JOURNAL LA MULTIAPP

VOL. 05, ISSUE 05 (630-645), 2024
DOI: 10.37899/journallamultiapp.v5i5.1524

TOGAF's Approach in Developing an Enterprise Architecture for the Information Technology Security Industry

Rachmad Syarul Hidayat[1], Richardus Eko Indrajit[1], Erick Dazki[1]

[1]Information Technology, Pradita University, Indonesia

**Corresponding Author: Rachmad Syarul Hidayat*
Email: rachmad.syarul@student.pradita.ac.id

Article Info

Article history:
Received 02 August 2024
Received in revised form 11 September 2024
Accepted 29 September 2024

Keywords:
Enterprise Architecture
TOGAF
Information Security Industry
Risk Identification
Security Policy Development
Security Solution Implementation

Abstract

The information technology security industry, encompassing various activities such as risk identification and assessment, policy development, and solution implementation, plays a crucial role in maintaining the integrity and security of information systems. This study aims to develop and implement an efficient and effective enterprise architecture within the information security sector, focusing on three key core processes identified as the major revenue contributors: risk identification and assessment, security policy development, and security solution implementation. Utilizing the TOGAF-based Enterprise Architecture framework, this research identifies and designs architecture that integrates various systems, applications, and business processes, facilitating better alignment within the organization. The architecture design process involves a thorough analysis of operational needs and business strategies, leading to the development of a model that enhances efficiency and reduces the risk of failure in technology implementation. The outcomes of this study are intended to provide practical guidance for information security companies to optimize operations, simplify system complexities, and achieve strategic goals more effectively. It is anticipated that the application of the designed architecture will have a significant positive impact on the company's ability to address challenges and dynamic needs within the information security industry.

Introduction

In the rapidly evolving digital era, the information technology (IT) security industry faces increasingly complex challenges in protecting organizational assets and data. Along with the increasing cyber threats and the need for compliance with various regulations, companies in this industry are required to develop a robust and adaptive enterprise architecture. Enterprise architecture (EA) is a strategic approach that can help organizations align business goals with the information technology that supports them. One of the most recognized and widely used EA frameworks is TOGAF (The Open Group Architecture Framework).

TOGAF provides a comprehensive methodology for designing, planning, implementing, and managing enterprise architectures (Dumitriu & Popescu, 2020). This framework allows organizations to optimize business and technology processes, ensure better integration, and improve operational efficiency and effectiveness. The IT security industry, with its unique dynamics and demands, requires a specialized and structured approach to developing enterprise architectures that are able to respond quickly to environmental changes and threats. According to research from The Open Group, the implementation of TOGAF has been proven to improve the ability of organizations to face technological and business challenges, including in the IT security industry (Al-Turkistani et al., 2021; Kotusev, 2018). Case studies

ISSN: 2716-3865 (Print), 2721-1290 (Online)

show that companies that adopt TOGAF as a guide in developing enterprise architectures are able to achieve a higher level of integration between security systems and businesses, as well as accelerate response to security incidents (The Open Group, 2023).

In addition, TOGAF also supports the development of frameworks that comply with international standards such as ISO/IEC 27001 for information security management (Najib et al., 2018). This is important given that the IT security industry often has to meet strict compliance requirements and face regular audits. The implementation of TOGAF can assist organizations in managing risk and ensuring that information security policies and procedures are implemented consistently and effectively (ISO/IEC, 2018).

Thus, this paper aims to explore TOGAF's approach in developing enterprise architecture in the information technology security industry. Through case studies and in-depth analysis, it is hoped that it can provide insight into best practices and challenges faced in the implementation of TOGAF in this sector.

The purpose of this study is to develop and design enterprise architecture in the information technology security industry using the TOGAF approach. This research aims to apply the TOGAF method in planning and management of information technology, so that it can help companies in developing comprehensive and structured IT plans. By using TOGAF, it is hoped that the company's internal system will be more organized, and information technology operations can run more efficiently. The application of a designed enterprise architecture will ensure that only application systems that are relevant and support operations will be implemented, thereby increasing the effectiveness and order in information technology management.

TOGAF (The Open Group Architecture Framework) is an enterprise architecture framework used to design, plan, implement, and manage information technology architectures throughout the organization. TOGAF is designed to provide systematic structural guidance in the development of enterprise architectures, with the primary goal of improving organizational efficiency and effectiveness through better IT integration and management (Gulledge, 2008).

TOGAF is built on a methodology known as ADM (Architecture Development Method), which is the core of this framework. ADM provides a cyclical and iterative approach to developing an architecture that includes eight main phases: Preliminary, Architecture Vision, Business Architecture, Information Systems Architectures, Technology Architecture, Opportunities and Solutions, Migration Planning, and Implementation Governance. These phases are designed to ensure that all aspects of the enterprise architecture are handled in a structured and integrated manner (The Open Group, 2018).

The TOGAF framework also includes the Architectural Content Framework and Enterprise Continuum. The Architectural Content Framework serves to compile and organize the architectural artifacts generated during the ADM process, while Enterprise Continuum provides context for understanding and managing the various architectures and solutions used across the organization. Enterprise Continuum helps in grouping architectures and solutions from the most general to the most specific levels, supporting a more cohesive and adaptive architecture (Lankhorst, 2009; Majstorović & Terzić, 2018).

One of the main advantages of TOGAF is its flexibility and scalability. TOGAF can be applied to different types of organizations, from large to small, as well as to various industries. This allows organizations to tailor the framework to specific needs and challenges. In addition, TOGAF supports standards-based approaches and methodologies that can be integrated with the latest best practices and technologies, ensuring that the architecture developed remains relevant and effective (Bernard, 2012).

Methods

The research was carried out in several stages, namely Literature Study, Data Collection, Business Architecture Design, Application Architecture Design, Data and Information Architecture Design, Technology Architecture Design, Discussion, and Conclusion.

