - Web Attacks	- Unauthorized Access - MITM - Web Attacks
Major	- Human Error - Malware	- Forces of Nature - Hardware Failure - Hardware Vulnerability - Social Engineering	- Unauthorized Access - Data Referential Integrity		- Sabotage	-Undermined Quality of Service - Hardware Failure - Hardware Vulnerability	- Network Error - DDoS - Malware
Moderate	- Hardware Vulnerability	- Data Referential Integrity	- Forces of Nature - Social Engineering		- Human Error	- Forces of Nature - Human Error	- Sabotage - Hardware Vulnerability
Minor or Insignificant		- Theft		- Hardware Failure			

Figure 13: Risk analysis matrix

Layer	Solutions	Tool
Application layer	Secure coding, security layer (reference monitor), anti-malware, DNSSEC, hash	Malwarebytes and Coding analyzer (Sonar, etc.)
Transport layer	Encryption through cryptography	TLS/SSL protocol
Network layer	Firewall, VPN, IDPS	Iptables, Fortigate, Snort, SolarWinds Log and Event Management, Cisco routers with built-in secure functions.
Link layer	Port security	Cisco switches with built-in secure functions
Physical layer	Access control, monitors	Token, fingerprint scanner, camera

Figure 14: Layered security