Cloud, IoT and Enterprise

Security Assignment

Case Study Report

M.Tech. Software Systems
WILP
BITS, Pilani

Team Members:

Name	Mail ID
Ashutosh Batra	2021MT12025@wilp.bits-pilani.ac.in
Saquib	2021MT12266@wilp.bits-pilani.ac.in
Rohit Joshi	2021MT12355@wilp.bits-pilani.ac.in

INDEX

Context 3
Why security is important in this setup? 4
BITS security goals 5
Use Cases 5
Different types of attack could occur 11
Security Architecture 13
Head Office 13
Regional Office 17
Regional Campus 21
Threats and Risk Assessment 25
Applicable Laws and Regulation 32

Context

BITS WILP (Work Integrated Learning Program) Division is aimed to provide the highest quality education alongside with your ongoing technical career, so that you stay up to date with the latest technology stacks. BITS provides facilities to attend classes and assessments online with amazing streaming platforms like Microsoft Teams to attend lectures, e-learn portal to access your courses, related documents, online library support etc. are available to access. Following are the key elements and provisions of BITS WILP Program:

- Learning material
- Facilities for practical work
- Enabling questions and discussions
- Assessments
- Student Support service

Lectures, simulations, Remote Labs and case studies are delivered by BITS faculties online. Which only works in BITS server, outside of BITS server it cannot access any material or any remote labs or online lectures. So, securities concerns are easily resolved by setup everything on own server and put restrictions for outside access and easily tackle below security concerns:

- Legal and Regulatory Compliance
- Internal and External Attacks
- Protection of confidentiality and privacy
- Any accidental damage to assets and system

WILP has in total 11 locations (1 Head Office, 3 Regional Offices, and 7 Regional Campuses)

Head Office

Head office controls the Central administration of Staff, students and central office systems.

Regional Offices

3 regional offices hold student records, regional office systems and payroll.

Regional Campuses

7 regional campuses have IT remote and in-house labs, staff workstations, and local office systems, hardware's, LAN cables, etc…

Why is security important in this setup?

COVID 19 forces many students, faculties and institutes to shift to online teaching, while all teaching started happening online, internet usage, software usage are also increasing and at the same time data is also started putting online on any secure cloud. With the increase in data collection, the need of having to secure the same is on the rise as well. BITS, being one of the most prestigious institutes in India as well as globally, so by using the opportunity of online study they decided to start WILP for IT professionals without their job break. With these changes being enforced, one can rightly assume that the cyber security landscape too has changed drastically. After COVID-19 cyber-attacks are also increased as most people are at home and suffering from the internet totally. Even though this might be the new normal, the cyber threat landscape remains the same as to what we faced while being in our workplace if not more.

While it may seem that the lectures and methods of grading the students are the most important data to protect, it's important to remember that other private information, including employment information, official enterprise ids, mentor employment information, etc., must also be protected from cyber-attacks. The increase in recent cyber-attacks and data exposures is mostly due to remote working.

Universities and colleges are reportedly still plagued by occurrences like ransomware, when offenders encrypt or otherwise limit access to the material and demand payment before releasing it. Threats to publish the stolen data on the dark web are occasionally made in an effort to raise the payment.

Poor data management and a lack of data hygiene constitute vulnerability. Poor data hygiene is still a danger, even though distance learning courses use 3rd party platforms to facilitate cooperation between the students and faculty. The biggest hazard is posed when students exchange unencrypted emails and files containing sensitive information back and forth via unencrypted emails or communication platforms. The only way to prevent data breaches and leaks is through appropriate data management.

While it is impossible to make an infrastructure completely secure, one may do their best to prevent serious harm by securing the systems and making sure the right procedures are followed while accessing and using the data.

BITS WILP - Security Goals

Security Goals
1. Compliance with privacy laws and other security rules.
2. Threats from both internal and external sources in terms of cyber security (rogue students)
3. Information asset confidentiality, integrity, and accessibility. example: student records
4. Safeguarding WILP computer systems from unintentional harm.
5. Align with the strategy, goals, and educational objectives.
6. A consistent approach to risk management
7. Meeting the required basic baseline security controls
8. Obtain security guarantees from the owner of the system or the data custodian.
9. For the data, apply classification and encryption rules.

Use Cases

As part of their WILP Program, BITS provides the essential materials (such as course notes, videos, etc.) and services (such as lectures) to distant students via the eLearn Portal (Taxila) and Teams over the Public Multimedia Network. Students can communicate and submit work using the same platform. The significance and kind of the following recognized information in the transmission determine security considerations:

- Student Records
- Marks for assignments and tests
- Payroll Data

This calls for a minimum of three layers of confidentiality:

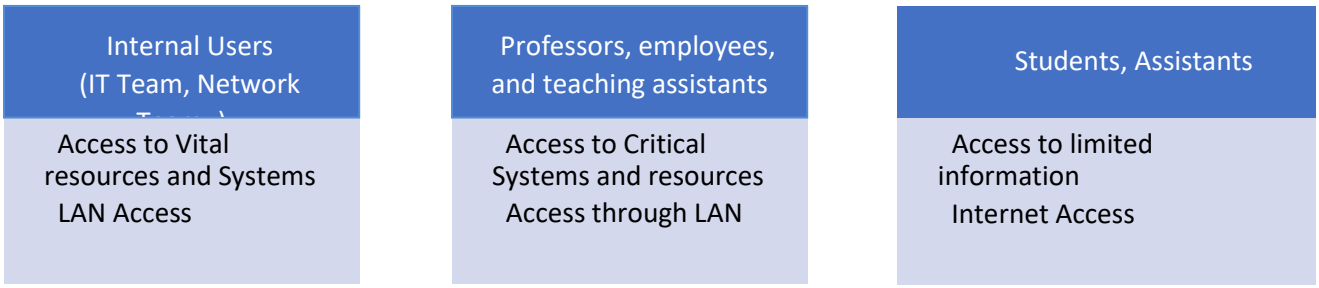
1. Data that is accessible to the public (like brochure)
2. Details that are only available to students who are enrolled (like notes)
3. Information only available to certain faculties or students (like grades, pay)

Consideration must be given to data availability and integrity in addition to confidentiality.

1. Staff, instructors, and students should have 24/7 access to course materials, lectures, texts, virtual labs, and online library servers. (Availability)

2. Educational data and metrics should be kept and maintained in their original, unaltered state (integrity)

For their various needs and via various channels, internal teams (IT Team, Network Team, etc.), faculties, assistants, and students engage with WILP's system. Based on the sensitivity of the information, the activities taken by the users, the security provided by the communication channel, and the level of confidence in the user, these are divided into three main use cases to examine the associated risk and security concerns.



1. The initial use case includes the IT Team, Network Team, and other Internal Department Users.

   These users evaluate the most vital system resources and have the highest level of confidence. These users' entry points into the system and methods of resource access determine the level of trust they develop. In a nutshell,

   These comprise the internal users that BITS management has hired after conducting a thorough interview and background check. These fall under the category of "Internal Users," and the security guidelines for internal users apply to them.

   These users have permission to access the vital resources and information in the BITS system. Despite the highest level of data sensitivity, these users can only access the system through internal systems and components. In the office, access is granted after physical authentication procedures.

   These users then gain access to the systems using a special credential that manages their least necessary rights and role-based access control.

In contrast to Public Media Channel, LAN provides the highest level of security assurance and removes the biggest threat from the systems that are being utilized by the users.

