Infotec Institute

Risk Assessment Report 2021

Submitted by:

Student Registration Number	Student Name
IT19013756	**M. H. D. V. Jayasinghe**
IT19102924	**J.G.L.A Jayasinghe**
IT19003610	**K. G. S. Shiranthaka**
IT19007984	**K. I. Karandeniya**

Date of submission

07th May 2021

Contents

1 Executive Summary

A precise and comprehensive risk assessment was conducted on the information technology assets of Infotec Institute from April 10th, 2021 to April 19th, 2021.

The risk assessment was carried out by the risk management team of Crypto Solutions, a third party to identify the risks associated with the information systems' key security components which include confidentiality, integrity, and availability (CIA), and to deliver a summary of them. This risk assessment is mainly focused on the following key factors,

- An assessment of frequent and man-made threats,
- Impact of the current security controls and policies.

Key issues and Recommendations

- SIMS's server room needs a new Air-Condition System.
    - Because of a physical expansion and arrangement, the existing air conditioning system being incapable - overheating the whole server of the 'Student Information Management System.' To reduce damage significantly, a new cooling unit needs to be purchased.

- SIMS's student information database needs new backup storage.
    - Due to a weakness in software planning, it does not have a recovery plan for the Student Information which belongs to the SIMS. It needs backup storage to reduce this risk.

- SIMS's Internet Portal security needs to be hardened and patched.
    - Authentication of the internet portal is weak since the current middleware version has known vulnerabilities so that both insiders and outsiders can sniff the traffic flowing through the network gateway. It needs to be hardened with more secure protocols and patched to the latest version to be more precise.

- The operating system of the HRMS server must be updated.
    - The outdated 'Human Resource Management System' server requires the urgent immediate next patch since the existing version has known loopholes that can be exploited through remote code.

- FMIS's server needs to be upgraded.
    - Due to the Vulnerability in Suite Commerce Advanced (SCA) Site's component of Oracle NetSuite service, the existing version of the FIMS server is considered vulnerable. Needing an urgent system upgrade.

- Strengthening the password policy of the Moodle
    - The current password policy cites that the students need to update their credentials and personal details once every two months. With the increasing number of phishing and identity theft attacks seeing a rise, it is recommended to update the password policy to be more secured and precise. Use of a strong password and account lockdown mechanisms should be implemented.

- A full upgrade and backup storage of the LMS database server is required.
    - Because of a software weakness in the outdated 'Library Resource Management System' database server which belongs to LMS (Learning Management System), the latest version needs to be patched and upgraded. In addition, it needs backup storage to dominate similar situations where there is no backup.

- IRMS physical security needs to be versatile.
    - All the computers in computer labs are included here with no CCTV support with the current implementation. It is recommended to install a new CCTV system to continuously monitor inside the labs to make note of other potential physical threats and risks.

2 Detailed Analysis

2.1 Introduction

Infotec Institute is a leading institute for offering Information Technology undergraduate programs located at - 79 Massachusetts Avenue Cambridge, MA 06139, USA. It has students from various parts of the globe providing its services. **Infotec** has earned a reputation over the years for its classic delivery addressing current topics with world - class undergraduate programs**.** Organizational policies and procedures are prioritized to enhance quality. Staff is slightly above a hundred and fifty and more than a thousand students are enrolled with the institute.

SIMS is the main core system that spans throughout the institute with several other main servers which ease the operations work in the institute. Student data, student details, and an internet access portal are the main features offered by the SIMS. FIMS, LMS, HRMS, and IRMS are the other servers that go along with SIMS integrating solutions to provide the students a reliable means to attend their academic work and the administration and authorities to handle the institute.

2.2 Purpose

The purpose of the risk assessment was to examine and discover flaws and vulnerabilities for different information technology assets belonging to Infotec institute to identify potential and already existing threats associated with the most critical assets and evaluate the risks according to the likelihood of impact and the financial impact on the organization. Furthermore, possible mitigation techniques and calculated cost estimations were represented at the end of the risk assessment to achieve the objectives and vision of the organization. These estimations and the procedures can then be examined by the relevant organization members to decide on a suitable course of action for the future.

2.3 Risk Assessment Framework

We have used the OCTAVE Allegro risk management framework for analyzing the risk assessment and impact due to the mentioned reasons.

- This framework is mainly focused on security practices.
- This is an organizational-wide evaluation.
- In this framework we have used top-down approach methodology so that it caters to the requirement of the high technical staff
- Several parameters such as time, personnel, investments, etc. focusing restrictions and limited boundaries

2.4 Appraisal Receivers

Role	Organization Member	Significance
Chancellor	Mr. John Keels	Executive
Vice-chancellor	Mr. Kylie Kayn	Executive
Dean	Mr. Garen Darius	Executive
Student Affairs	Mrs. Haylie Smith	Administration
HR Manager	Mr. Albert Morkel	Administration
Finance Manager	Mrs. Nicole Johnson	Administration
DB Admin	Mr. Zeyn Michael	High Technical
Network Admin	Mr. Malik Hassan	High Technical

2.5 Risk assessment scope

Refer [Appendix C] to properly understand the network scope using the network diagram.

Functional	Factorial	Personnel	Geographical
Five main systems were taken as critical systems along with many sub-systems included with them. Hardware was also assessed as assets of the organization.	This risk assessment provides a comprehensive layout of the risks which breaches the information assurance and information systems of Infotec Institute	150 associates overall – Appraisal receivers as mentioned above, and their sub-teams, finance, Human Resource, and Third-party influencer like the risk assessment team. All these associates are directly or indirectly employed in the organization	Over 8 IT sector locations were covered such as server rooms, computer labs, etc.

