BITS - WILP

Assignment – Cloud, IoT and Enterprise Security (SSZG570)

GROUP MEMBERS

Harsh Tak(2020MT13202)
Dibyendu Senapati (2021MT12324)
Suneeja (2020MT13154)
Shreyas Sharma (2021MT12201)

ABOUT

This report presents high level and detailed Security Architecture of BITS business processes including risk assessments and cost estimations.

Contents

Assignment Statement

Task:

Provide a security architectural design for the Work Integrated Learning Program (WILP), a division of BITS Pilani, whose brief it is to provide the highest quality education experience to industry professionals. WILP is currently implementing new IT systems, something that also requires a complete overhaul of their IT security. This latter task is your responsibility. WILP is worried about several security issues:

1. Compliance with various security policies and privacy legislations
2. Cybersecurity - attacks from external sources, as well as from internal sources (rogue students)
3. Confidentiality of student records
4. Protection of WILP computer systems from inadvertent damage

WILP, BITS Pilani has IT systems in all of their offices:

Head office 1 - central administration of staff and students, central office systems

Regional offices 3 - student records, regional office systems, payroll

Regional campuses 7 - IT teaching laboratories, staff workstations, local office systems (file servers, printers)

Components to deliver (Deliverables):

1. High-level security architecture. You can use any reference architectures that you can find. The purpose of this work product is to show what **types** of security services you intend to provide, what **types** of networks and servers are required, for each **type** of location (head office, regional office, regional campus).

   You will need to make reasonable assumptions about sizing, capacity, etc. of the various IT systems, and you need to provide a design for best security practice, i.e. cost is less of an issue than having security exposures and weaknesses.

2. Detailed security architecture for each **type** of office (HO, RO, RC). This will include specific details of what security services you will provide at office type, what networking you will provide, what application systems you will be protecting, what tools you will be using.
3. Detailed design for HO, 1 RO, 1 Campus. This will include security equipment, networking devices, storage systems, management tools, operational components for the detailed security architecture.
4. Costing estimates (hardware and software, both for implementation and operation)

Pre-cursor (Deliverable) work products:

Apart from the set of work products listed above, you may need to produce, before the final deliverables, the following additional work products:

1. **Business requirements and risk assessments** on which you will base your designs.
2. **Use cases and/or Business Processes** - to describe interactions between WILP users, systems and subsystems.

Approach:

Use any well-known security framework as a guide for your work products (including the data-centric approach discussed in class). Concentrate on the How, Who and Where (Process, People and Location) aspects. You will need to describe the existing WILP IT systems for which you will need to provide security services based on your security architecture. That means you have to do some research about how an organisation like WILP would be running its IT systems and what they would consist of. Use any tools or security appliances available in the market, as COTS or base solutions that can be extended.

Submission:

Due date: 10-April-2022, 11:55 pm

Format: report, suggested length 25-30 pages (incl. diagrams and tables), in a standard report format, submitted in electronic form as PDF document

Assessment/ Marking:

This assignment is worth 20% of the total course marks, and will be marked out of 20.

Marks will be awarded for:

1. Report format and style - 2
2. Thoroughness and reasonableness of your assumptions - 2
3. Application of use cases to your assumptions - 2
4. Linking of business requirements to your solution - 2
5. Consistency between high-level architecture, detailed architectures and detailed designs - 2
6. The relevance of your architectures and designs to business requirements and use cases - 3
7. Delivery of all required work products and completeness of your solution - 4

Proof of application of security best practice in your solution -3

BITS WILP Security Architecture

Pre-requisites:

- The Business (What)
- The Business Risk Model (Why)
- The Business Process Model (How)
- The People (Who)
- The Location(s) (Where)
- The Business Time Dependencies

SABSA Model Overview

The SABSA model consists of 6 layers – Identified and categorized in the table below:

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Facilities Manager's View	Operational Security Architecture

In order to bring context to the model, SABSA uses the same 6 questions across each of the 6 layers. Those questions are:

1. What are you trying to do at this layer?
2. Why are you doing it?
3. How are you doing it?
4. Who is involved?
5. Where are you doing it?
6. When are you doing it?

The table below illustrates this matrix as it is applied:

The SABSA matrix

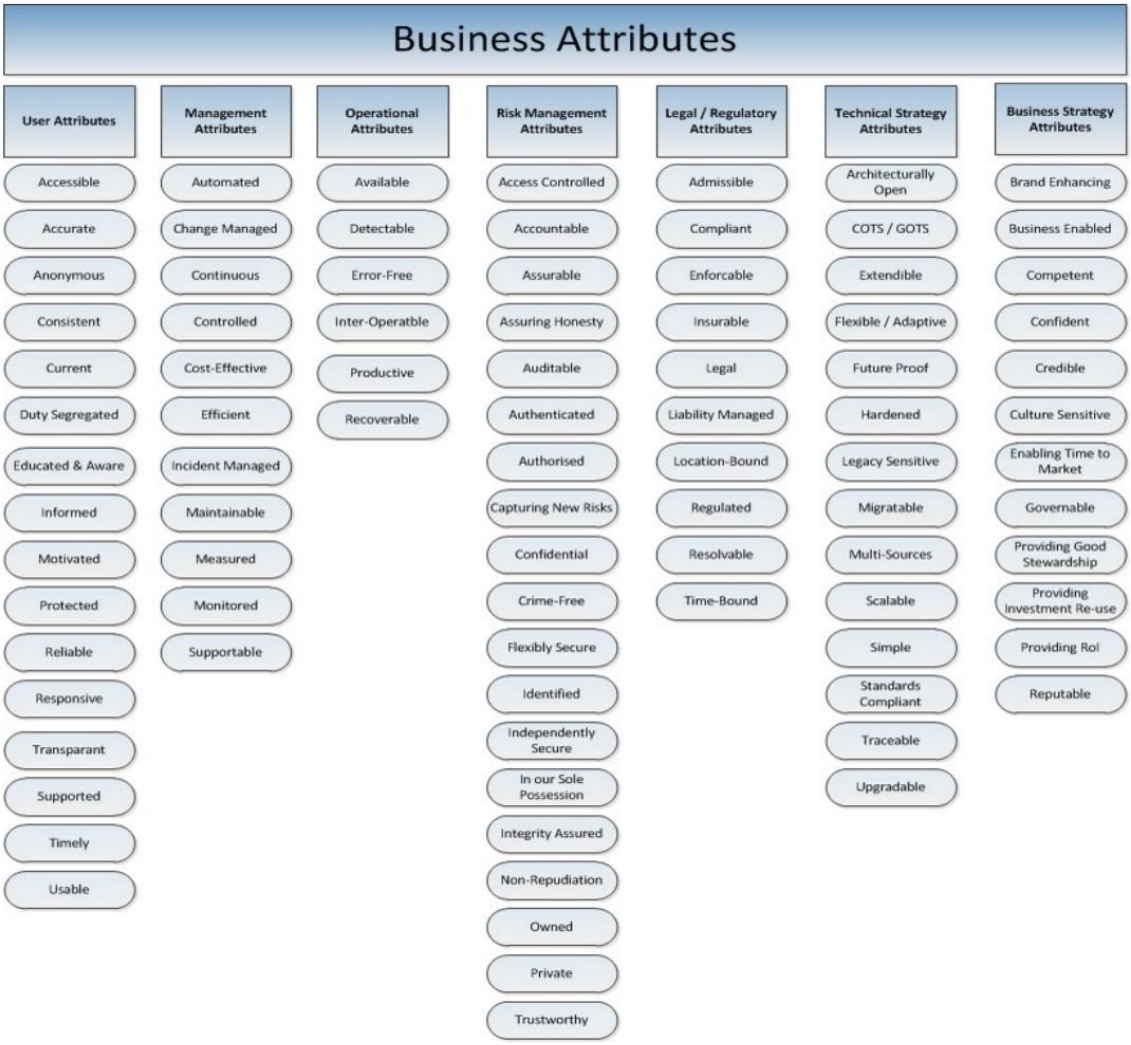
SABSA	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetime and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites and Platforms	Security Operations Schedule

Focus for this Proposal – The Conceptual Layer (Security Strategy)

From the highest levels working downstream in a multi layered model we will look at, address and document the following as outputs the organization:

Multi-Layered Security Framework:

- Tier 1 Top Level – Policy, Organization & Responsibilities
- Tier 2 – Procedures & Practices; Security Management; Training & Awareness; Personnel Security; Document Security; Security Audit and Business Continuity Planning
- Tier 3 – Physical Security
- Tier 4 – Hardware Security
- Tier 5 – System Software Security
- Tier 6 – Application Software Security
- Tier 7 – Cryptography & Encryption Security
- Tier 8 – Information Asset


Business Attributes
User Attributes
Accessible
Accurate
Anonymous
Consistent
Current
Duty Segregated
Educated & Aware
Informed
Motivated
Protected
Reliable
Responsive
Transparant
Supported
Timely
Usable
Management Attributes
Automated
Change Managed
Continuous
Controlled
Cost-Effective
Efficient
Incident Managed
Maintainable
Measured
Monitored
Supportable
Operational Attributes
Available
Detectable
Error-Free
Inter-Operatble
Productive
Recoverable
Risk Management Attributes
Access Controlled
Accountable
Assurable
Assuring Honesty
Auditable
Authenticated
Authorised
Capturing New Risks
Confidential
Crime-Free
Flexibly Secure
Identified
Independently Secure
In our Sole Possession
Integrity Assured
Non-Repudiation
Owned
Private
Trustworthy
Legal / Regulatory Attributes
Admissible
Compliant
Enforcable
Insurable
Legal
Liability Managed
Location-Bound
Regulated
Resolvable
Time-Bound
Technical Strategy Attributes
Architecturally Open
COTS / GOTS
Extendible
Flexible / Adaptive
Future Proof
Hardened
Legacy Sensitive
Migratable
Multi-Sources
Scalable
Simple
Standards Compliant
Traceable
Upgradable
Business Strategy Attributes
Brand Enhancing
Business Enabled
Competent
Confident
Credible
Culture Sensitive
Enabling Time to Market
Governable
Providing Good Stewardship
Providing Investment Re-use
Providing RoI
Reputable