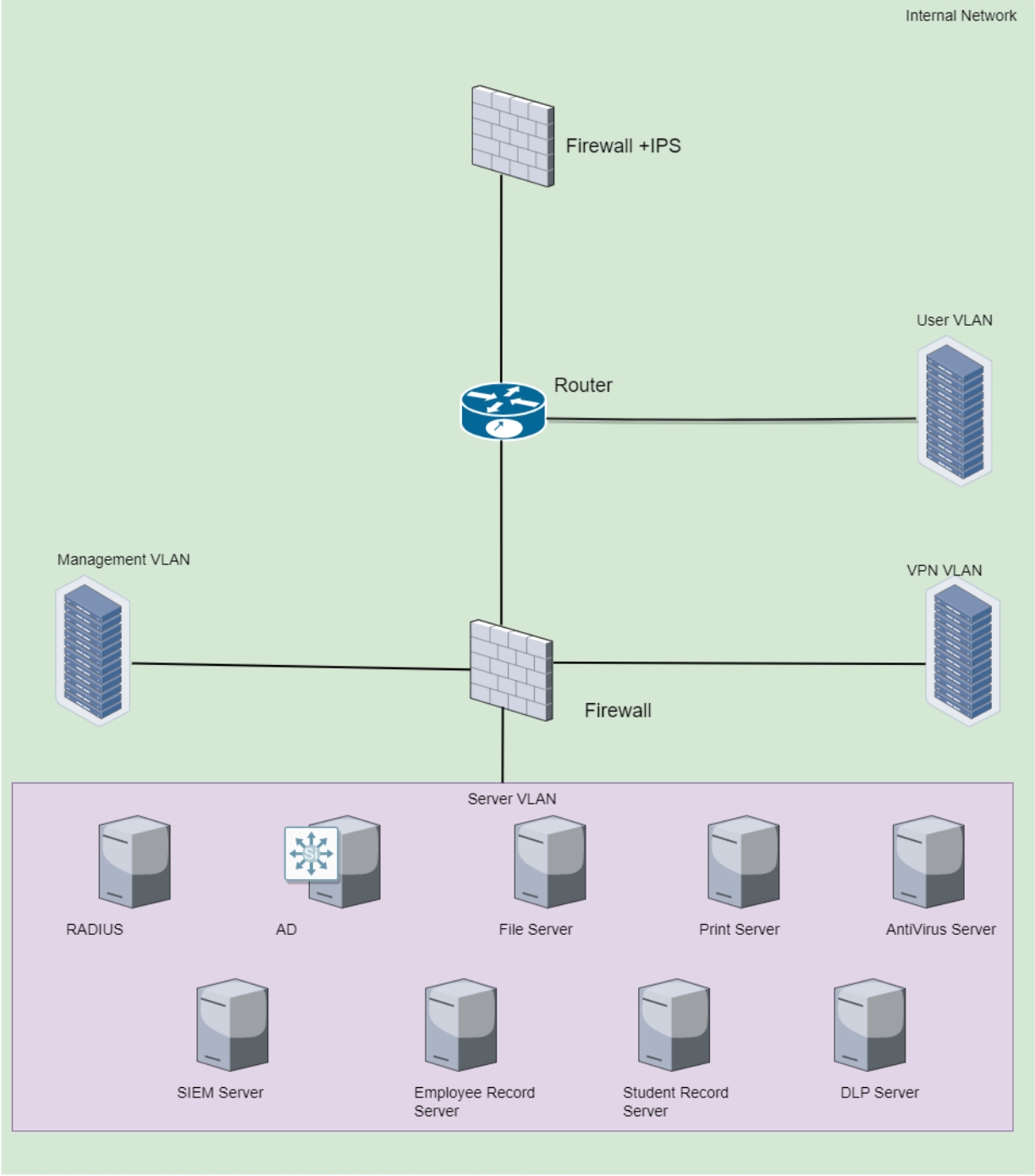


Fig 1.1: Internal User Network

A data loss prevention system is in place to stop any data from leaking to the public.

The relevant policies and processes clearly declare that these users' physical and logical access is ended upon termination.

2. In this second use scenario, where users are given remote access to vital systems, services, and resources, faculty, staff, and assistants are taken into account. These users' access to the resources is crucial because they have access to the student's personal information and evaluation records.

   Only the domain systems offered by the university, remote desktop, or a virtual private network are used by these individuals to access the system.

   A secure tunnel is built between the user's PC and the university's resources thanks to the VPN. The sensitivity of the data/resources and the necessity for their integrity level are both quite high. However, every interaction with the data is recorded, and any reading, updating, or publishing of the data is the user's responsibility and accountability.

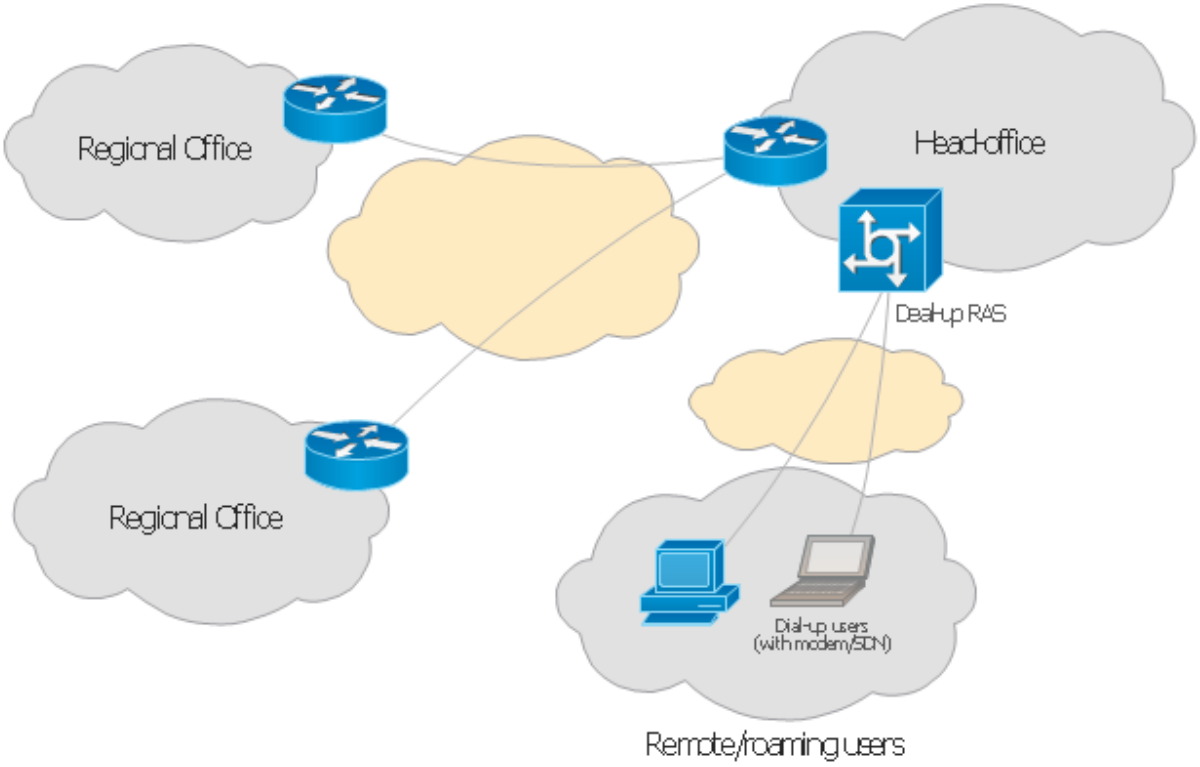


Fig 1.2: Communication between Head Office & Remote Users

Users can only access the system using their individual identity after being authenticated. For authorized users, role-based access control and authorization are maintained.

Users must adhere to recommended best practices and methods when using remote systems.

3. In the third use case, where users access the system through a public channel, the majority of security concerns are raised; students and certain assistants are taken into consideration. The student only has restricted access to non-business sensitive information as necessary by their function. Use cases that are pertinent to students are being carefully examined to determine the risks and security concerns involved.