2.6 Risk Model

The Risk Assessment Criteria – Quantitative Analysis

Risk = Value of Impact × Likelihood of Occurrence

This equation will be used to evaluate the risk to help us calculate the risk. This is the common equation for risk evaluation.

2.6.1 Value of Impact

Impact	Definition
High (10)	The high impact will lead to critical damage or failure of the Institute flow which makes a huge impact on the intuitional reputation and the loss of client trust and financial loss.
Medium (5)	The medium but reasonable obstacle to the growth of businesses. Furthermore, the effectiveness and productivity of the services can cause financial and resource failure to the customer, but this could have a conservative impact compared to the high impact of this service.
Low (2)	The impact of business growth is considered a minor issue. This would result in a minor drop compared to moderate and critical impact.

2.6.2 Probability of Occurrence

Probability	Definition
High (1.0)	The threat source for the exploitation of vulnerabilities is extremely capable and efficient. Either the current controls are not vulnerable, or the countermeasures employed are not effective when the threat is continuously obstructed. Effective countermeasures are immediately necessary.
Medium (0.5)	The threat source can exploit vulnerability moderately and efficiently. There are comparatively adequate countermeasures to prevent the continued exploitation of the weakness. The threat is substantially managed.
Low (0.1)	Comparably, the source of the threat is unable to use the weakness effectively. Countermeasures and controls used to obstruct the threat are exceptionally sufficient.

2.6.3 Risk Calculation

Probability Impact	High (1.0)	Medium (0.5)	Low (0.1)
High (10)	10 × 1.0 = 10	10 × 0.5 = 5.0	10 × 0.1 = 1.0
Medium (5)	5 × 1.0 = 5.0	5 × 0.5 = 2.5	5 × 0.1 = 0.5
Low (2)	2 × 1.0 = 2.0	2 × 0.5 = 1.0	2 × 0.1 = 0.2

Low Risk 0-2 **Medium Risk 3-6** **High Risk 7-10**

2.6.4 Quantitative Analysis Parameters

Variable	Description
Exposure Factor (EF)	The percentage value of how much a certain asset is exposed to an identified risk scenario.
Single Loss Expectancy (SLE)	Value of the Asset x EF (How much impact/loss to the asset can be expected from a single threat occurrence)
Annualized Rate of Occurrence (ARO)	The number of times a threat will transpire in a year. Given one year, how likely the risk scenario is to happen. (Probability)
Annualized Loss Expectancy (ALE)	SLE x ARO (How much loss to the asset can be expected from the threat over a year, this value represents the risk)
Safeguard Cost/Benefit	ALE before Safeguard – ALE after Safeguard – Annual cost of the Safeguard

2.7 Assets Profiles

Critical Asset	Description	Container and Specifications	Security Requirement				Asset Value (USD)
			Property	L	M	H	
SIMS	SIMS is the most critical asset in the institute which manages all the student details, examination details along with results, student registrations done by online payments, and specifically the student accounts associated with the internet portal and physical access logins to computers inside the computer labs. SIMS is maintained and accessed by Administrators, Academic, and Technical Staff.	PowerSchool SIS h/w SolarWinds-security-event-manager Active Directory - Windows Server 2016 Oracle WebCenter Portal	Confidentiality			X	$ 22151
			Integrity			X	
			Availability			X	
HRMS	HRMS is responsible for managing employees maintaining their details and respective roles. Administrators are using this system.	Dell PowerEdge T30 Xeon E3-1225 Windows 2012 Server	Confidentiality		X		$ 6054
			Integrity		X		
			Availability	X			
FIMS	FIMS manages the financial handling throughout the organization focusing on all new purchases, employee payroll management, and other financial records. Administrators and Finance have access to this system.	Dell PowerEdge T30 Xeon E3-1225 v5 ORACLE NetSuite	Confidentiality			X	$ 10049
			Integrity			X	
			Availability		X		

LMS	LMS handles the blackboard, the online learning portal offered by the institute for the students who are enrolled, and the library resource management system (LRMS) is also managed by this. Students and academic staff are given access to this system.	Talent LMS HPE ProLiant DL380 Gen10 server	Confidentiality	X			$ 4445
			Integrity		X		
			Availability			X	
IRMS	All the servers, computers in labs, and all other infrastructures are managed by the IRMS. The technical staff has access to this system.	Lenova ThinkServer TS150 Bitdefender GravityZone Business Security	Confidentiality	X			$ 7566
			Integrity		X		
			Availability		X		
L – Low; M – Moderate; H – High							
See Appendix A for Asset Value derivation.							
PII – Personally, Identifiable Information							

2.8 Threat Profiles and Mitigation Analysis

Critical Assets – SIMS | Active directory server 2016 (A) [1]	
Vulnerability and Threat Profile	The server on the AD is in a separate room with minimal space and conditions. The existing mini air conditioning system is not able to handle the current heating issues. **Vul. –** This unit is not capable of keeping the server from overheating. **Threat –** The server shutdowns abruptly due to overheating.
Impact Assessment	This risk scenario violates the most important security requirement for the system – availability - resulting in interruption of the services. No impact on Confidentiality and integrity. Considering the framework chosen the risk was calculated as **6/10** which falls under medium range impact on the system
Mitigation Plan	The best control is to purchase the 'SRXCOOL12K SmartRack 12,000 BTU 230V Portable Server Rack Cooling System'. This unit is powerful enough and capable of controlling the heat of the server. **Cost $899**