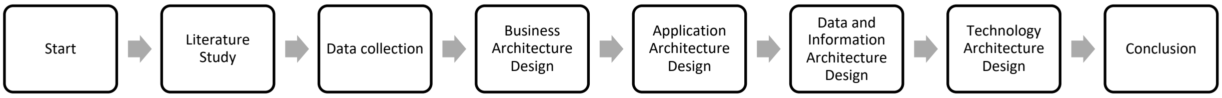

Start
Literature Study
Data collection
Business Architecture Design
Application Architecture Design
Data and Information Architecture Design
Technology Architecture Design
Conclusion

Figure 1. Research Stages

Enterprise Architecture (EA) defines the current and desired state of organizational processes, capabilities, application systems, data, and IT infrastructure. EA provides the necessary roadmap to achieve the architectural goals that have been set. EA documents record the adaptations that occur in various elements of the organization, as well as the time and reason for the change. This makes the EA a useful tool in flexibility and customization analysis. With EAs, organizations can make early identification of important trends and events, as well as provide quick responses both inside and outside the company (Bernard, 2012;Ross et al., 2006; The Open Group, 2018).

The benefits of implementing Enterprise Architecture in the industry include identifying dependencies and synergizing resources, improving solution development, and increasing customer and employee satisfaction. EA also contributes to improved information quality, organizational alignment, internal communication, as well as better operational efficiency (Haeckel, 1999).

In managing complexity, EA uses a variety of views and layers to describe architectural elements such as processes, data, and technology. Each view offers a different perspective that is relevant to a particular stakeholder, while those layers group related components that provide services to the next layer. ArchiMate is a modeling standard used to describe enterprise architecture through six layers: Strategy, Business, Application, Technology, Physical, and Implementation & Migration. Published by The Open Group (TOG) in 2009, ArchiMate is specifically designed to model the architecture of companies as a whole. ArchiMate allows architects to model elements such as an organization's products and services, the business processes that support those products and services, as well as the support of information systems and IT infrastructure. Many authors recommend the use of ArchiMate in Enterprise Architecture modeling following The Open Group Architecture Framework (TOGAF) to maximize the effectiveness of implementation (Bernard, 2012; The Open Group, 2009; The Open Group, 2009; The Open Group, 2018).

Results and Discussion

A general business model that describes core components, such as core processes, suppliers, customers, and supported resources in the development of Enterprise Architecture in the information technology security industry, obtained from interviews with experts, can be presented in the following figure:

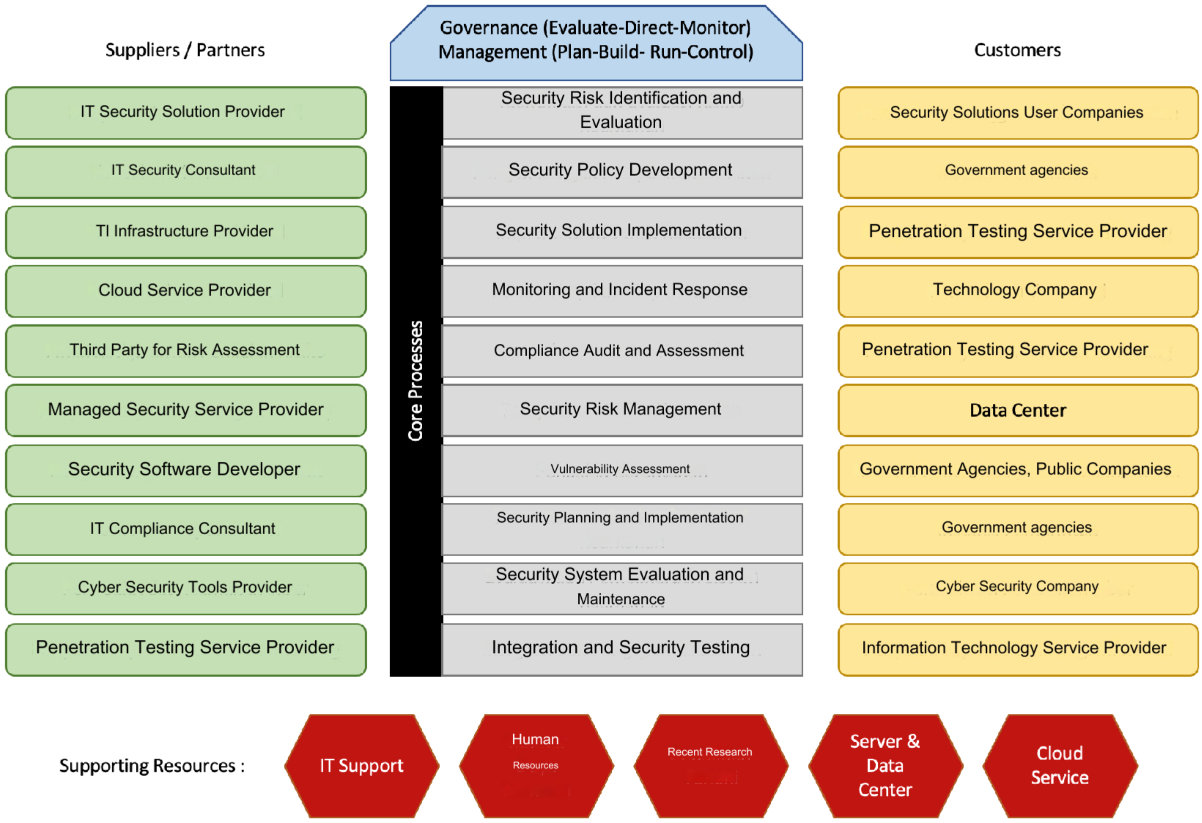

Governance (Evaluate-Direct-Monitor)
Management (Plan-Build- Run-Control)
Suppliers / Partners
Customers
Core Processes
IT Security Solution Provider
IT Security Consultant
TI Infrastructure Provider
Cloud Service Provider
Third Party for Risk Assessment
Managed Security Service Provider
Security Software Developer
IT Compliance Consultant
Cyber Security Tools Provider
Penetration Testing Service Provider
Security Risk Identification and Evaluation
Security Policy Development
Security Solution Implementation
Monitoring and Incident Response
Compliance Audit and Assessment
Security Risk Management
Vulnerability Assessment
Security Planning and Implementation
Security System Evaluation and Maintenance
Integration and Security Testing
Security Solutions User Companies
Government agencies
Penetration Testing Service Provider
Technology Company
Penetration Testing Service Provider
Data Center
Government Agencies, Public Companies
Government agencies
Cyber Security Company
Information Technology Service Provider
Supporting Resources :
IT Support
Human Resources
Recent Research
Server & Data Center
Cloud Service

Figure 2. Core Processes, Suppliers / Partners, Customer, and Supporting Resources

According to the experts we interviewed, there are three core processes that are the largest revenue contributors in the IT security industry, namely: Security Risk Identification and Evaluation, Security Policy Development, and Security Solution Implementation. With each explanation as follows:

Security Risk Identification and Evaluation: This process involves a thorough analysis of potential risks that could affect IT security systems. Risk identification helps organizations understand the threats they may face, while risk evaluation makes it possible to determine the impact and likelihood of such threats, as well as develop effective mitigation strategies.

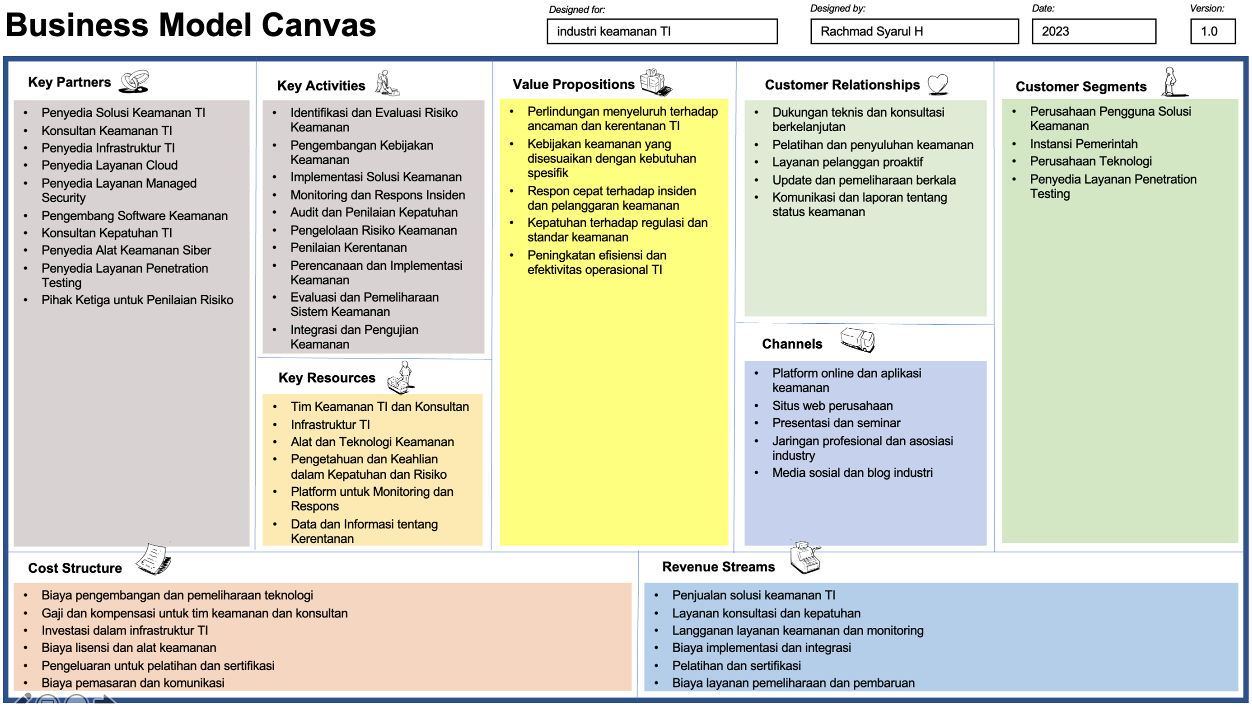
Security Policy Development: This process includes the drafting and implementation of security policies that define rules and procedures for protecting data and systems. These policies include access controls, data protection, and security incident handling. Strong policy development ensures that all aspects of IT security are well-regulated and consistent across the organization.

Security Solution Implementation: This process involves implementing technologies and tools designed to protect IT systems from threats. Security solution implementation includes security software settings, firewalls, intrusion detection systems, and other solutions that help maintain data integrity and confidentiality. This process also involves configuring and maintaining the system to ensure the effectiveness of protection (Pourzolfaghar et al., 2020).

Business Architecture

In this section, the aspects that affect the running of business in the IT security industry will be explained. These aspects can be described in the form of a Business Model Canvas, which describes various important elements that affect the company's strategy and operations in this sector. This Business Model Canvas includes various components such as Key Partners, Key Activities, Key Resources, Value Propositions, Customer Relationships, Channels, Customer

Segments, Cost Structure, and Revenue Streams. Figure 3 shows a visualization of the Business Model Canvas for the IT security industry, which provides a comprehensive overview of how companies run operations, interact with partners and customers, and manage costs and revenue.