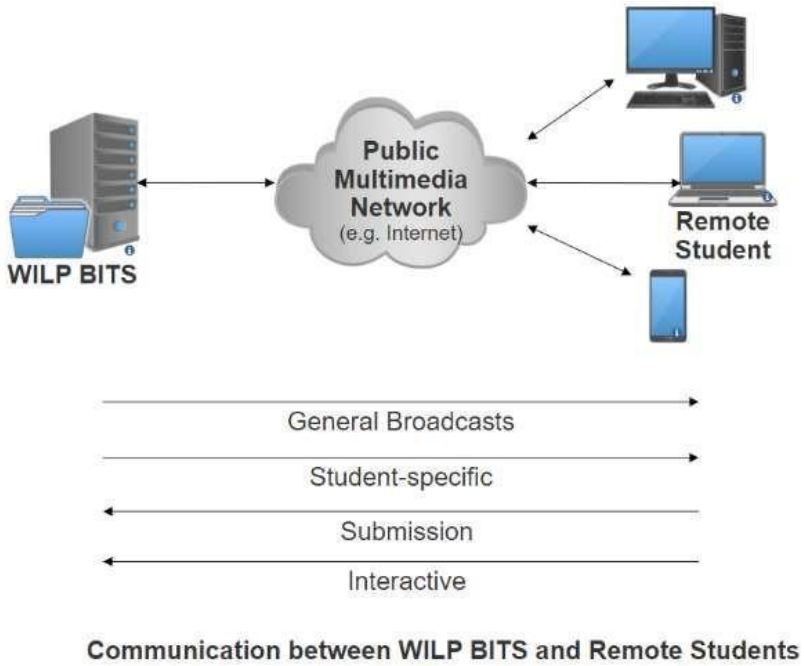
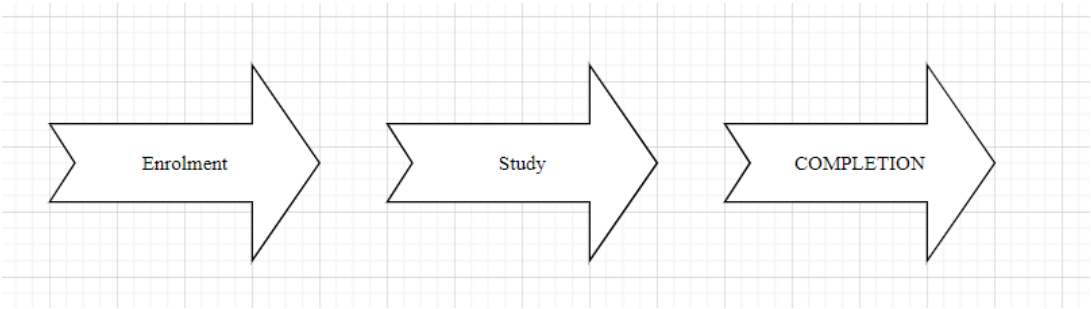


Fig 1.3: Communication between WILP & Remote User

The stages of the student contact lifecycle using WILP systems are as follows:



Use cases with respect to each stage involve different security concerns which are stated below.

Enrolment

Remote students are identified at this stage who are then enrolled and access to allocated resources is enabled. Following are the considerations from a security point of view.

To enroll in the WILP program, the student must provide the necessary documentation in addition to their prior credentials. Student Records safely store all the information that can contain personal information. Legislation pertaining to privacy must be regulated and followed.

Students' payments are sent to payment gateways or other EMI-supporting settings. The WILP division does not retain card information, and the Payment Interaction Page has been made PCI/DSS compliant.

Here, an authentication system is set up for future communication and access. It takes care of Authentication, Authorization, Confidentiality, and Non-repudiation. Before gaining access to the system, each time, user credentials must be produced, distributed, and entered.

Study

Students and faculties both access the system in this stage and are considered as End Users for Study stage. End Users are actively engaged in this stage and interact with the system frequently for consumption of course material, assignments, quizzes, examinations, grading etc. Following are the identified consideration in this stage:

Only the information that is pertinent to the end user should be shown to them and accessible to them. Unauthorized information access must be avoided. In order to address security concerns, role-based access control has been added to the security architecture.

Systems must be accessible to end users whenever they need them. The integrity of any submissions made by the end user must be protected along with non-repudiation.

The lecture/tutorial sessions must retain a secure communication connection. Unauthorized users cannot communicate with or access the

resources.

To specific students and other parties who may be interested, grade disclosure must be kept confidential.

Interaction with end users and overall statistics will be tracked, recorded, and kept in the system. Information that should be kept private and only seldom made public.

Completion

With regards to completion of the module following security scenarios shall be considered. Access to future information shall be restricted, and requires the completion of the current stage to move forward. Proof of submission shall be provided and access to modify shall be restricted. Access to previously held modules shall be allowed to restrict if required.

Different Types of attack could occur

As seen by the recent widespread reporting of breaches in universities and schools, cyber-attacks in the education industry appear to be increasing year over year. This could cause significant harm in the form of monetary loss or, worse yet, compromises in student safety and data. It is crucial for a university, like BITS, Palani, to assess the risk and comprehend what information is exposed to unauthorized access. Let's examine some of the most well-known cyber-attacks and how BITS security mechanisms and architecture work to stop them.

DDoS Attacks-The majority of attacks used by cybercriminals are distributed denial of service attacks. The attacker's primary goal is to interfere with the institute's network in order to reduce production. In a Dodos assault, the attacker floods the target with Internet traffic, overwhelming it or its infrastructure. Consequently, regular traffic is kept from getting to its destination.
BITS has implemented the WAF solution, which includes the "Bot Manager Premier" tool. This tool analyses traffic and uses advanced bot detection methods based on AI models for analyzing user behavior and browser fingerprinting.

Injection Attacks- these kinds of attacks occur when the attacker inserts malicious payloads/code into the server using SQL, commands forcing the server to deliver protected information.

BITS using Site Defender which has a set of predefined WAF Rules to prevent SQL Injection, Command Injections and all the other injections. Additionally, it has enhancements where admin can add Custom Rules to prevent any advanced injection attacks. The application also undergoes penetration testing both internally and from external vendors bi-annually.

Phishing- one of the most common types of attack. It relies solely on the victim's own vulnerabilities, mostly the emotions and ignorance. It is the practice of sending fraudulent communication that appears to come from a reputable source. Most of the phishing attempts occur via email.

Currently, BITS uses Fortinet's antivirus solution which includes phishing prevention solutions which include powerful anti-spam techniques and impersonation detection. Additionally, educating the students and employees receive annual training regarding identification of phishing mails.

Privilege escalation- this happens when a malicious user exploits a bug or design flaw to gain elevated access to resources that should ideally be unavailable to them. There are two types of escalations possible – horizontal and vertical. It is very hard to detect privilege escalation attacks especially if a rogue user who might have access to a legitimate system compromises the security.

BITS ensures that all data that is sent from server to client is tamper proof using a digital certificate. Additionally, all critical data is kept on the server side and data sent to the client is always encrypted.

Cross-Site Scripting (XSS)- Cross-site scripting targets the users of a site instead of the web application itself. The malicious hacker inserts a piece of code into a vulnerable website, which is then executed by the website's visitor. The code can compromise the user's accounts, activate Trojan horses or modify the website's content to trick the user into giving out private information.

BITS can protect the website against XSS attacks by setting up a web application firewall (WAF). WAF acts as a filter that identifies and blocks any malicious requests to your website. BITS already have WAF in place which protects it from cross site scripting attacks.

Password Attacks: It is one of the most common types of personal data breaches. It is when a hacker tries to steal the user's password. There are multiple ways to implement a password attack based on the design of the system. Some of the most common methods include brute force attacks, spear phishing, dictionary attacks and credential stuffing.

Lately, BITS has implemented Open Athens SSO authentication which reduces the attack surface of an attack largely. This ensures that the user needs to login once each day and use only one set of credentials. It uniquely identifies the user and ensures compliance and the information provided by SSO is encrypted and transmitted across the network.

Security Architecture

Security Architecture has been prepared for each of the office with following considerations:

1. Responsibilities of office
2. Services provided by office
3. Data held at each office

The identified security issues are being addressed by the designed security framework and following architecture. The architecture has been designed with a combination of established and enhanced security technologies.