Before mitigation		**After mitigation**	
EF	50%	**EF**	20%
SLE	$22151 × 50% = $11075.5	**SLE**	$22151 × 20% = $4430.2
ARO	0.5	**ARO**	0.2
ALE	$11075.5 × 0.5 = $5537.75	**ALE**	$4430.2 × 0.2 = $886.04
Cost / Benefit	**$5537.75 - $886.04 - $899 = $3752.71**		

Critical Assets – SIMS | Power school SIS (B) [2]	
Vulnerability and Threat Profile	Power school SIS handles all the student information relating to SIMS. This does not include a recovery option or backup option in case of a sudden system compromise. **Vul. –** the unexpected loss of data or information **Threat –** Critical information might not be available to carry out the operation tasks assigned to the origination via the provided asset due to lack of backup and recovery initiations.
Impact Assessment	This risk scenario violates the most important security requirement for the system – availability - resulting in interruption of the services in case of a sudden system failure enabling them to restore the system information. Less impact on Confidentiality and integrity. The Risk is calculated to be **7/10** and it affects the availability.
Mitigation Plan	Invest in a cloud backup solution that cites along with the company requirement and implement proper recovery controls. **Cost $500**

Before mitigation		**After mitigation**	
EF	20%	**EF**	5%
SLE	$22151 × 20% = $4430.2	**SLE**	$22151 × 5% = $1107.55
ARO	0.8	**ARO**	0.2
ALE	$4430.2 × 0.8 = $3544.16	**ALE**	$1107.55× 0.2 = $221.51
Cost / benefit	**$3544.16 - $221.51 - $500 = $2828.65**		

<table>
<tr><td colspan="4"><b>Critical Assets: SIMS Oracle Web Portal (C)</b> [3]</td></tr>
<tr><td><b>Vulnerability and Threat Profile</b></td><td colspan="3">Vulnerabilities identified in Oracle WebCenter Sites product of Oracle Fusion Middleware. (Advanced User Interface).
Effected Versions: 12.2.1.30 and 12.2.1.4.0: CVE-2020-14613

<b>Vul. –</b> CVE-2020-14613
<b>Threat -</b> Attacker can Easily exploit the vulnerability that allows unauthenticated attackers with network access via HTTP to compromise Oracle WebCenter Sites.
Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert, or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data.</td></tr>
<tr><td><b>Impact Assessment</b></td><td colspan="3">Considering the framework chosen the risk was calculated as <b>6.5/10</b> which falls under the Medium risk. It violates the Confidentiality, Integrity of the organization.</td></tr>
<tr><td><b>Mitigation Plan</b></td><td colspan="3">Strongly recommends that customers apply security patches as soon as possible. patching the server up with the latest version is the best mitigation plan for this threat profile.

<b>Cost $299</b></td></tr>
<tr><td colspan="2"><b>Before mitigation</b></td><td colspan="2"><b>After mitigation</b></td></tr>
<tr><td><b>EF</b></td><td>60%</td><td><b>EF</b></td><td>20%</td></tr>
<tr><td><b>SLE</b></td><td>$ 22151 x 60% = $13290.6</td><td><b>SLE</b></td><td>$ 22151 x 20% = $4430.2</td></tr>
<tr><td><b>ARO</b></td><td>0.5</td><td><b>ARO</b></td><td>0.2</td></tr>
<tr><td><b>ALE</b></td><td>$13290.6 x 0.5 = $6645.3</td><td><b>ALE</b></td><td>$4430.2 x 0.2 = $ 886.04</td></tr>
<tr><td><b>Cost / Benefit</b></td><td colspan="3"><b>$6645.3 - $886.04 - $299 = $5460.26</b></td></tr>
<tr><td colspan="4"><b>Critical Assets – HRMS | Windows server 2012 (D)</b> [4]</td></tr>
<tr><td><b>Vulnerability and Threat Profile</b></td><td colspan="3">HRMS manages all Human resources-related tasks and runs on top of the windows server 2012 version which contains some outdated instances.

<b>Vul -</b> A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2019-1358.
<b>Threat –</b> A remote attacker can use this vulnerability to gain elevated privileges resulting in complete violation of the server</td></tr>
<tr><td><b>Impact Assessment</b></td><td colspan="3">This risk scenario completely violates all three security requirements of the system – Confidentiality, Integrity, and Availability - resulting in unauthorized disclosure and modification of information and interruption to the system services.
HRMS contains sensitive information, and this risk scenario can result in harming the reputation of the organization and employees and many other factors at a moderate level.
The Risk was identified as <b>8.0/10</b>, which will highly impact the system.</td></tr>
</table>

Mitigation Plan	The best control is to update the existing version of the server-to- the latest server 2016 version which has all the patches to the addressed problems. This will result in better reliable performance with high-security controls in place. **Cost $799**

Before mitigation		**After mitigation**	
EF	75%	**EF**	30%
SLE	$6054 × 75% = $4540.5	**SLE**	$6054 × 30% = $1816.2
ARO	0.4	**ARO**	0.2
ALE	$4540.5 × 0.4 = $1816.2	**ALE**	$1816.2× 0.2 = $363.24
Cost / Benefit	**$1816.2 - $363.24 - $799 = $653.96**		

Critical Assets: FIMS's Oracle NetSuite (E) [5]