Business Model Canvas

Designed for: industri keamanan TI

Designed by: Rachmad Syarul H

Date: 2023

Version: 1.0

Key Partners
- Penyedia Solusi Keamanan TI
- Konsultan Keamanan TI
- Penyedia Infrastruktur TI
- Penyedia Layanan Cloud
- Penyedia Layanan Managed Security
- Pengembang Software Keamanan
- Konsultan Kepatuhan TI
- Penyedia Alat Keamanan Siber
- Penyedia Layanan Penetration Testing
- Pihak Ketiga untuk Penilaian Risiko

Key Activities
- Identifikasi dan Evaluasi Risiko Keamanan
- Pengembangan Kebijakan Keamanan
- Implementasi Solusi Keamanan
- Monitoring dan Respons Insiden
- Audit dan Penilaian Kepatuhan
- Pengelolaan Risiko Keamanan
- Penilaian Kerentanan
- Perencanaan dan Implementasi Keamanan
- Evaluasi dan Pemeliharaan Sistem Keamanan
- Integrasi dan Pengujian Keamanan

Key Resources
- Tim Keamanan TI dan Konsultan
- Infrastruktur TI
- Alat dan Teknologi Keamanan
- Pengetahuan dan Keahlian dalam Kepatuhan dan Risiko
- Platform untuk Monitoring dan Respons
- Data dan Informasi tentang Kerentanan

Value Propositions
- Perlindungan menyeluruh terhadap ancaman dan kerentanan TI
- Kebijakan keamanan yang disesuaikan dengan kebutuhan spesifik
- Respon cepat terhadap insiden dan pelanggaran keamanan
- Kepatuhan terhadap regulasi dan standar keamanan
- Peningkatan efisiensi dan efektivitas operasional TI

Customer Relationships
- Dukungan teknis dan konsultasi berkelanjutan
- Pelatihan dan penyuluhan keamanan
- Layanan pelanggan proaktif
- Update dan pemeliharaan berkala
- Komunikasi dan laporan tentang status keamanan

Channels
- Platform online dan aplikasi keamanan
- Situs web perusahaan
- Presentasi dan seminar
- Jaringan profesional dan asosiasi industry
- Media sosial dan blog industri

Customer Segments
- Perusahaan Pengguna Solusi Keamanan
- Instansi Pemerintah
- Perusahaan Teknologi
- Penyedia Layanan Penetration Testing

Cost Structure
- Biaya pengembangan dan pemeliharaan teknologi
- Gaji dan kompensasi untuk tim keamanan dan konsultan
- Investasi dalam infrastruktur TI
- Biaya lisensi dan alat keamanan
- Pengeluaran untuk pelatihan dan sertifikasi
- Biaya pemasaran dan komunikasi

Revenue Streams
- Penjualan solusi keamanan TI
- Layanan konsultasi dan kepatuhan
- Langganan layanan keamanan dan monitoring
- Biaya implementasi dan integrasi
- Pelatihan dan sertifikasi
- Biaya layanan pemeliharaan dan pembaruan

Figure 3. Business Model Canvas in the IT Security Industry

Key Partners

IT Security Solution Provider, a company that provides a wide range of solutions and software to protect information systems from cyber threats and attacks. (Hacks et al., 2019)

IT Security Consultant, a specialist who provides consultation on strategies and best practices in IT security risk management. (Pourzolfaghar et al., 2020)

IT Infrastructure Providers, which offer the technological infrastructure, including servers and networks, that are necessary to support the operation of IT security systems. (Gong et al., 2020)

Cloud Service Providers, companies that offer cloud-based platforms for data storage and security applications, enable secure and efficient access. (Korhonen & Halén, 2017)

Managed Security Service Provider, which offers managed security services, including continuous monitoring and response to security incidents. (Niemi & Pekkola, 2020)

Security Software Developer, an individual or company that designs and develops specialized software to protect data and systems from cyber threats. (Pourzolfaghar et al., 2020)

IT Compliance Consultant. Professionals who assist organizations in meeting regulations and compliance standards related to information security. (Sales et al., 2019)

Cybersecurity tool providers. A company that provides tools to monitor, detect, and respond to cyber threats in IT systems (Ellerm & Morales-Trujillo, 2020).

Penetration Testing Service Providers. A provider that conducts penetration tests to find weaknesses in security systems through attack simulation. (de Kinderen et al., 2014)

Third Parties for Risk Assessment. An independent organization that evaluates and assesses IT security risks to provide mitigation recommendations. (Sadovykh et al., 2020)

Key Activities

Identification and Evaluation of Security Risks. The process of identifying potential risks to IT security and evaluating the impact and likelihood of such risks. (Korhonen & Halén, 2017).

Security Policy Development. Policy creation that establishes rules and procedures to protect IT information and systems from security threats (Shanks et al., 2018).

Security Solution Implementation. Implementation of technological solutions and procedures to protect IT systems from attacks and security threats (Niemi & Pekkola, 2020).

Incident Monitoring and Response. Continuous monitoring of the system to detect security incidents and quick response to address issues as they arise. (Pourzolfaghar et al., 2020)

Compliance Audits and Assessments. The audit process is to ensure that IT security practices comply with applicable standards and regulations. (de Kinderen et al., 2014)

Security Risk Management. Managerial processes for managing IT security risks through appropriate mitigation and controls. (Sadovykh et al., 2020)

Vulnerability Assessment. Evaluate IT systems to identify vulnerabilities that can be exploited by unauthorized parties. (Gong et al., 2020; Hacks et al., 2019)

Security Planning and Implementation. The process of planning and implementing a security strategy to protect IT assets as a whole. (Sales et al., 2019)

Evaluation and Maintenance of Security Systems. Periodic assessment and maintenance of the security system to ensure effectiveness and compliance with the established standards. (Hacks et al., 2019)

Security Integration and Testing. Integration of security solutions into IT systems and testing to ensure that they work as expected. (Ellerm & Morales-Trujillo, 2020)