SABSA Framework Matrix

The high-level architecture has been developed using the SABSA framework: -

SABSA Framework	**ASSETS** (What)	**MOTIVATION** (Why)	**PROCESS** (How)	**PEOPLE** (Who)	**LOCATION** (Where)	**TIME** (When)
CONTEXTUAL ARCHITECTURE	Business Decisions Taxonomy of Business Assets, including Goals & Objectives Contextual Assets Model	Business Risk Opportunities & Threats Inventory Contextual Motivation Model	Business Processes Inventory of Operational Processes Contextual Process Model	Business Governance Organizational Structure & Extended Enterprise Contextual People Model	Business Geography Inventory of Buildings, Sites, Territories, Jurisdictions, etc. Contextual Location Model	Business Time Dependence Time dependencies of business objectives Contextual Time Model
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy Business Attributes Profile Conceptual Assets Model	Risk Management Objectives Enablement & Control Objectives; Policy Architecture Conceptual Motivation Model	Strategies for Process Assurance Process Mapping Framework; Architectural Strategies for ICT Conceptual Process Model	Roles & Responsibilities Owners, Custodians and Users; Service Providers & Customers Conceptual People Model	Domain Framework Security Domain Concepts & Framework Conceptual Location Model	Time Management Framework Through-Life Risk Management Framework Conceptual Time Model
LOGICAL ARCHITECTURE	Information Assets Inventory of Information Assets Logical Assets Model	Risk Management Policies Domain Policies Logical Motivation Model	Process Maps and Services Information Flows; Functional Transformations; Service Oriented Architecture Logical Process Model	Entity & Trust Framework Entity Schema; Trust Models; Privilege Profiles Logical People Model	Domain Maps Domain Definitions; Inter-domain associations & interactions Logical Location Model	Calendar & Timetable Start Times, Lifetimes & Deadlines Logical Time Model
PHYSICAL ARCHITECTURE	Data Assets Data Dictionary & Data Inventory Physical Assets Model	Risk Management Practices Risk Management Rules & Procedures Physical Motivation Model	Process Mechanisms Applications; Middleware; Systems; Security Mechanisms Physical Process Model	Human Interface User Interface to ICT Systems; Access Control Systems Physical People Model	ICT Infrastructure Host Platforms, Layout & Networks Physical Location Model	Processing Schedule Timing & Sequencing of Processes and Sessions Physical Time Model
COMPONENT ARCHITECTURE	ICT Components ICT Products, including Data Repositories and Processors Component Assets Model	Risk Management Tools & Standards Risk Analysis Tools; Risk Registers; Risk Monitoring & Reporting Tools Component Motivation Model	Process Tools & Standards Tools and Protocols for Process Delivery Component Process Model	Personnel Management Tools & Standards Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists Component People Model	Locator Tools & Standards Nodes, Addresses and other Locators Component Location Model	Step Timing & Sequencing Tools Time Schedules; Clocks, Timers & Interrupts Component Time Model
SERVICE MANAGEMENT	Service Delivery Management Assurance of Operational Continuity & Excellence	Operational Risk Management Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Process Delivery Management Management & Support of Systems, Applications & Services	Personnel Management Account Provisioning; User Support Management	Management of Environment Management of Buildings, Sites, Platforms & Networks	Time & Performance Management Management of Calendar and Timetable

A top-down approach is taken —start by looking at the business goals, objectives and vision.

The initial steps of a simplified Agile approach to initiate an enterprise security architecture program are:

- Identify business objectives, goals and strategy
- Identify business attributes that are required to achieve those goals
- 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:
    - Define conceptual architecture for business risk:
        - Governance, policy and domain architecture
        - Operational risk management architecture
        - Information architecture
        - Certificate management architecture
        - Access control architecture

        - Incident response architecture
        - Application security architecture
        - Web services architecture
        - Communication security architecture
    - Define physical architecture and map with conceptual architecture:
        - Platform security
        - Hardware security
        - Network security
        - Operating system security
        - File security
        - Database security, practices and procedures
    - Define component architecture and map with physical architecture:
        - Security standards (e.g., US National Institute of Standards and Technology [NIST], ISO)
        - Security products and tools (e.g., antivirus [AV], virtual private network [VPN], firewall, wireless security, vulnerability scanner)
        - Web services security (e.g., HTTP/HTTPS protocol, application program interface [API], web application firewall [WAF])
    - Define operational architecture:
        - Implementation guides
        - Administrations
        - Configuration/patch management
        - Monitoring
        - Logging
        - Pen testing
        - Access management
        - Change management
        - Forensics, etc.