Head Office

Head Office contains most of the critical infrastructure including RADIUS server, Active Directory, DLP Server, SIEM correlation server, personnel records amongst others. Since the crown jewels are within the Head Office network, they need to be protected sufficiently. For that reason, there are a total of 3 Next Generation Firewalls and VLAN (Virtual Local Area Network) segregation to ensure that access to the server VLAN (crown jewels) is restricted and only role based. Further, there is an external Demilitarized Zone (eDMZ) which hosts the web server and ensures that the BITS website is accessible to users from the internet. The web server resides behind a load balancer to ensure that latency issues are taken care of. Internal Demilitarized Zone (iDMZ) resides on the other interface of the perimeter firewall, and hosts servers supporting the web server (DB server, Application server, Mail server and FTP server). Head Office is connected to regional offices and regional campuses using a dedicated and secure MPLS link.

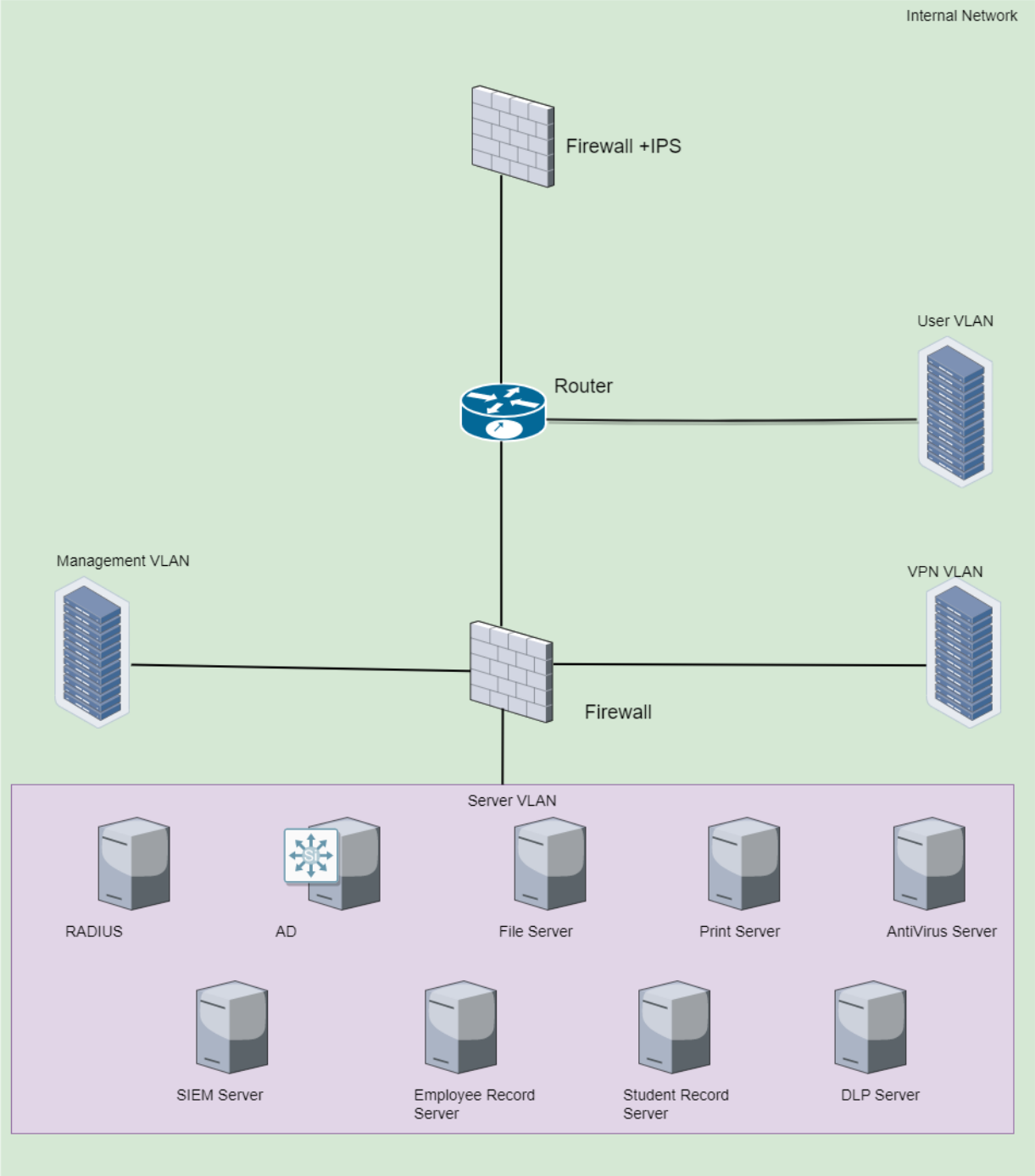


Fig 2.1: High level diagram of Head Office

Head Office is one of the most critical infrastructures to the BITs system. One must give equal importance to security and redundancy at the same time to ensure the infrastructure is always secure and up and running. The system is supported by two ISP providers (Airtel and Jio) which work with 5Ghz and 2.4 GHz bandwidth of the internet. This ensures that there is

connectivity throughout. Cisco Router is used to route traffic from ISP which is then monitored and filtered by the next gen firewall by Fortinet. Mesh topology is followed at this phase where the routers and the firewall are connected with each other.

Our infrastructure has an internal and external DMZ. The external DMZ ensures that all traffic that is going to the end user via the web server is monitored via WAF. We have also implemented an Application Load Balancer Cloudlet which is a multi-layered global server load balancer purpose-built to solve hybrid/multi-cloud application delivery and traffic management challenges. MS Defender is the WAF solution that has been placed in front of the Web Server. MS Defender is one in a suite of security products that also includes DDoS protection, bot management, and an API gateway. F5 Web Application Firewall provides always-on and highly scalable protection against web application attacks including SQL injections, cross-site scripting, and remote file inclusion – while keeping application performance high. The Load balancer and WAF in turn leverages the advantages of the globally distributed F5 Intelligent platform and delivers end users the authorized data without any hassle. The internal DMZ consists of business-critical servers including Mail Server (Google), FTP server, DB server (My SQL) and the application server.

The internal network is supported by a Dell DMZ switch which is connected to a Fortigate IPS/Firewall which then routes traffic to different VLANs. For the user VLAN, the F5 WAF is again in position to prevent various attacks. Fortinet firewall is in place for Management VLAN.

Since data stored in BITs is very critical and there needs to be a disaster recovery plan, there is a Disaster Protection or a primary site that is in place behind the management VLAN. It also ensures that static data is presented to the end user in case the server is down instead of displaying any server errors.

The server VLAN is managed by DELL EMC VxRail which integrates everything in a hybrid fashion. The Server VLAN consists of all the critical server which includes File Server, SIEM server, DLP Server, Replication server, Antivirus server, Print server, RADIUS, ERP Server, Employee Record server and finally, the student record server.

Lastly, a secure MPLS link is connected from the head office to the regional office regional campus.