Key Resources

IT Security Team and Consultants. Personnel are experienced in managing and protecting IT systems from security threats. (Gong et al., 2020)

IT infrastructure. Systems and hardware required to support IT security operations. (Varl et al., 2022)

Security Tools and Technology. Software and hardware used to detect and prevent security threats. (Coronado Mondragon & Coronado Mondragon, 2018)

Knowledge and Expertise in Compliance and Risk. Competence in ensuring that IT systems are compliant with regulations and managing risks. (Szczepaniuk et al., 2020)

Platform for Monitoring and Response. A system that enables real-time monitoring and response to security incidents. (Mirsalari & Ranjbarfard, 2020)

Data and Information about Vulnerabilities. Important information regarding weaknesses that can be exploited by attackers. (Ali et al., 2019)

Alue Proposition

End-to-end protection against IT threats and vulnerabilities. Provides comprehensive solutions to protect IT systems from various threats (Ali et al., 2019).

Security policies tailored to specific needs. Develop policies that suit the unique needs of each organization (Hanafi & Purba, 2021).

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Rapid response to incidents and security breaches. Provides rapid response to minimize the impact of security incidents (de Kinderen et al., 2014).

Compliance with regulations and safety standards. Guarantee that the solution meets all regulations and industry standards (Hacks et al., 2019).

Increased efficiency and effectiveness of IT operations. Improve IT operational performance through integrated solutions (de Kinderen et al., 2014).

Customer Relationship

Technical support and ongoing consulting. Provide continuous technical assistance and consultation (Ellerm & Morales-Trujillo, 2020).

Security training and counseling. Provide training to improve safety awareness and skills (Sales et al., 2019).

Proactive customer service. Take proactive steps to maintain good relationships with customers (Sadovykh et al., 2020).

Regular updates and maintenance. Offers periodic system maintenance and updates (Niemi & Pekkola, 2020).

Communication and reporting on security status. Provides regular reports on the status and health of IT security (Shanks et al., 2018).

Channels

Online platforms and security apps. Provide solutions through web-based applications and platforms (Korhonen & Halén, 2017).

Company website. Provide information and services through the company's website (Pourzolfaghar et al., 2020).

Presentations and seminars. Conveying information and education through formal events (Varl et al., 2022).

Professional networks and industry associations. Using networks to build relationships and share information (de Kinderen et al., 2014).

Social media and industry blogs. Disseminate information and attract attention through social media platforms and blogs (Szczepaniuk et al., 2020).

Customer Segments

Security Solution User Companies. Organizations that use security solutions to protect their IT assets (Mirsalari & Ranjbarfard, 2020).

Government Agencies. Government agencies that need security solutions to protect sensitive data (Ali et al., 2019).

Technology Companies. Companies that need protection for their technology products and services (Gao et al., 2019).

Penetration Testing Service Providers. Companies that focus on penetration testing to identify vulnerabilities (Hanafi & Purba, 2021).

Cost Structure

Technology development and maintenance costs. Expenditure on creating and updating security technologies (Martynov et al., 2018).

Salaries and compensation for security teams and consultants. Payments to staff involved in IT security (Sadovykh et al., 2020).

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Investments in IT infrastructure. Expenditure on infrastructure that supports IT operations (Niemi & Pekkola, 2020).

License fees and security tools. Expenditure on necessary software and tools (Shanks et al., 2018).

Expenditure on training and certification. Costs incurred to improve skills and qualifications (Korhonen & Halén, 2017).

Marketing and communication costs. Expenditure on promoting services and communicating with customers (Pourzolfaghar et al., 2020).

Revenue Stream

Sales of IT security solutions. Revenue from the sale of security products (de Kinderen et al., 2014).

Consulting and compliance services. Revenue from providing security and compliance-related consulting (Szczepaniuk et al., 2020).

Security and monitoring service subscriptions. Revenue from the subscription model for security monitoring services (Mirsalari & Ranjbarfard, 2020).

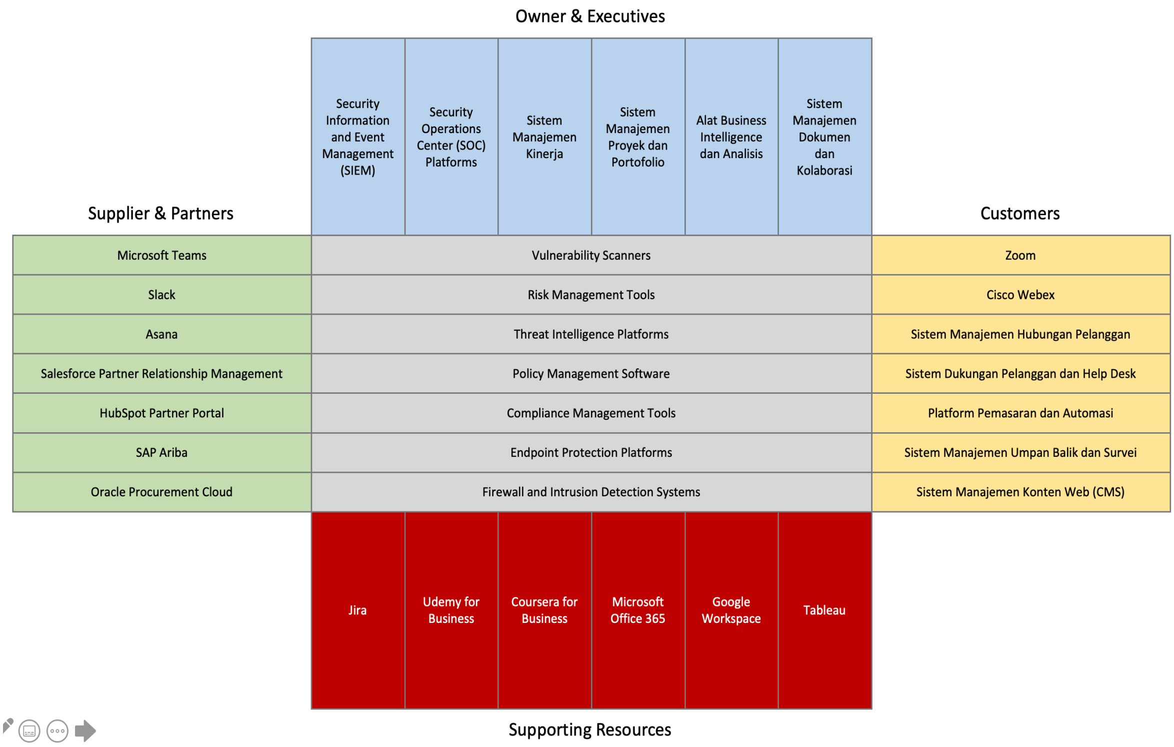
Implementation and integration costs. Revenue from security solution implementation costs (Ali et al., 2019).