BITS WILP - Security Goals

Security Goals
1. Compliance with various security policies and privacy legislation.
2. Cybersecurity - attacks from external sources, as well as from internal sources (rogue students)
3. Confidentiality, integrity and availability of information assets. (eg:- student records)
4. Protection of WILP computer systems from inadvertent damage.
5. Align with educational objectives, goals and strategy.
6. Consistent Risk Management approach
7. Meet minimum mandatory baseline security controls
8. Obtain security assurances from system owner/ data custodian
9. Apply classification and encryption rules for the data.

BITS WILP - Identification of Assets

WILP Assets	Asset Types
Users	Admin Staff Professors Students
Systems and Software Applications	BITS-WILP Admission Portal E-learning Portal – Impartus Course Management – Taxilla Examination Portal – Wheebox Communication Tools – Gmail
Data	Student Records, Professor Records Course Content Lecture Recordings Examination Data (Questions Papers, Answer Images) Public Data (Websites, Recorded Videos, etc)
Network	WILP Global Network, Head Office Network Regional Office Network Campus Network
Physical Assets	Application Servers Database Servers Networking Equipment's Office Systems Students BYOD Devices Lab Systems Professors Laptops Mobile Phones etc.

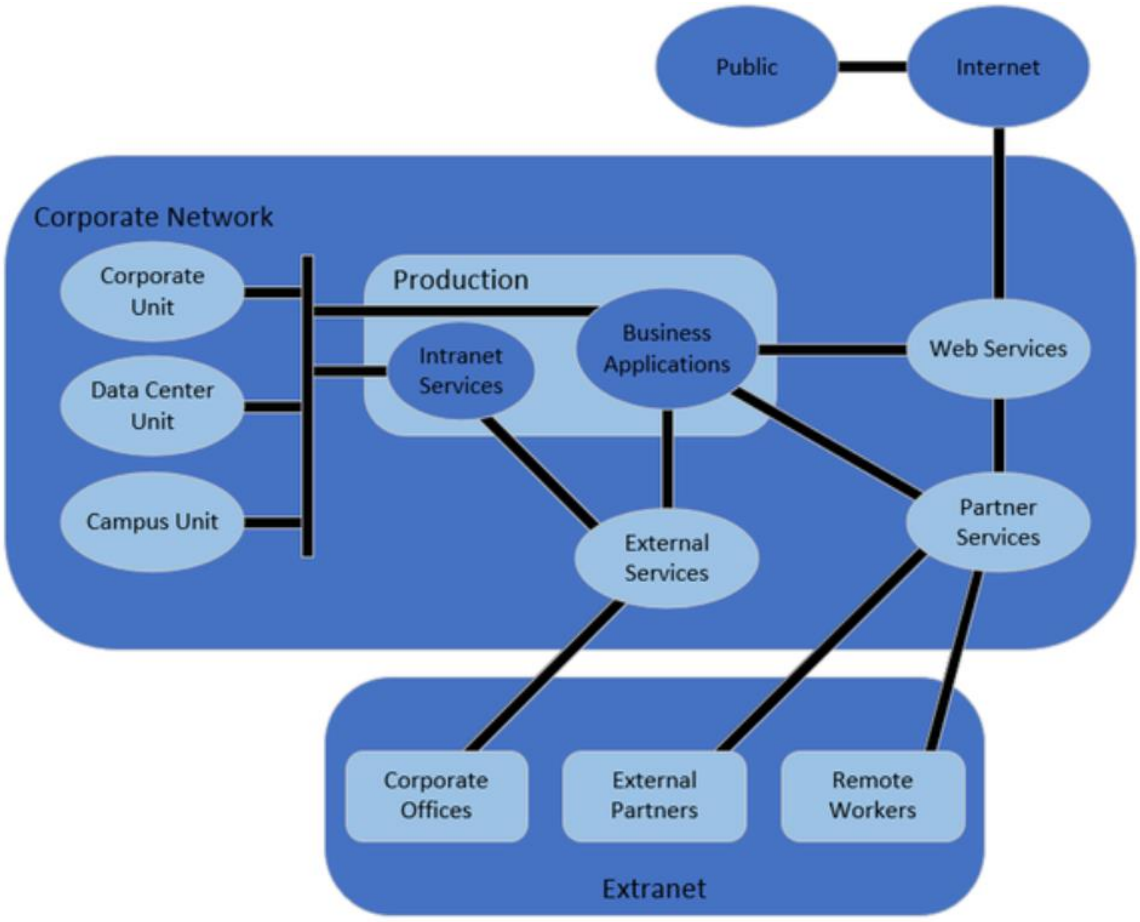
Controls required to protect Assets

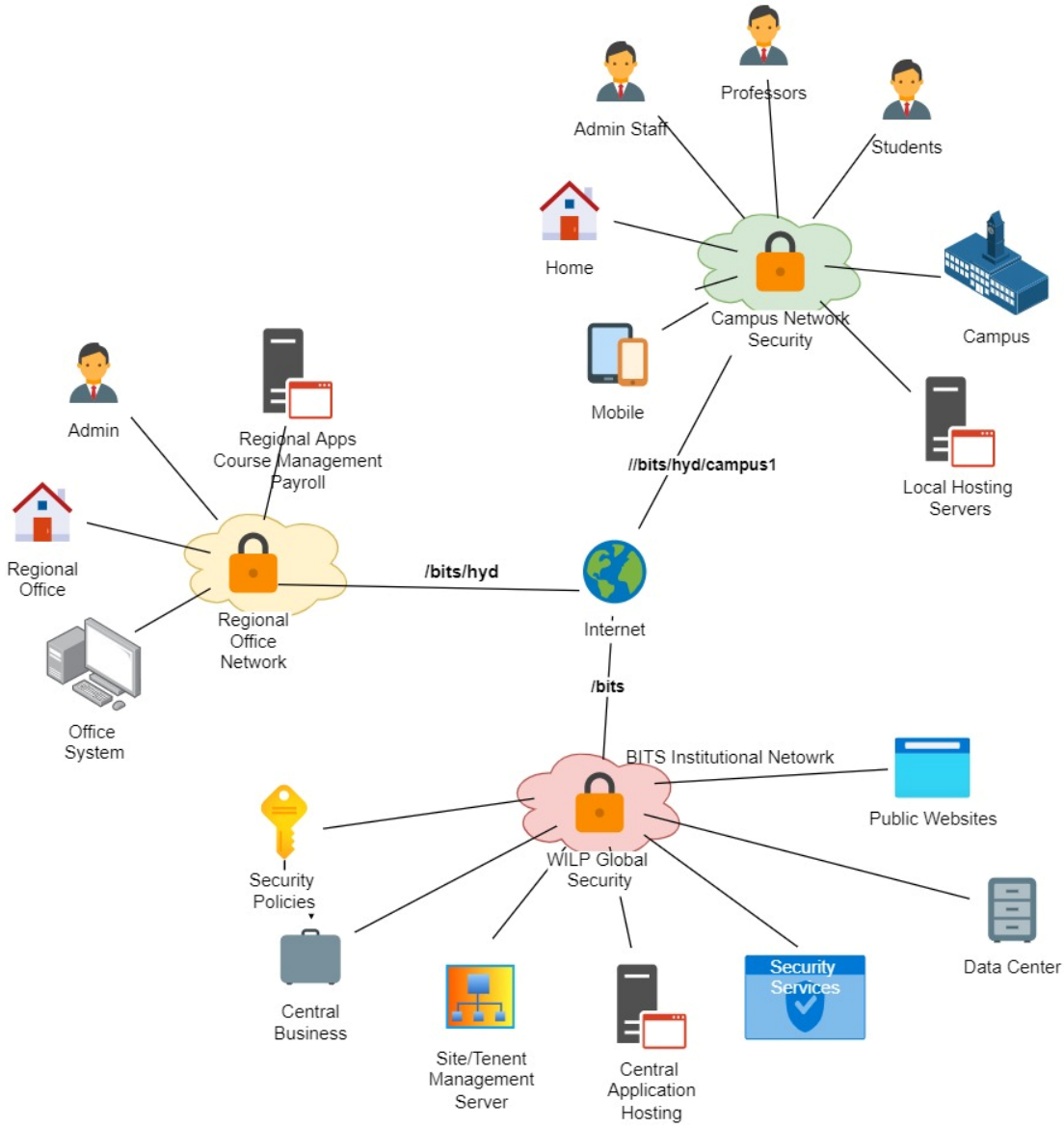