Vulnerability and Threat Profile	Vulnerability in SuiteCommerce Advanced (SCA) Site's component of Oracle NetSuite service, by exploiting the vulnerability allows low privileged threat agent with network access via HTTP to compromise NetSuite SCA. A vulnerability is classified under CVE-2020-14728, CVE-2020-14729. **Vul. -** CVE-2020-14729. Affected Versions: Supported versions that are affected are before 2020.1.4. **Threat -** Successful attacks of this vulnerability can result in unauthorized creation, deletion, or modification access to critical data or all NetSuite SCA accessible data as well as unauthorized read access to a subset of NetSuite SCA data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts).
Impact Assessment	The Risk was calculated as **5.4/10**, where it mediumly impacts the confidentiality, integrity of the data stored in the server
Mitigation Plan	Upgrade Oracle NetSuite to the latest version. **Cost $999**

Before mitigation		**After mitigation**	
EF	25%	**EF**	10%
SLE	$ 10049 x 2.5 = $2512.25	**SLE**	$ 10049 x 0.1 = $1004.9
ARO	3	**ARO**	2
ALE	$2512.25 x 3 = $7536.75	**ALE**	$1004.9 x 2 = $2009.8
Cost / Benefit	**$7536.75 - $2009.8 - $999 = $ 4527.95**		

Critical Assets: LMS's Moodle (F) [6]

Vulnerability and Threat Profile	Identified the current password policies are not implemented strongly. CWE-521: Weak Password Requirements: In such a case, the vulnerability is considered critical with a CVSSv3 score of 8.1: **Vul.-** Current Password policies are not implemented strongly. **Threat -** The vulnerability may allow an attacker to guess users' passwords and gain unauthorized access to the application
Impact Assessment	The Risk was calculated as **8.5/10,** where it Critically impacts the confidentiality, of the student's information of the system.

Mitigation Plan	Highly recommended to Strengthening the password policy of Moodle to mitigate this vulnerability. A strong password should contain lower- and upper-case characters, digits, special symbols and be 8 – 12 characters long. Recommended implementing account lockdown mechanisms after the specific incorrect attempts of logins. The current password policy cites that the students need to update their credentials and personal details once every three months. With the increasing number of phishing and identity theft attacks seeing a rise, it is recommended to update the password policy to be more secured and precise. **Cost $200**

Before mitigation		**After mitigation**	
EF	35%	**EF**	25%
SLE	$ 2566 x 3.5 = $ 1555.75	**SLE**	$ 2566 x 2.5 = $ 1111.25
ARO	5	**ARO**	4
ALE	$ 1555.75 x 5 = $ 7778.75	**ALE**	$ 1111.25 x 4 = 4445
Cost / Benefit	**$ 7778.75 - $4445 - $200 = $ 3133.75**		

Critical Assets – LMS | HPE ProLiant MicroServer Gen10 X3216 (G) [7]

Vulnerability and Threat Profile	LMS has another LRMS which utilizes a single dedicated server which is an older initial release and was found unpatched for a vital vulnerability. **Vul -** HPE's (Hewlett Packard Enterprise) initial devices through the production lines come with a known factory vulnerability that involves Intel server platform service (SPS) v4.0 firmware present in certain HPE devices including this HPE ProLiant MicroServer Gen10. (Vul. Det. - CVE-2018- 3643) **Threat -** This SPS firmware present in Intel's architecture can be compromised by physical access thus, exposing this device to local DOS attacks and execution of arbitrary code by attackers
Impact Assessment	Execution of arbitrary code can lead to buffer overflows which normally results in system crashes. Disrupting service thereby directly violating availability which is a high-security requirement for this asset. Considering the framework chosen the risk was calculated as **6.5/10** which falls under the medium risk. It violates availability of the organization assets.
Mitigation Plan	Firmware update patch is available to be downloaded at HPE's support site. Recommend immediate download and installation. **Cost $0**

Before mitigation		**After mitigation**	
EF	45%	**EF**	10%
SLE	$4445 × 45% = $2000.25	**SLE**	$4445 × 10% = $444.5
ARO	0.6	**ARO**	0.3
ALE	$2000.25 × 0.6 = $1200.15	**ALE**	$444.5 × 0.3 = $133.35
Cost / Benefit	**$1200.15 - $133.35 - $0 = $1066.8**		