Training and certification. Income from the provision of training and certification (Gao et al., 2019).

Maintenance and renewal service fees. Revenue from security system maintenance and update costs (Hanafi & Purba, 2021).

Application Architecture

In this section, we will explain the applications that support architectural components which include suppliers, core processes, support, owner and executive, and customers. This description includes the applications required for each element of the architecture, from how the application supports supplier functions and core processes, to the role of the application in providing support, management, and oversight by the owner and executive. The application architecture is depicted through the visualization in figure 4, which shows the relationship between the application and the various components of the architecture to provide a clear picture of how the application supports the overall structure and operations.



Owner & Executives

Security Information and Event Management (SIEM)	Security Operations Center (SOC) Platforms	Sistem Manajemen Kinerja	Sistem Manajemen Proyek dan Portofolio	Alat Business Intelligence dan Analisis	Sistem Manajemen Dokumen dan Kolaborasi

Supplier & Partners		Customers
Microsoft Teams	Vulnerability Scanners	Zoom
Slack	Risk Management Tools	Cisco Webex
Asana	Threat Intelligence Platforms	Sistem Manajemen Hubungan Pelanggan
Salesforce Partner Relationship Management	Policy Management Software	Sistem Dukungan Pelanggan dan Help Desk
HubSpot Partner Portal	Compliance Management Tools	Platform Pemasaran dan Automasi
SAP Ariba	Endpoint Protection Platforms	Sistem Manajemen Umpan Balik dan Survei
Oracle Procurement Cloud	Firewall and Intrusion Detection Systems	Sistem Manajemen Konten Web (CMS)

Jira	Udemy for Business	Coursera for Business	Microsoft Office 365	Google Workspace	Tableau

Supporting Resources

Figure 4. Application architecture in the IT security industry

The applications and systems needed to support the core business, or core business, are as follows: a) Vulnerability Scanners (e.g., Nessus, Qualys) to detect vulnerabilities in the system; b) Risk Management Tools (e.g., RiskWatch, FAIR) to assess and manage risk; c) Threat Intelligence Platforms (e.g., Recorded Future, ThreatConnect) to get information about the latest threats; d) Policy Management Software (e.g., PolicyTech, ConvergePoint) to compile and distribute security policies; e) Compliance Management Tools (e.g., Qualys Compliance, MetricStream) to ensure policies are compliant; f) Endpoint Protection Platforms (e.g., CrowdStrike, McAfee) to protect devices from threats; g) Firewall and Intrusion Detection Systems (e.g., Palo Alto Networks, Snort) to monitor and protect the network.

The applications and systems needed to establish cooperation or communication with suppliers / partners are as follows: a) Microsoft Teams. Facilitate team communication and collaboration with chat, video calling, and file sharing; b) Slack: A team messaging platform that makes it easy to communicate in real-time and integrate with a variety of other tools; c) Asana: Provides project and task management features that enable collaboration and progress tracking; d) Salesforce Partner Relationship Management: Enables relationship management with partners, including performance tracking and collaboration; e) HubSpot Partner Portal: Offers tools for partner management and marketing automation; f) SAP Ariba: Facilitating supply chain management and relationships with suppliers, including procurement and payments; g) Oracle Procurement Cloud: Offers solutions to manage the entire procurement cycle and collaborate with suppliers.

The applications and systems needed for owners & executives are as follows: a) Security Information and Event Management (SIEM) (e.g., Splunk, IBM QRadar) to collect and analyze security logs; b) Security Operations Center (SOC) Platforms (e.g., Exabeam, Sumo Logic) to monitor security activities in real-time; c) Performance Management System, to assist in measuring organizational performance and supporting strategic decision-making by presenting key performance indicators (KPIs); d) Project and Portfolio Management System, to carry out project planning and tracking in monitoring progress and resource allocation; e) Business Intelligence and Analysis tools, for data analysis and report generation that assist executives in making strategic decisions; f) Document Management and Collaboration Systems, as a solution for document management and team collaboration, allow executives to share information efficiently.

The applications and systems needed to establish business and as a means of communication with customers are as follows: a) Zoom, used for video meetings and webinars with partners and customers.; b) Cisco Webex, as an alternative to zoom for some customers. As a meeting solution through video and collaboration with additional features; c) Customer Relationship Management (CRM) System, to track customer interactions, manage customer data, and personalize customer experiences; f) Customer Support System and Help Desk, as a solution for ticket management, customer support, and equipped with a knowledge base that allows for efficient handling of customer issues; g) Marketing and Automation Platform, to perform email campaign management, enable newsletter delivery, and marketing automation to communicate with customers proactively; h) Feedback and Survey Management System, to create and manage surveys, collect customer feedback, and analyze results for service improvement; i) Web Content Management System (CMS), allows the creation and management of web content that is integrated with customer communication features such as contact forms and live chat. Thus offering flexibility and integration with various customer communication tools.