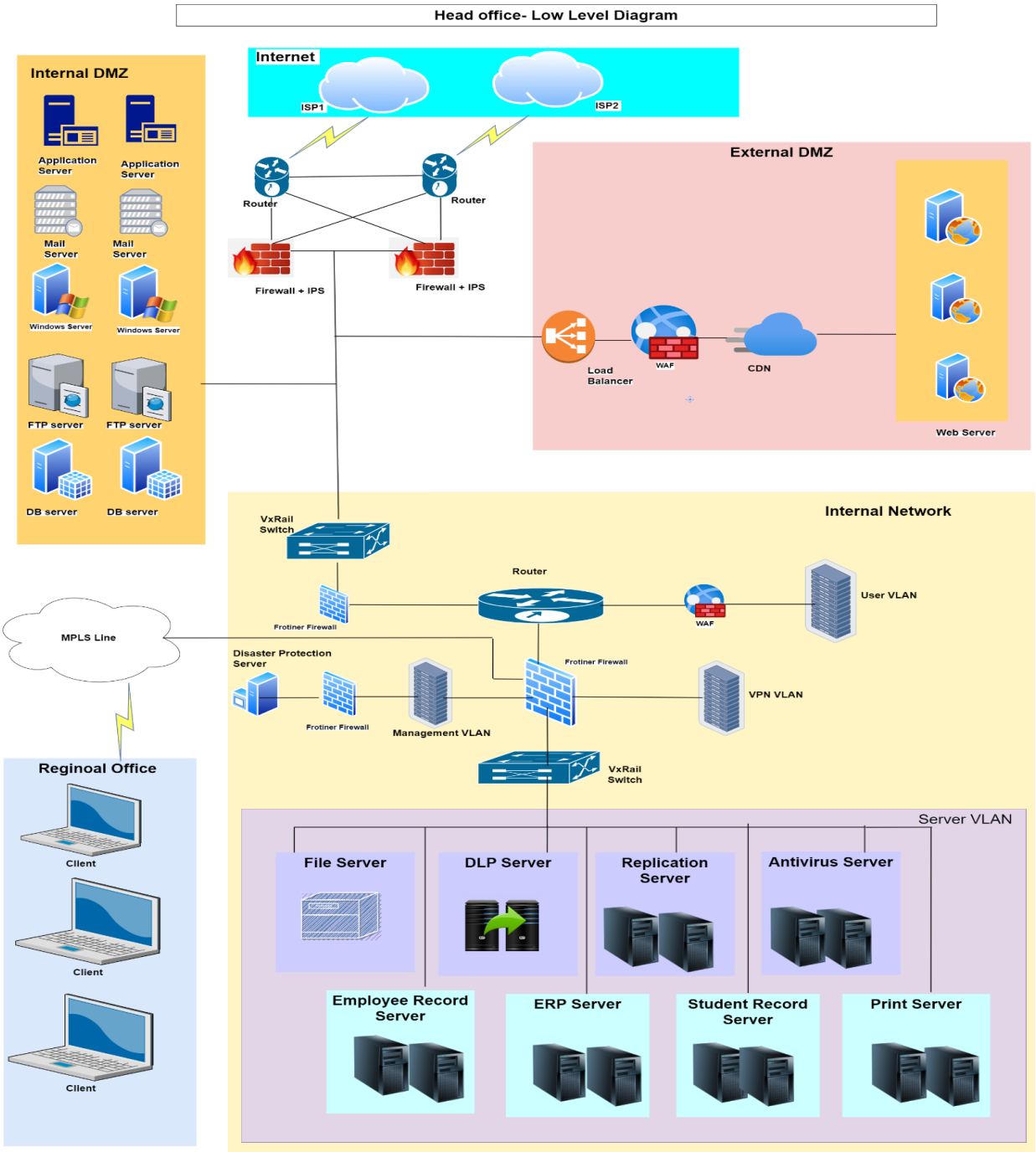


Fig 2.2: Low level diagram of Head Office

Regional Office

Regional Office is spread across locations and provides access to employees across offices to access student records and process applications and other student related information. The network has a perimeter firewall and a router which segregates server VLAN, user VLAN and payroll VLAN.

Payroll, user and server VLAN are segregated to ensure no unauthorized access takes place on the payroll data or student records. Routers use ACL to create the logical segregation.

There is an MPLS link to ensure dedicated and secure connectivity to head office and regional campus.

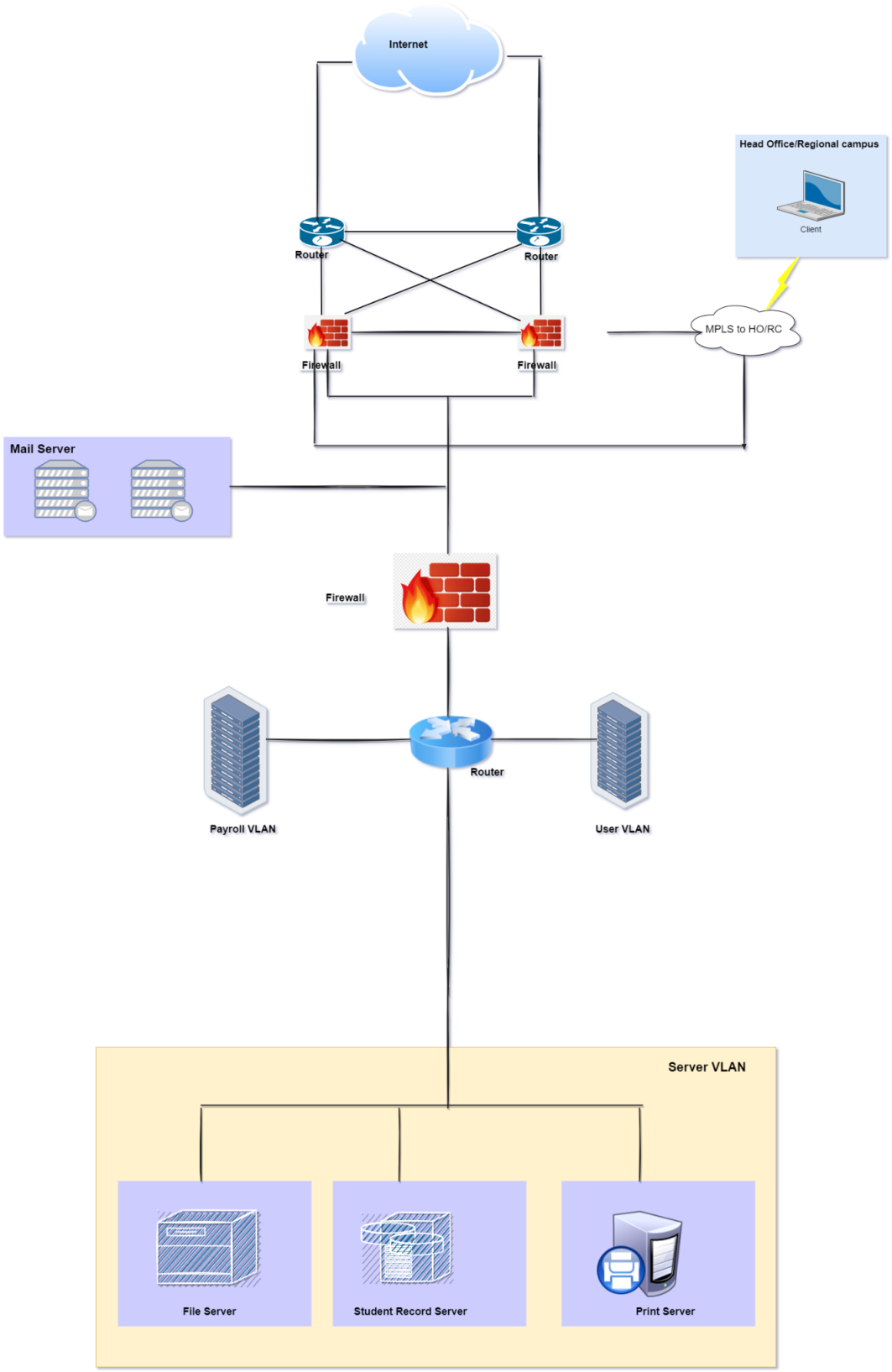


Fig 3.1: High level diagram of Regional Office

Regional Office LLD- Multiple regional offices are present across various locations. Major use case of the regional office is to access the student records and process applications. The system is supported by two ISP providers (Airtel and Jio) which work with 5GHz and 2.4 GHz bandwidth of the internet. This ensures that there is connectivity throughout. Cisco Router is used to route traffic from ISP which is then monitored and filtered by the next gen firewall by Fortinet. Mesh topology is followed at this phase where the routers and the firewall are connected with each other.

A secure MPLS link connects the regional office with the head office. Additionally, a mail server (Google) is in place to ensure proper usage of the mail services. The Cisco branch router links the traffic to the various VLANs. One such VLAN is the User VLAN which is secured by the WAF (Site Defender). The other VLAN connected to the router is the Payroll VLAN which consists of all the financial data. The Server VLAN is the most critical VLAN which is integrated with the VxRail which consists of the File Server, Student Record Server, Replication Server for back-ups and lastly, Print Server.