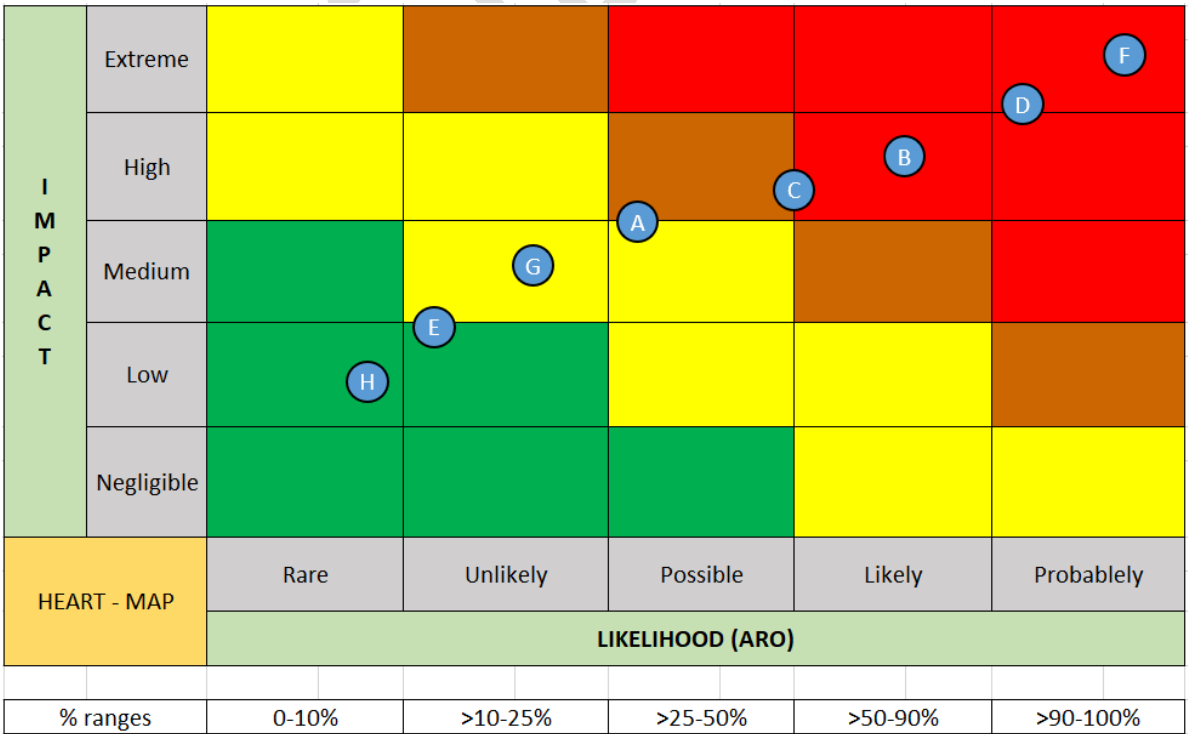
Critical Assets: IRMS (H)

Vulnerability and Threat Profile	No implementation against the unauthorized access to the computers, servers in the IRMS room. This will lead to:

	• Unauthorized disclosure of information. • Interruption of regular operations **Vul. -** Unauthorized personnel can access to the system intentionally manner. **Threat -** This vulnerability may allow an attacker to unauthorizedly access to the system and that may lead to the information disclosure		
Impact Assessment	The Risk was calculated as **4/10,** where it Critically impacts the availability of the physical assets and confidentiality, the integrity of the data stored in the server.		
Mitigation Plan	Implement a CCTV system for the monitor activities and operations IRMS. **Cost $799**		
Before mitigation		After mitigation	
EF	50%	EF	10%
SLE	$ 7566 x 0.5 = $ 3783	SLE	$ 7566 x 0.1 = $ 756.6
ARO	2	ARO	1
ALE	$ 3783 x 2 = $ 7566	ALE	$ 756.6 x 1 = 756.6
Cost / Benefit	**$ 7566 - $ 756.6 - $799 = $ 6010.4**		
Vul. – Vulnerability; Risk Level = Qualitative Risk Level = Heat Level of the Threat			

2.9 Heat Map

The Bellow diagram represents the heat/risk level of each asset in an illustrative manner.



3 Summary

The risk assessment was conducted using the Octave Allegro framework and Quantitative Analysis framework to determine and analyze the critical assets of the Infotec Institute. It has been identified that multiple hardware/physical and software threats during the risk assessment.

1. SIMS

It was identified that this system is the core system within the institute. Due to the lack of space and pertaining conditions, it is recommended to purchase a new server rack cooling system to prevent heating issues. Additionally, it was also identified to upgrade the oracle web portal of SIMS since the existing version was exploitable due to a middleware vulnerability. An attacker can easily exploit the vulnerability that allows unauthenticated attackers with network access via HTTP to compromise Oracle WebCenter Sites. Effected Versions: **12.2.1.30 and 12.2.1.4.0: CVE-2020-14613.** It has been recommended to patch the portal firmware to the latest version.

2. HRMS

HRMS is responsible for managing employees maintaining their details and respective roles. The existing server windows 2012 version is vulnerable to remote code execution - **CVE-2019-1358.** A remote attacker can use this vulnerability to gain elevated privileges resulting in complete violation of the server. Recommended updating the server version to 2016 which has all the patched to the addressed issues.

3. FIMS

According to the assessment, the SCA site's component of Oracle NetSuite service which is running in FIMS is found to be vulnerable. A vulnerability is classified under **CVE-2020-14728, CVE-2020-14729.** Successful attacks of this vulnerability can result in unauthorized creation, deletion, or modification of access to critical data. The recommendation was to upgrade the Oracle NetSuite to the latest version.

4. LMS

Moodle was identified as a possible target because of the poor password policies implemented. It was recommended to improve and consider high technical password protection mechanism to mitigate the threat. LMS | HPE ProLiant MicroServer Gen10 X3216 server was identified with an exploitable vulnerability **CVE-2018- 3643** which will lead to buffer overflows. It is recommended to patch the latest version from the official support site according to the subscription.

5. IRMS

All the servers, computers in labs, and all other infrastructures are managed by the IRMS. The technical staff has access to this system. The main area of concern was lacking a proper monitoring system for the computer labs connected with IRSM room. The recommendation was to implement a CCTV system to monitor activities and operations on IRMS.

It is evident, that most of the vulnerabilities exist due to irregular updating and installations, of version and patches, and improper decisions in first installs. It is highly recommended that the organization reevaluates the security policy and enforces new update and install policies to avoid effectively and efficiently most similar risk scenarios in the future.

4 References

[1] “Windows Server 2016 - Wikipedia.” https://en.wikipedia.org/wiki/Windows_Server_2016 (accessed May 07, 2021).

[2] “Student Information System Software | PowerSchool.” https://www.powerschool.com/solutions/student-information-system/powerschool-sis/ (accessed May 07, 2021).