Asset	Security Controls
Users Security Controls	Authentication and Authorization Access Controls using RBAC Least Privilege Security Trainings and Policies Code of conduct policies
Software and Web Applications Security	Authentication Least Privilege Secure Communication Protocols (HTTPS, TLS) Access Management Non-Repudiation Logging & Monitoring Session Management Web application Firewall (WAF)
Data Security Controls	Data encryption at rest, in transit and in use. Password Vaults Data Backups Data Integrity Measures Data access controls PII data monitoring DLP Systems Certifications and Compliance from regulatory bodies. (If applicable) Data protection policy Data usage policy
Network Security Controls	Ddos NGFW/Firewalls DMZ (Defense in depth) Traffic Monitoring Tools IDS/IPS VPN API Gateways Secure Communication Protocols Private Cloud Hosting's
Physical Assets Controls	Authentication Antivirus Installation Security Patch Management BYOD Policy Application Whitelisting Internet Usage Policy Disk Encryption
Incident Response	Forensics Tool

	Digital Services Unit , eg:- ServiceNow Logging and monitoring Security event monitoring management (SIEM, eg:- QRADAR) Vulnerability scanning tool Eg:- nmap, tenable, Rapid 7 Penetration test – internal and external

High Level Security Architecture

Utilizing SABSA framework, we then assess the data from the previous layer, conceptual, and transpose that data into a logical network architecture diagram.