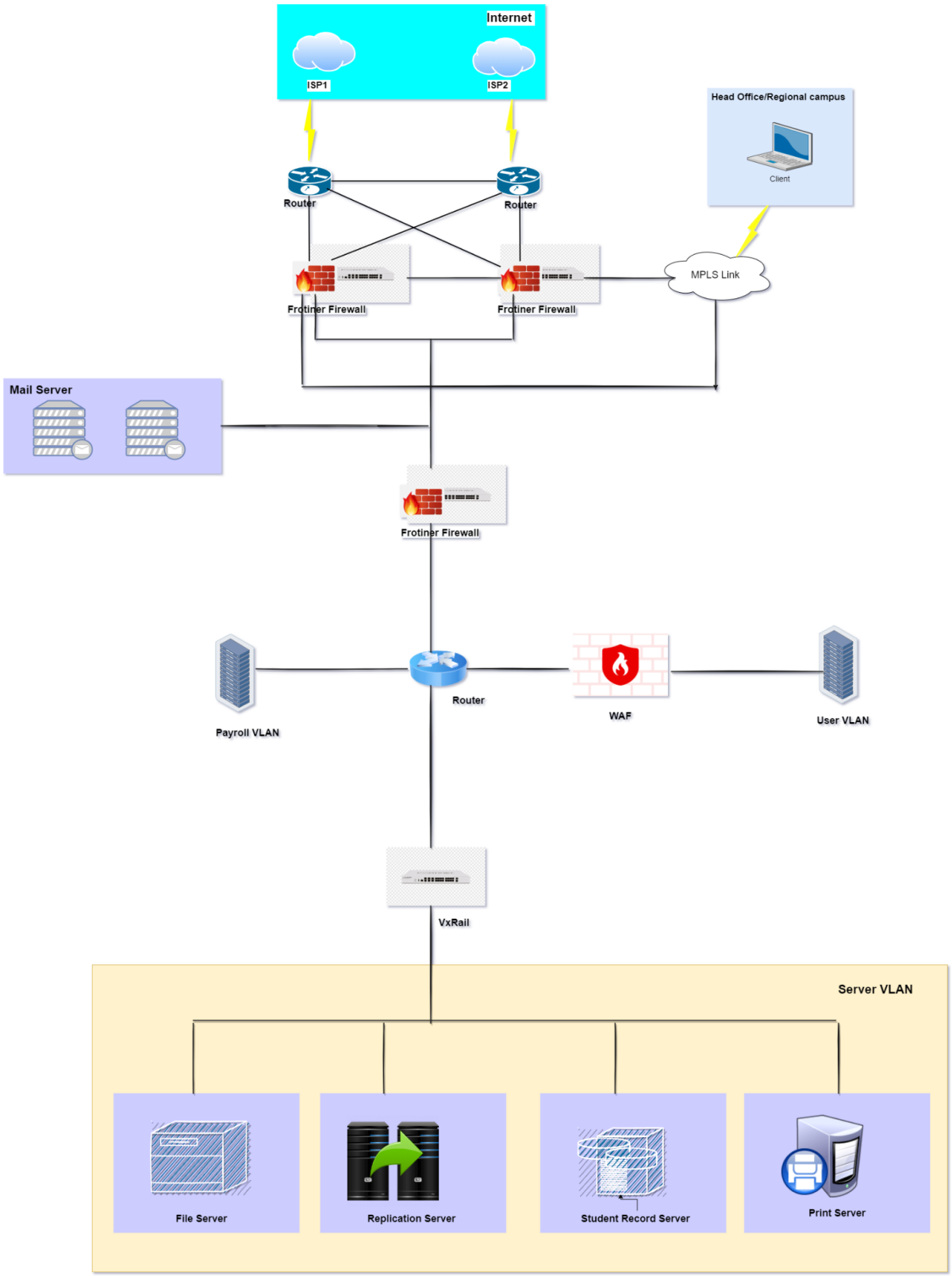


Fig 3.2: Low level diagram of Regional Office

Regional Campus

Regional campus is that part of the network where we see heavy traffic from most of the internal users. This is the region where faculties access networks to take classes and students refer to books and periodicals stored on file servers. Labs are hosted on a separate VLAN which cater to a variety of hands-on practice opportunities to the students. Servers have been placed in a separate VLAN to ensure segregation and reduce chances of unauthorized access.

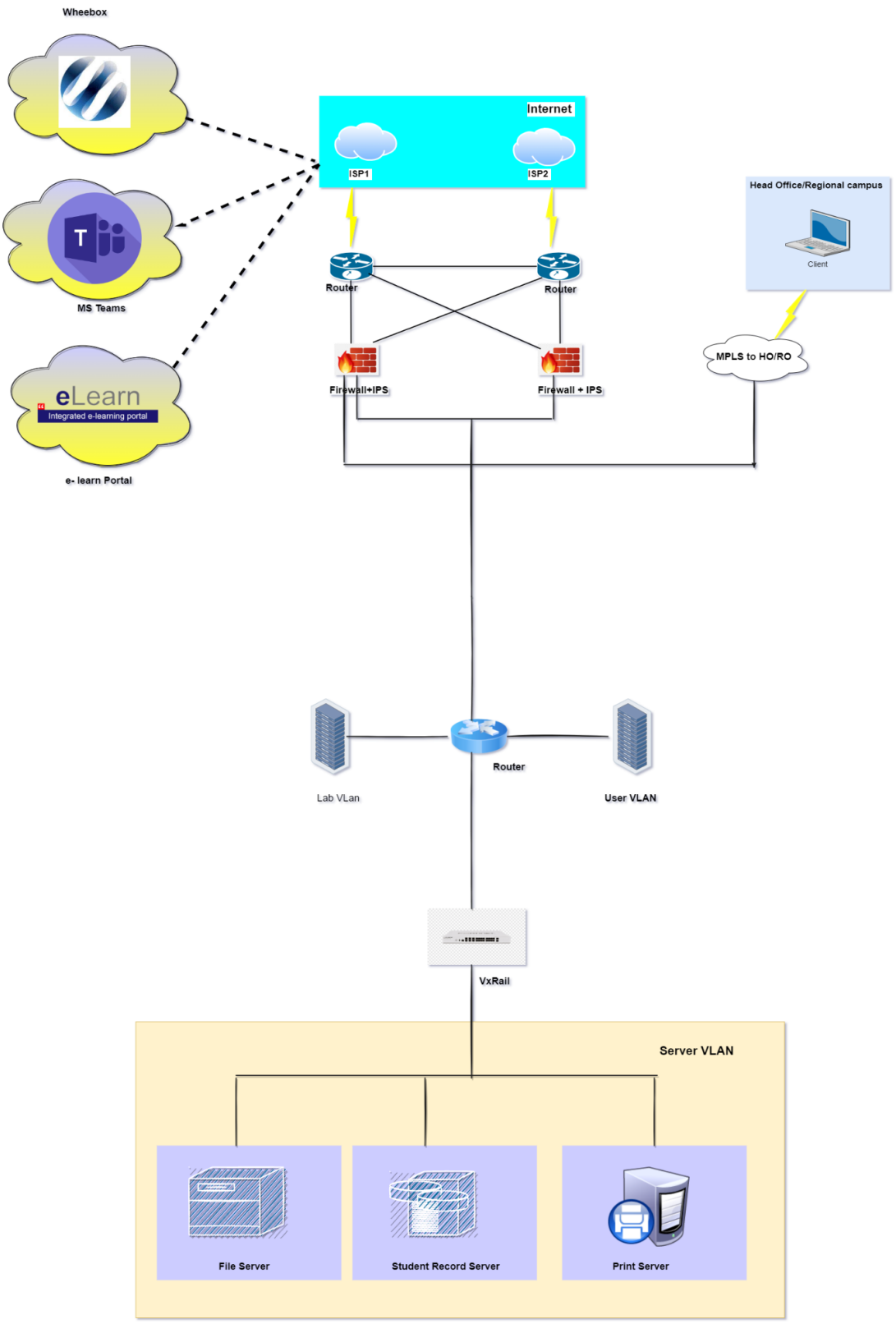


Fig 4.1: High level diagram of Regional Campus

The Low-Level Diagram for Regional Campus is more or less the same as that of the Regional Office. We can expect more traffic on the servers as WILP programs offered by BITS host online classes in MS Teams. All the Assignment e-learning modules shared by e-learn Portal. There is very little or minimal traffic from wheebox as it is only used during exam time.