[3] “Oracle WebCenter Portal Reviews & Ratings 2021.” https://www.trustradius.com/products/oracle-webcenter-portal/reviews (accessed May 07, 2021).

[4] “Windows Server 2012 - Wikipedia.” https://en.wikipedia.org/wiki/Windows_Server_2012 (accessed May 07, 2021).

[5] “NetSuite | Oracle Academy.” https://academy.oracle.com/en/solutions-cloud-netsuite.html (accessed May 07, 2021).

[6] “Moodle - Open-source learning platform | Moodle.org.” https://moodle.org/ (accessed May 07, 2021).

[7] “proliant server dl380 | eBay.” https://www.ebay.com/sch/i.html?_nkw=proliant+server+dl380&norover=1&mkevt=1&mkrid=711-34000-13078-0&mkcid=2&keyword=proliant+server+dl380&crlp=_2-1300-0-1-1&MT_ID=&geo_id=&rlsatarget=kwd-77515702970723%3Aloc-36&adpos=&device=c&mktype=&loc=36&poi=&abcId=&cmpgn=329851884&sitelnk=&adgroupid=1240249267725566&network=s&matchtype=e&msclkid=685784cea75f1d1cf726e45a719ae7f5&ul_noapp=true (accessed May 07, 2021).

[8] C. Alberts, A. Dorofee, T. Operationally, C. Threat, V. Evaluation, and T. Profile, “Threat Profiles,” pp. 1–14.

[9] C. Alberts and J. Stevens, “Introduction to the eastern approach,” *Pregnancy and Childbirth*, no. August, pp. 121–129, 2010, doi: 10.1016/b978-0-7020-3055-0.00004-2.

[10] S. Institute, “Interested in learning SANS Institute InfoSec Reading Room In tu , A ll r igh,” *Worm Propag. Countermeas.*, p. 36, 2004.

[11] “Online Payroll + HR That Small Businesses Love | OnPay.” https://onpay.com/ (accessed May 07, 2021).

[12] “TalentLMS: Cloud LMS Software - #1 Online Learning Platform.” https://www.talentlms.com/ (accessed May 07, 2021).

[13] “TS150 | Tower Server | Lenovo US.” https://www.lenovo.com/us/en/data-center/servers/towers/ThinkServer-TS150/p/77LS7TS150V (accessed May 07, 2021).

[14] “Open Source ERP and CRM | Odoo.” https://www.odoo.com/ (accessed May 07, 2021).

[15] “Bitdefender GravityZone Business Security.” https://www.bitdefender.com/business/smb-products/business-security.html (accessed May 07, 2021).

Appendices

Appendix A

A.1 Asset Value Parameters

A.1.1 Qualitative

It has been identified that there exist 3 types of qualitative labels to define information system assets belonging to Winterfell. These three labels were established after concluded discussions with the Managers, High Technical Staff, and separate system custodians. The labels were authorized by the Executive Members. The Labels are as follows.

1. Primary
2. Secondary
3. Tertiary

A.1.2 Quantitative

$$\boxed{Asset\ Value = Physical\ Value + \text{Informational}\ Value}$$

• Physical Value – Monetary value given to the asset based on perceptible values such as the prices of the hardware, subscriptions paid for services related to the assets – firewall subscriptions, etc.- and many other similar physical prices. This was considered a responsibility of the risk management team. Managers, High Technical Staff, and separate system custodians were involved in defining the monetary values of those hardware, subscriptions, etc.

• Informational Value – Monetary value is given to the asset-based on its importance to the organization. This was considered not a responsibility of the risk management team. The informational value of each asset was decided by the Managers, High Technical Staff, and separate system custodians and was finalized and authorized by the Executive Members.

A.2 Assets Values Calculations

Asset No	Asset	Qualitative Label	Quantitative Value		
			Informational Value (USD)	Physical Value (USD)	
1	**SIMS**	Primary	$10,000	Hardware	
				Name	Price
				IDS and IPS	$499
				Firewall - Cloudflare	$2,499
				PowerSchool SIS	$6,000
				Total Hardware Value = $8998	
				Software	
				Name	Price
				Solarwinds-security-event-manager	$399
				Cloud Subscription (2000TB) – Back up	$2,000
				Active Directory Server	$555
				Oracle WebCenter Portal	$199
				Total Software Value = $3153	
			Asset Value = $8998 + $3153 + $10000 = $22151		
2	**HRMS**	Secondary	$3,500	Hardware	
				Name	Price
				Dell PowerEdge T30 Xeon E3-1225 v5 8GB 1TB SATA Tower Server	$600
				Fingerprint Time Attendance Machine	$200
				Total Hardware Value = $800	
				Software	
				Name	Price
				Windows 2012 Server	$555

				Cloud Subscription (2000TB) – Back up	$200
				Workday EMS	$999
				Total Software Value	
			Asset Value = $800 + $1754 + $3500 = $6054		
3	**FIMS**	Primary	$8,000	Hardware	
				Name	Price
				Dell PowerEdge T30 Xeon E3-1225 v5 8GB 1TB SATA Tower Server	$600
				Total Hardware Value = $600	
				Software	
				Name	Price
				OnPay	$450
				ORACLE NetSuite	$999
				Total Software Value = $1449	
			Asset Value = $8000 + $1449 + $600 = 10049		
4	**LMS**	Tertiary	$1,899	Hardware	
				Name	Price
				HPE ProLiant DL380 Gen10 server	$899
				Total Hardware Value = $899	
				Software	
				Name	Price
				Talent LMS	$799
				web librarian Web Application	$149
				Moodle	$699
				Total Software Value = $1647	
			Asset Value = $1899 + $1647 +$899 = $4445		
5	**IRSM**	Tertiary	$999	Hardware	
				Name	Price
				Lenova ThinkServer TS150	$699