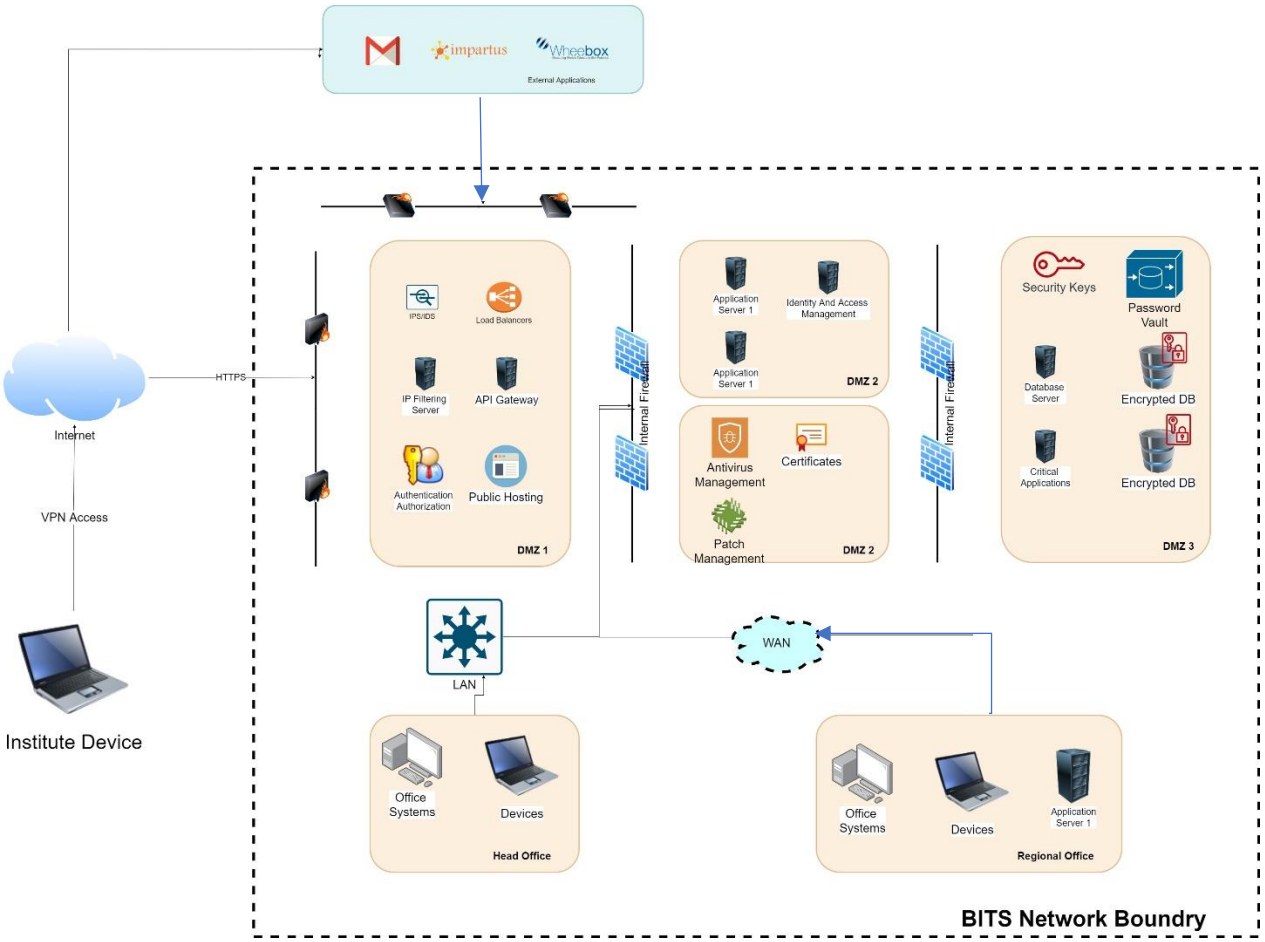




High Level Security and Network Diagram for BITS WILP

Head Office	Regional Office	Campus
WILP Global Security Network	Regional Office Network	Campus Internal Network
Central Business Process	Regional Office Building	Campus Public Wifi
Security Policies	Administrative Staff	Student Attendance System
Site/Tenant Management	Regional Application Hosting	Campus Building
Central Application Hosting	Course Management Tools	Admin Staff
Security Services	Payroll Management Tools	Professors
Data Center	Office Systems	Students
Public Website Hosting		Visitors
Office Systems		Local Websites
Higher Management Data		Labs and Workshops
Research Centers		Campus Systems
		BYOD Devices