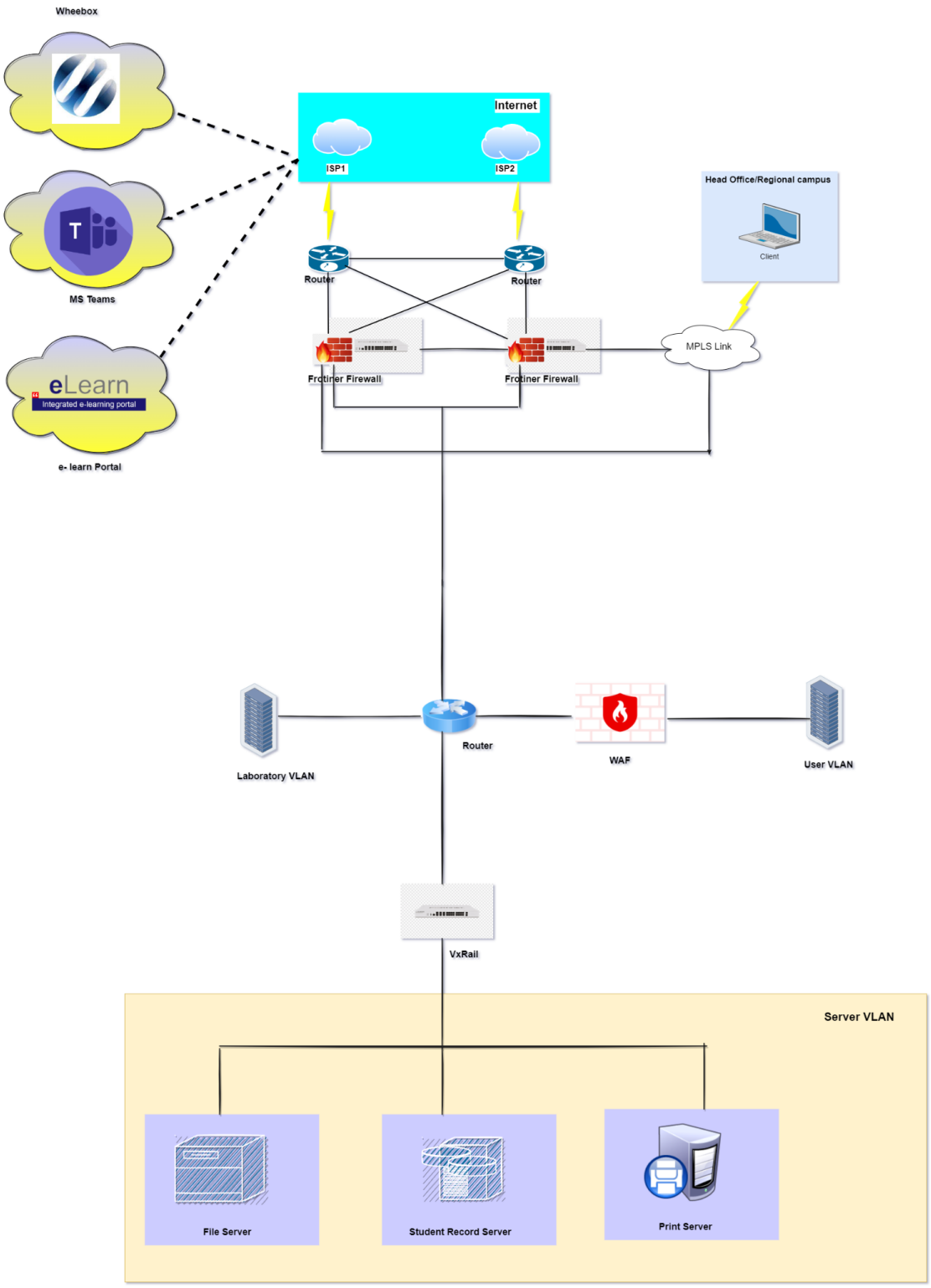
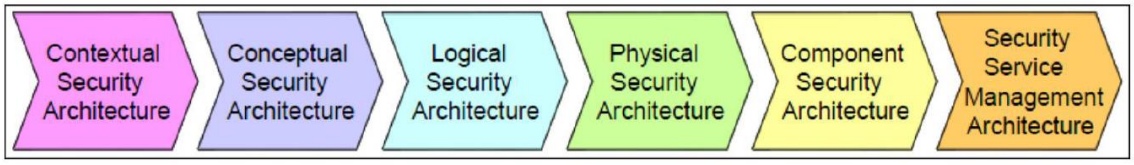


Fig 4.2: Low level diagram of Regional Campus

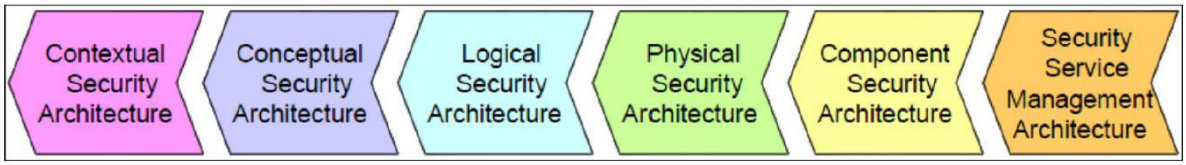
Business Processes and Business Requirements (Threat and Risk Assessment)

• State Informal Security Policies
• Apply Content Protection
• Prevent and detect cheating
• Prevent Plagiarism
• Manage User Accounts
• Authenticate Users
• Deploy PKI
• Manage Privileges – Least Privilege
• Apply RBAC
• Logging & Monitoring
• Non-Repudiation
• Identify all the risk associated with the attributes that can prevent a business from achieving its goals
• Identify the required controls to manage the risk
• Define a program to design and implement those controls

Background According to SABSA framework: - Two-way Traceability
Completeness – has every business requirement been met? The matrix allows every requirement to be traced down to the component providing the solution.



Business Justification – is every component in the architecture needed?
Every aspect of the solution can be traced back to the related business requirement/



Some of the business risk includes when a Threat and Risk Assessment is undertaken: -
• Not having a proper disaster recovery plan for applications (this is linked to the availability attribute)
• Vulnerability in applications (this is linked to the privacy and accuracy attributes)
• Lack of segregation of duties (SoD) (this is linked to the privacy attribute)
• Not Payment Card Industry Data Security Standard (PCI DSS) compliant (this is linked to the regulated attribute)
Some of the controls are:
• Build a disaster recovery environment for the applications
• Implement vulnerability management program and application firewalls
• Implement public key infrastructure (PKI) and encryption controls
• Implement SoD for the areas needed
• Implement PCI DSS controls some other example controls are:

• **Procedural controls**
o Risk management framework
o User awareness
o Security governance
o Security policies and standards

• **Operational controls**
o Asset management
o Incident management
o Vulnerability management
o Change management
o Access controls
o Event management and monitoring

Application controls
o Application security platform (web application firewall [WAF], SIEM, advanced persistent threat [APT] security)
o Data security platform (encryption, email, database activity monitoring [DAM], data loss prevention [DLP])
o Access management (identity management [IDM], single sign-on [SSO])

• **Endpoint controls**
o Host security (AV, host intrusion prevention system [HIPS], patch management, configuration and vulnerability management)
Mobile security (bring your own device [BYOD], mobile device management [MDM], network access control [NAC])

o Authentication (authentication, authorization, and accounting [AAA], two factor, privileged identity management [PIM])

• **Infrastructure controls**
o Distributed denial of service (DDoS), firewall, intrusion prevention system (IPS), VPN, web, email, wireless, DLP, etc.