				Computers	$5,000
				Total Hardware Value = $5699	
				Software	
				Name	Price
				Talent LMS	$799
				web librarian Web Application	$69
				Moodle	$868
				Total Software Value = $1647	
			Asset Value = $868 + $699 + $999 + $5000 = $7566		

Appendix B

Allegro Worksheet 8	**Critical Information Asset Profile**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
SIMS	SIMS is the most important asset of this institution. Because of that this SIMS system managing student details, examination details, internet portal login details, and student registration & online payment details.	All the examination information, student information, internet portal information, online payment, and registration information are stored on this system.
(4) Owner(s) *Who owns this information asset?*		
Student Affairs, High Technical Staff		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Student Affairs
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	High Technical Staff

❑ Availability	This asset must be available for this personnel to do their jobs, as follows:		Students Student Affairs Academic Staff
	This asset must be available for __24___ hours, __7___ days/week, ___52__ weeks/year.		99.9%
❑ Other	This asset has special regulatory compliance protection requirements, as follows:		Audit Redundancy
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk	Threat	Information Asset	SIMS - Power school SIS		
		Area of Concern	Power school SIS does not have a proper recovery control mechanism		
		(1) Actor *Who would exploit the area of concern or threat?*	Unauthorized Personnel		
		(2) Means *How would the actor do it? What would they do?*	If the services get sudden pauses and needed to recover, the lack of proper recovery mechanisms will ensure there are fewer chances to recover the data fully to restore them to a working state.		
		(3) Motive *What is the actor's reason for doing it?*	Accidental		
		(4) Outcome *What would be the effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	To disrupt the process of the functional operations and making services unavailable		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **70 %**	❑ **Medium** **35%**	❑ **Low** **15%**
	(7) Consequences			(8) Severity	

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Unavailability of proper records in case of recovery will result in the sudden collapse of institutional functions.	Reputation & Customer Confidence	4	2.8
	Financial	5	3.5
Legal issues and Fines will be issued since students will be left with no choice at all but to expect the institute to carry out their work	Productivity	8	2.4
	Safety & Health	-	-
There is a chance that the institute will face financial collapse if the situation gets worse.	Fines & Legal Penalties	6	4.2
	User-Defined Impact Area	-	-
		Relative Risk Score	**12.9**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply to this container? What residual risk would still be accepted by the organization?*
Power School SIS server	Invest in a cloud backup solution choosing a proper subscription method and implement proper recovery control mechanisms

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**		
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*	
Human Resource Management System (HRMS)	This system responsible for all HR activities, Employee attendance Information, Payroll system information, Employee profiles information	All Employee information is stored in this system.	
(4) Owner(s) *Who owns this information asset?*			
HR Manager			
(5) Security Requirements *What are the security requirements for this information asset?*			
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	HR Manager HR Support staff	
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	HR Manager HR Support staff DB admin	
□ **Availability**	This asset must be available for this personnel to do their jobs, as follows:	HR Manager HR Support staff Executives	
	This asset must be available for __24___ hours, __365___ days/week, __52__ weeks/year.	99.9%	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Audit Non-repudiation	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	Threat	Information Asset	Human Resource Management System (HRMS)
		Area of Concern	*The server firmware version has vulnerabilities.*
		(1) Actor *Who would exploit the area of concern or threat?*	Black Hat Hackers
		(2) Means *How would the actor do it? What would they do?*	The attacker will use a remote code execution vulnerability that is already existing in the server firmware to exploit.
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome *What would be the effect on the information asset?*	□ **Disclosure** □ **Destruction** □ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Exploiting this will result in disclosure of employee details and disruption of services in a way that will affect the operational functions of the institute
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **75%** □ **Medium** **50%** □ **Low** **20%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Data and Information disclosed to the external parties since the attacker can get access through the exploitation which will result in loss of customer confidence	Reputation & Customer Confidence	6	3
	Financial	7	3.5
Can modify Data/Information which will affect the financial and productivity of the company	Productivity	7	3.5
	Safety & Health	-	
	Fines & Legal Penalties	4	2
	User-Defined Impact Area	-	
		Relative Risk Score	**12**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply to this container? What residual risk would still be accepted by the organization?*		
HRMS Win 2012 Server	The best possible control is to upgrade the existing version of the server to the latest 2016 version which patches this vulnerability with more security controls that will eventually provide reliable and secure transactions among the operations in the institute.		

