Project Part 1:

Enterprise Architecture Analysis

Justin Langevin

8648380

Conestoga College

SECU74020:

Secure Enterprise Architecture

July 28, 2024

Description of XYZ Corporation

XYZ Corporation is a global leader in the pharmaceutical industry, it manufactures and markets a wide range of healthcare products. This company has a workforce of over 20,000 employees and a presence in over 50 countries, XYZ Corporation is renowned for its commitment to improving patient health and well-being with its innovations in medicines.

Industry: Pharmaceutical

Employees: 20,000

Global Presence: Offices, manufacturing facilities, and R&D centers in North America, Europe, Asia, and Latin America

Annual Revenue: $10 billion

Specific Characteristics

Business Goals and IT Capabilities Alignment

XYZ Corporation's business goals are innovations in the field of drug development. The goal is to ensure high-quality manufacturing standards, maintain regulatory compliance, and expanding business around the world.

Key Business Goals

- Innovation in drug development
- High-Quality Manufacturing
- Expanding business around the world
- Regulatory Compliance

IT Capabilities

- Research and Development: Advanced computational biology and bioinformatics tools.
- Manufacturing Systems
- Global Supply Chain Management
- Regulatory Compliance Management Systems
- Data Analytics

Enterprise Architecture Framework

XYZ Corporation uses the TOGAF (The Open Group Architecture Framework) for its enterprise architecture.

Key Components of the EA Framework

- Preliminary Phase
    - Scope: Global Operation covering research and development, manufacturing, and distribution.
    - Stakeholders: Management, IT, research and development, regulatory affairs, manufacturing, supply chain management.
    - Governance: Architecture Review Board: CTO, Key IT members, research and development, Key members of the different business units. The Architecture Review Board will meet quarterly.
- Architecture Vision:
    - Vision statement: To leverage technology and data-driven insights to drive innovation and ensure quality, and expand the company's global reach.
    - Business Drivers: Regulatory changes, market competition, technological advancements, patient needs.
    - Executive Sponsorship: from the CEO and Board of Directors which ensures alignment with corporate strategy.
- Business Architecture
    - Process Models: Developed models for drug discovery, manufacturing, and distribution, drug trials.
    - Business Functions: Research and development, regulatory compliance, quality assurance, supply chain management.
    - Capabilities: advanced analytics, global logistics, and regulatory adherence.
- Information Systems Architectures
    - Data models: Manufacturing records, Clinical Trial Data, patient information
    - Data Entities: drug formulas, patient records
    - Data Governance: Chief Data Officer (CDO) leading Data Governance Council
- Application Architecture
    - Application portfolio: PharamaSuite, SAP SCM, Veeva
    - Integration points API middleware for seamless data exchange.
- Technology Architecture
    - Technology Standards: Cloud Computing(Azure), ISO/IEC 27001, Hybrid cloud storage
    - Technology models:
        - Network Architecture: Firewalls Palo Alto Networks, Routers and switches(Cisco), IDS/IPS(Fortinet FortiGate)
        - Data Centers: Distributed Data centers for load balancing and disaster recovery.
        - Endpoint Security: CrowdStrike Falcon, Windows Server Update Services (WSUS)

- Opportunities and Solutions
    - Projects Portfolio: Implementing a new MES, upgrading the Research and Development Platform, and deploying advanced analytics.
    - Prioritization: depending on which will impact the business the most.
- Migration Planning
    - Plan: specific timelines and resources that are required.
    - Risks: system downtime.
    - Mitigation Strategies data validation check and backup systems
- Implementation Governance
    - Architecture Review Board: quarterly reviews of ongoing projects
    - Compliance Assessments: Regular Audits
    - Implementation Support IT department
- Architecture Change Management
    - Change Management Process: processes for submitting, reviewing, and approving changes to architecture.
    - Monitoring Continuous monitoring of changes to ensure they align with business goals.
    - Continuous Improvement: Regular reviews and updates to architecture if required due to emerging technologies.
- Requirement Management
    - Requirement Repository: Centralized repository for all requirements.
    - Tracking Changes: Implement a system that tracks changes to the requirements.
    - Alignment: Regularly reviewed requirements to ensure they meet business objectives.

Security Controls

Key Security Controls

1. Identity and Access Management (IAM): OKTA will be implemented to control access to systems and data based on specific roles and employee responsibilities.
2. Network Security: Integrate a firewall like Palo Alto Networks, IDS/IPS Fortinet FortiGate
3. Endpoint Security: Implement CrowdStrike Falcon
4. Data Encryptions: Encrypt all data at rest and in transit using technologies like AES-256
5. Regular Audits: ensure continuous security posture improvement with regular audits and penetration tests
6. Continuous monitoring: Ensure all the logs are aggregated into an SIEM this will be Splunk.
7. Incident Response Plan: create and test the incident response plan playbook for responding to security incidents.
8. Business Continuity Plan: implement a business continuity plan that will ensure minimal downtime.

Key Stakeholders

Internal Stakeholders

- Management
- IT Department
- Research and Development
- Regulatory Affairs
- Manufacturing
- Supply Chain Management

External Stakeholders

- Regulatory Bodies
- Suppliers
- Customers
- Partners
- Investors

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

CISCO. (n.d.). *Networking, Cloud, and Cybersecurity Solutions*. Cisco. https://www.cisco.com/site/ca/en/index.html

CrowdStrike. (n.d.). *The CrowdStrike Falcon® platform*. Crowdstrike.com. https://www.crowdstrike.com/platform/

Fortinet. (2023). *Next-Generation Firewall (NGFW)*. Fortinet. https://www.fortinet.com/products/next-generation-firewall

ISO. (2023). *ISO/IEC 27001:2022(en)*. Iso.org. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

NIST. (2020). Security and privacy controls for information systems and organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

paloalto networks. (n.d.). *Global Cybersecurity Leader - Palo Alto Networks*. Www.paloaltonetworks.com. https://www.paloaltonetworks.com/

rockwell. (n.d.). *MES Solutions for Life Sciences | FactoryTalk | US*. Rockwell Automation. Retrieved July 25, 2024, from https://www.rockwellautomation.com/en-ca/products/software/factorytalk/operationsuite/mes/life-sciences.html

SAP. (n.d.). *MES: The Power of Real-Time Data*. SAP. https://www.sap.com/canada/products/scm/execution-mes/what-is-mes.html

SOLARWINDS. (n.d.). *What Is WSUS? Windows Server Update Services Guide - IT Glossary | SolarWinds*. Www.solarwinds.com. https://www.solarwinds.com/resources/it-glossary/wsus-windows-server-update-services