Expected Results
We expect our proposed solution to provide the following ROI and benefit results:

Financial Benefits
• Reduced Overheads on Insurance Premiums related to Information Security Risk
• Penalty and fine avoidance in relation to security compliance standards for Financial Industry
• Reduced risk of Brand reputation post implementation based on increased and elevated security posture
• Future Asset Loss Prevention – Elevated security strategy and posture should reduce risk profile post implementation

Functional Benefits
• Formalized and Documented set of Strategic Plans to map to lower layers of the SABSA Architecture Model
• Roadmaps for daily operatives to map strategic intention to tactical and day-to-day activities
• Documented Policies and Procedures that tie directly to business drivers established at Board and Executive Level

Risk Assessments:
Risk is uncertain events associated with future events which have a probability of occurrence but it may or may not occur and if occurs it brings loss to the project. Risk identification and management are very important tasks during software project development because success and failure of any software project depends on it.

Task	Hazard	Risk	Priority	Control
Hardware	Data storage disk crashes	Data will not available, Data loss	High	Data backed up and stored in a secure off-site location (may be in multiple location)
	Network adapter failure	Connection will be lost; Student will face lots of challenges during exam	Medium	There should be backup route to send network traffic
	Hardware failure due to Malware & Viruses	Data loss, budget issue for new hardware	High	Outdated hardware should be upgraded and Firewall should be placed to protect Malware
	Human error caused by poor training i.e. How to keep computers free of dust and dirt, How to identify phishing emails, What to do if you suspect a system is infected, How to recognize key performance issues,	Hardware failure, Overheating issue, Slow performance, Malware & Viruses attack	Medium	Human error may be due to a lack of training so should arrange proper training session to educate them. Training like cybersecurity so that they should identify phishing emails, also can suspect a system which is infected
	Lack of performance checks and maintenance	Overheating issue, Hardware failure, Fire in data center, Slow performance	Medium	Regular maintenance is key for avoiding IT hardware failure.

	Technology overdue for a replacement	Crash, Security weaknesses, Harm productivity with slow performance, Lead to compliance issues	Medium	If we used same computers and servers for years, update aging hardware, Install virtual environments
Software	System Vulnerabilities	Data loss, System corrupted, Viruses & Malware attack	High	These are the below method, which can implement to prevent vulnerabilities. Penetration testing, user access levels, secure passwords, anti-malware software, firewalls, Software update on time basis
	Compliance Issues	Legal implications	Medium	Should use all compliance software
	Stability Problems	Data availability issue, Performance issue	Medium	Performance and endurance testing should arrange properly so that can check system stability
	Efficiency Weaknesses	Processing time increase	Medium	Integration of software and hardware should be implemented accurately to get maximum throughput
	Performance Degradation	Performance issue, Data availability issue	Low	Software performance issue sometimes came because of outdated hardware. Some upgraded software

	Security Flaws	Viruses & Malware attack, Data loss	High	Owasp scan, Penetration testing can lead to find security flaws, there are below methods to overcome this issue: Authentication and Authorization, Access Controls using RBAC, Least Privilege, Security Trainings and Policies
	Lack of software patches	Legal implications, Viruses & Malware attack, Data loss	High	Patches are part of essential preventative maintenance necessary to keep machines up-to-date, stable, and safe from malware and other threats. So, Patches should implement frequently
	Software design flaws. i.e., Firewall design/integration issue	Increase attack surface, Data loss	High	Software design should follow certain strict rules to eliminate design flaw. Rules are like: Make sure all data from an untrusted client are validated, use an authentication mechanism that can't be bypassed, authorize after you authenticate so all these managed by APIGateway. Also, there are technology

Project schedule	Time is not estimated perfectly, Improper resource allocation, Frequent project scope expansion, Failure in function identification and its' completion	Project failure	Medium	Manager/Lead should understand the project and requirement first and schedule all the hazard point accordingly
Budget Management	Wrong/Improper budget estimation, Unexpected Project Scope expansion, Mismanagement in budget handling, Improper tracking of Budget	Project failure	High	Budget related risks refers to the monetary risks mainly it occurs due to budget overruns. Always the financial aspect for the project should be managed as per decided but if financial aspect of project mismanaged then their budget concerns will arise by giving rise to budget risks. So proper finance distribution and management are required for the success of project
Operational Management	Insufficient resources, Conflict between tasks and employees, Improper management of tasks, No proper planning about project, Less number of skilled people, Lack of clarity in roles and responsibilities	Project failure	Medium	Operational risk refers to the procedural risks means these are the risks which happen in day-to-day operational activities during project development due to improper process implementation so every day status call needed here

Role Based Access Control:

Role-based access control (RBAC), also known as role-based security, is a mechanism that restricts system access. It involves setting permissions and privileges to enable access to authorized users. Tenant can be created under one user and set different permissions and policies to those tenants (can say 'role') so that student tenant has module (one subject is a module and it is a microservice) access and permissions and policies are set to only can view those modules but there is no upload, update, edit, delete access. Whereas Teacher is another tenant and has created permission and policies to update, upload, delete, view, edit access. So Based on Role-based access control we can restrict the user access

RBAC Example Impartus Application

Role	Authentication	Access/Entitlement	Default Access
Admin	Required	Admin	Admin, Read, Write, Edit, Record
Professors	Required	Professor	Read, Write, Record
Students	Required	Student	Read Only
Other Users	Not Allowed	Not A User	Access Denied

Applicable Laws and Regulation

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) aims at giving users residing in California, more control over how businesses collect and use their personal information. This is intended to enhance the user's privacy rights which includes –

- The right to know about the personal information a business collects about them and how it is used and shared.
- The right to delete personal information collected from them (with few exceptions)
- The right to opt-out of the sale of their personal information
- The right to non-discrimination for exercising their CCPA rights

Personal information as defined by CCPA is, information that can (directly or indirectly) identify, relate, describe, reasonably associate, or reasonably link to a particular consumer or household, such as personal IDs, online IDs, Internet Protocol addresses, email address, account name, social security number, driver's license number, license number, passport number geo-location data, biometrics, purchase history, or another similar identifier.

Information which is publicly available from federal, state, or local government records, such as professional licenses and public real estate/property records are not considered as personal information which in turn is not covered under CCPA.

The CCPA requires business privacy policies to include information on consumer's privacy rights and how to exercise them (the right to know, the right to delete, the right to opt-out & the right to non-discrimination)

As the Work-Integrated Learning Program (WILP) by BITS Pilani offers its courses to all students without any location barrier, the CCPA will be applied for students and staff who are residing in California.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) primarily aims to enhance an individual's control and rights over their personal data and simplify the regulatory environment for international business. The GDPR is a regulation in the European Union (EU) Law on data protection and privacy in the EU and the European Economic Area (EEA) which also addresses the transfer of personal data outside the EU and EEA. As the GDPR is a

regulation, not a directive, it is directly binding and applicable, and provides flexibility for certain aspects of the regulation to be adjusted by individual member states.

The GDPR provides various rights to the data subject, such as – transparency, right of access, right to be forgotten for rectification and erasure of data, right to object and automate decisions.

Key differences between CCPA and GDPR include the scope and territorial reach of each, definitions related to protected information, levels of specificity, and an opt-out right for sales of personal information. CCPA differs in definition of personal information from GDPR as in some cases the CCPA only considers data that was provided by a consumer. The GDPR does not make that distinction and covers all personal data regardless of source. In the event of sensitive personal information, this does not apply if the information was manifestly made public by the data subject themselves, following the exception under Art.9(2, e). As such, the definition in GDPR is much broader than defined in the CCPA.

GDPR will be applied to any student or faculty residing in any country which is under the EU. An organization's physical location doesn't exempt it from GDPR applicability.

International standard for information security (ISO/IEC 27001)

ISO/IEC 27001 is an international standard which defines how information security can be managed which was originally published jointly by the International Organization of Standardization (ISO) & International Electrotechnical Commission (IEC). It mostly focuses on requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – aiming to help organizations make the information assets they hold more secure.

ISO/IEC 27001 requires that management

- Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and their impacts
- Designs and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle payment cards from the major card schemes. PCI compliance is mandated by most credit card companies to help ensure the security of the transactions in the payment industry. This mainly focuses on increasing the controls around the cardholder data to reduce credit card fraud by creating an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data.

As students enrolling in WILP are given the opportunity to pay their fees via credit card, it is mandatory for BITS to be PCI DSS compliant, even if it is not handling the collection, processing, and storage of the protected cardholder data directly.