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
FMIS Financial Management Information System	Responsible for the process of planning funds, organizing available funds, controlling financial activities including student payment handling, staff salary information, etc.	All the financial information is stored in this system.
(4) Owner(s) *Who owns this information asset?*		
Financial Manager		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Financial manager, Financial support staff, HR Manager
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	financial manager, DB Admin

□ **Availability**	This asset must be available for this personnel to do their jobs, as follows:	Financial manager, Administrator Financial support staff
	This asset must be available for __24__ hours, __7___ days/~~week~~, _365____ weeks/~~year~~.	99.99%
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Audit

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10		Information Asset Risk Worksheet	
Information Asset Risk	Threat	Information Asset	Financial information and records
		Area of Concern	System firmware is not up to date. The current version has known vulnerabilities.
		(1) Actor *Who would exploit the area of concern or threat?*	Unauthorized Personnel
		(2) Means *How would the actor do it? What would they do?*	An attacker will use network access to escalate the privileges already assigned to the user using various tools
		(3) Motive *What is the actor's reason for doing it?*	Deliberate
		(4) Outcome *What would be the effect on the information asset?*	□ **Disclosure** □ **Destruction** □ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	This will disrupt the workflow of the company and disclosure the financial records violating integrity and confidentiality.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **75%** □ **Medium** **50%** □ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*

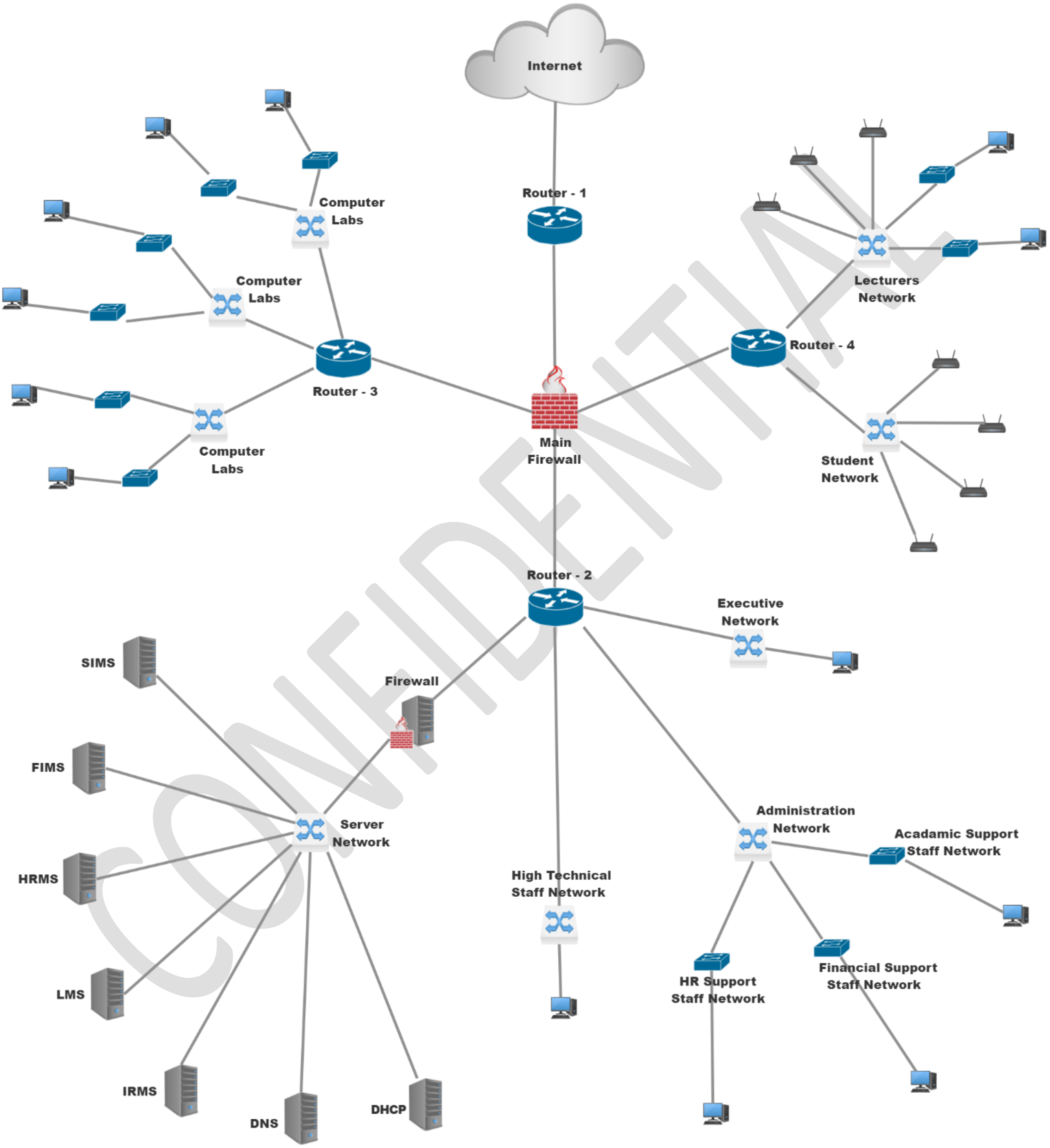
		Impact Area	Value	Score
	Disclosure of financial and sensitive information can harm the confidence of employees and damage the reputation	Reputation & Customer Confidence	6	3
		Financial	5	2.5
	Overall productivity will be affected since competitors will gain an advantage	Productivity	8	4
		Safety & Health	-	-
		Fines & Legal Penalties	2	0.5
		User-Defined Impact Area	-	
			Relative Risk Score	**10**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
□ **Accept**	□ **Defer**	□ **Mitigate**	□ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply to this container? What residual risk would still be accepted by the organization?*
FIMS - Oracle NetSuite	Review the latest security patches and upgrade Oracle NetSuite to the latest version.

Appendix C

Network Diagram


Internet
Router - 1
Computer Labs
Computer Labs
Router - 3
Computer Labs
Main Firewall
Router - 4
Lecturers Network
Student Network
Router - 2
Executive Network
Firewall
SIMS
FIMS
HRMS
LMS
IRMS
DNS
DHCP
Server Network
High Technical Staff Network
Administration Network
Acadamic Support Staff Network
HR Support Staff Network
Financial Support Staff Network