Data and Information Architecture

The information architecture and relationships between data stored in various databases in the applications discussed earlier will be explained in detail. Every data element contained in the core process, supplier & partner, owner & executive, customer, and supporting resources is integrated to support the overall operation and business strategy. A complete visualization of this architecture can be seen in figure 5.

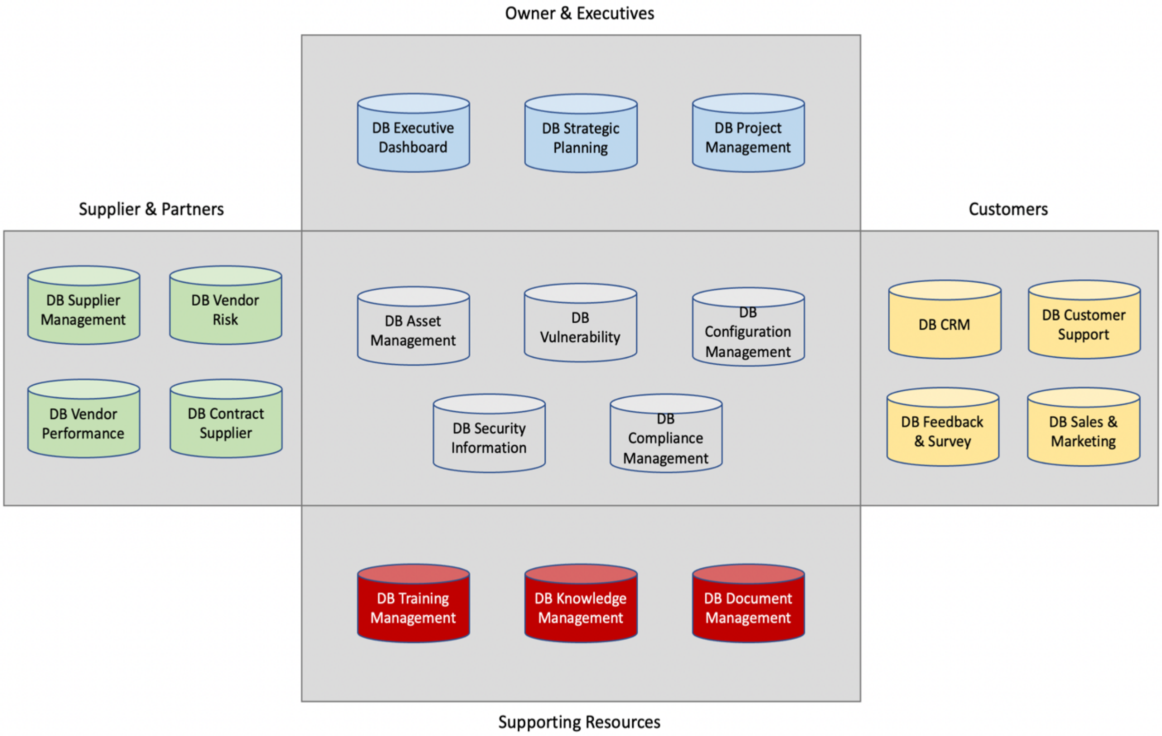


Figure 5. Data and information architecture in the IT security industry

Core Process

The core process segment has 5 databases, namely the asset management database used to store data from the Endpoint Protection Tools application and the Firewall & Intrusion

Detection System application. The vulnerability database is used to store data from the Vulnerability Scanner application. The configuration management database is used to store data from the Policy Management Software application. The security information database is used to store data from the Risk Management Tools application and the Threat Intelligence Platforms application. As well as a compliance management database for the Compliance Management Tools application.

Supplier & Partners

The supplier & partners segment has 4 databases, namely the Supplier Management database which is used to store data from the Microsoft Teams app, Slack app, and Asana app. A vendor risk database used to store data from the Salesforce Partner Relationship Management app. A vendor performance database used to store data from the Hubspot Partner Portal app. As well as the supplier contract database which is used to store data from the oracle procurement cloud application and the SAP Ariba application.

Owner & Executives

The owner & executives segment has 3 databases, namely the executive dashboard database which is used to store data from the Security Information and Event Management (SIEM) application and the Security Operation Center (SOC) Platform application. A strategic planning database used to store data from business intelligence and analysis tool applications. As well as a project management database used to store data from performance management system applications, project and portfolio management system applications, and document and collaboration management system applications.

Customer

The customer segment has 4 databases, namely the CRM database used to store data from the Zoom application, the Cisco Webex application, and the Customer Relationship Management System application. Customer Support database used to store data from Customer Support System and Help Desk applications. Feedback & Survey database used to store data from the Feedback Management System and Suebey applications. As well as the Sales & Marketing database which is used to store data from Marketing and Automation Platform applications and web content management system (CMS) applications.

Supporting Resources

The supporting resources segment has 3 databases, namely the training management database which is used to store data from the Jira application and the Microsoft 365 application. The knowledge management database is used to store data from the udemy for business application, and the Coursera for business application. As well as a document management database used to store data from Google workspace applications and Tableau applications.

Technology Architecture

Technology architecture is comprehensively designed with attention to the integration between Data and Information Architecture, and is tailored to the specific needs of Application Architecture and Business Architecture. This approach ensures that all technology components optimally support key functions in the Information Technology security industry. The design of the Technology Architecture applied to meet these needs is shown in Figure 6.