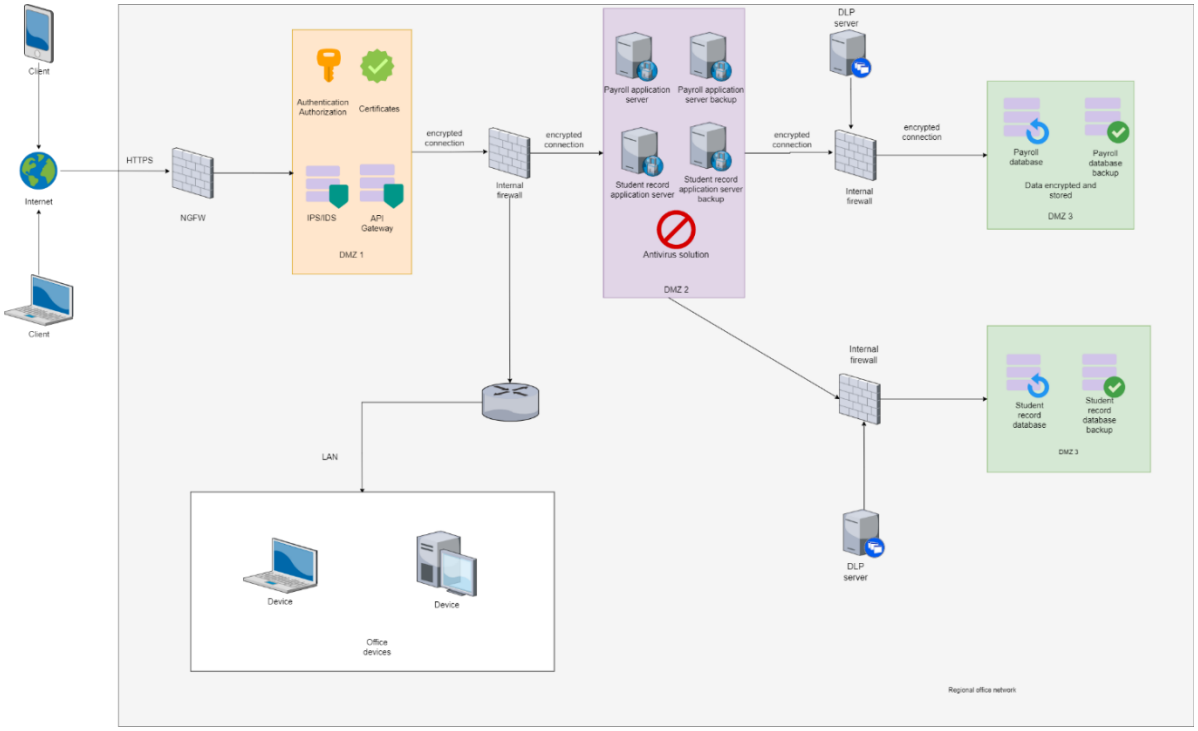
Security Architecture – Head Office



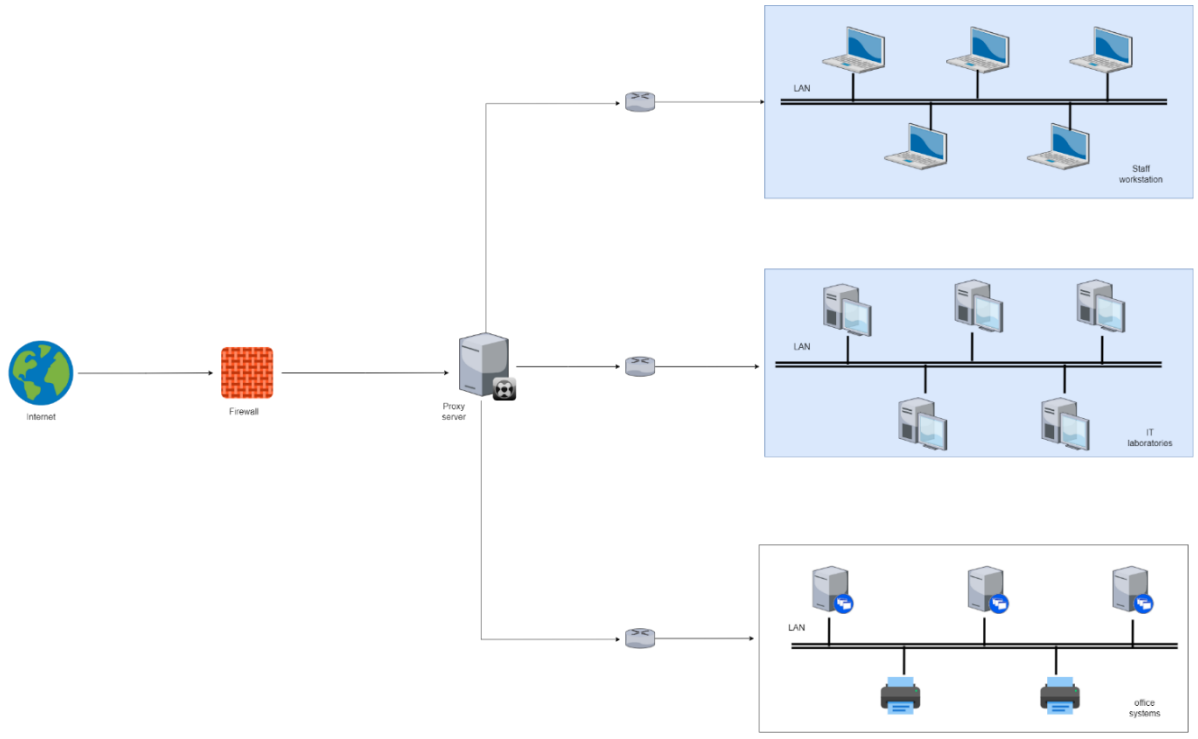
Defense In Depth Architecture

DMZ1	DMZ2	DMZ3
External Network Facing Applications	Internal Applications	Internal Data Applications
External Firewall/NGFW	Internal Firewall	Internal Firewall
IDS/IPS	Research Applications	Database Servers
Load Balancers	Identity and Access Management	Security Keys
IP Filtering	Antivirus and Patch Managment	Password Vaults
Incoming API Gateway	Public Certificates	Encrypted Database
Authentication and Authorization services	Security Policies	Least Access
Public Hosting Servers	External Application Inhouse Hosting's	Critical Applications
External Application Access		All Data Records
		Research Data

Security Architecture – Regional Office



Security Architecture – Regional Campus



Cost Estimations

Head office:

Device	Cost per unit	Units	Total cost
Firewall	$5000	3	$15000
IPS/IDS	$8000	1	$8000
Load balancer	$4000	1	$4000
IP filtering server	$5000	1	$5000
IAM server	$20000	1	$20000
Antivirus	$50/device	1	$50
Password vault	$5000	1	$5000
Database servers	$5000	3	$15000

Regional office:

Device	Cost per unit	Units	Total cost
NGFW	$30000	1	$30000
Firewall	$5000	2	$10000
IPS/IDS	$8000	1	$8000
Antivirus	$50/device	1	$50/device
DLP server	$5000	2	$5000
Database servers	$5000	4	$20000

Regional campus:

Device	Cost per unit	Units	Total cost
Firewall	$5000	1	$5000
Proxy server	$6000	1	$6000

Business Processes and Business Requirements (Threat and Risk Assessment)

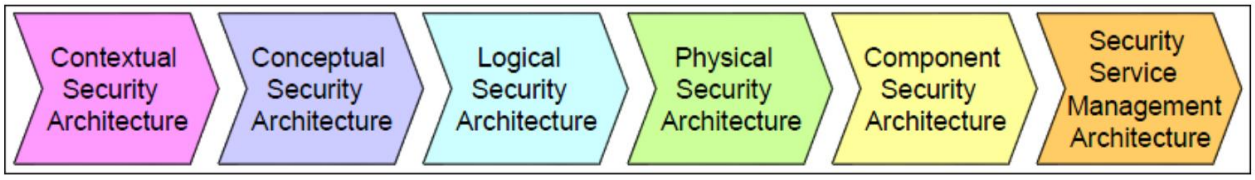
- State Informal Security Policies
- Apply Content Protection
- Prevent and detect cheating
- Prevent Plagiarism
- Manage User Accounts
- Authenticate Users
- Deploy PKI
- Manage Privileges – Least Privilege
- Apply RBAC
- Logging & Monitoring
- Non-Repudiation
- Identify all the risk associated with 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: -

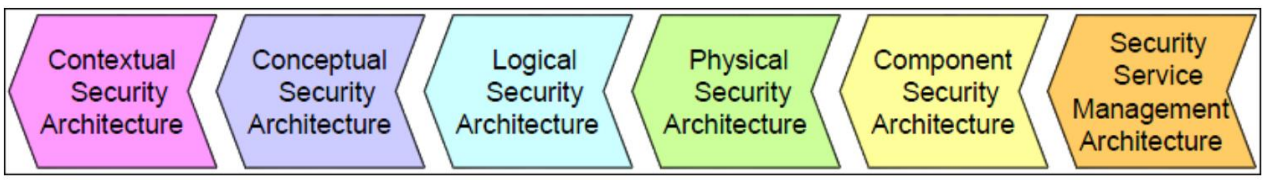
Two-way Traceability

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/s.



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**
    - Risk management framework
    - User awareness
    - Security governance
    - Security policies and standards
- **Operational controls**
    - Asset management
    - Incident management
    - Vulnerability management
    - Change management
    - Access controls
    - Event management and monitoring
- **Application controls**
    - Application security platform (web application firewall [WAF], SIEM, advanced persistent threat [APT] security)
    - Data security platform (encryption, email, database activity monitoring [DAM], data loss prevention [DLP])
    - Access management (identity management [IDM], single sign-on [SSO])
- **Endpoint controls**
    - 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])
    - Authentication (authentication, authorization, and accounting [AAA], two factor, privileged identity management [PIM])
- **Infrastructure controls**
    - 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 task 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 used more core and memory to provide better performance

	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 like VPN, secure communication protocol which are used to protect the product

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
Technical Function	Frequent changes in requirement, Less use of future technologies, Less number of skilled employees, High complexity in implementation, Improper integration of modules	It associated with functionality of product or performance part of the product	High	To overcome technical risk, Architect should design good roadmap, product layout and function, requirement specification as per market trend

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 have 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

References

Enterprise Security Architecture | ISACA Journal
Modeling a SABSA based Security Architecture using Enterprise Architect (enterprisemodelingsolutions.com)