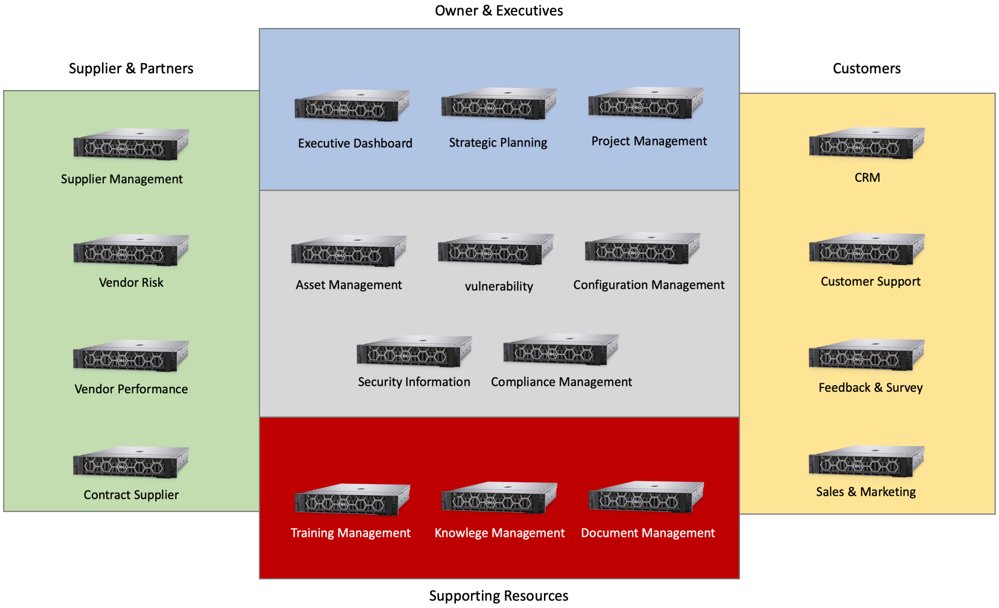


Figure 6. Technology Architecture in the IT security industry

In total, there are 33 applications and systems that support the operations of the IT security industry. Of these applications, not all require a separate database; Some applications are already bundling with their own databases. This allows for more efficient management and reduces the complexity of data management. So, there are only 19 databases that are managed separately. In the technology architecture, there are 19 servers used to run these various applications and systems. Multiple applications that don't require a lot of resources are combined into a single server for cost and resource efficiency, so that the use of technology infrastructure can be well optimized. In this study, business architecture modeling is focused on three core processes that are the largest revenue contributors in the IT security industry. Based on interviews with experts, the three main processes are Security Risk Identification and Evaluation, Security Policy Development, and Security Solution Implementation. Each of these processes has a crucial role in maintaining and increasing the company's revenue through increasing IT security effectiveness and mitigating risks that can threaten operational sustainability.

Security Risk Identification and Evaluation, a business architecture scheme on Security Risk Identification and Evaluation

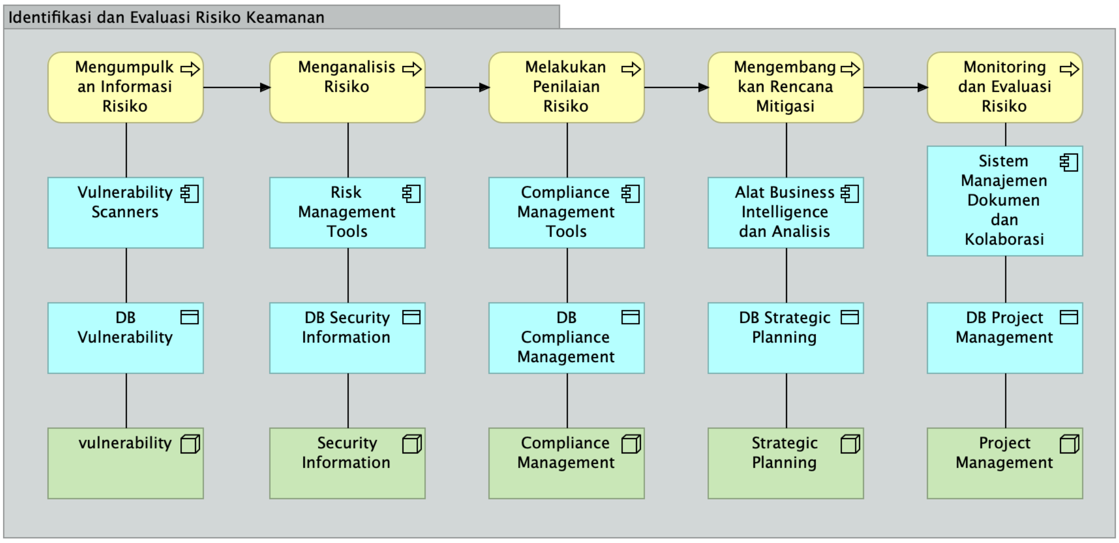

Identifikasi dan Evaluasi Risiko Keamanan
Mengumpulkan Informasi Risiko
Menganalisis Risiko
Melakukan Penilaian Risiko
Mengembangkan Rencana Mitigasi
Monitoring dan Evaluasi Risiko
Vulnerability Scanners
Risk Management Tools
Compliance Management Tools
Alat Business Intelligence dan Analisis
Sistem Manajemen Dokumen dan Kolaborasi
DB Vulnerability
DB Security Information
DB Compliance Management
DB Strategic Planning
DB Project Management
vulnerability
Security Information
Compliance Management
Strategic Planning
Project Management

Figure 7. Business architecture of security risk identification and evaluation

ISSN: 2716-3865 (Print), 2721-1290 (Online)

The process of identifying and evaluating security risks begins with the customer collecting risk information using the Vulnerability Scanners tool to identify weak points in the security system. This step is followed by a risk analysis with Risk Management Tools, which classifies and prioritizes risks based on their impact on the business. Furthermore, customers conduct a more in-depth risk assessment with Compliance Management Tools to ensure that all risks are in accordance with applicable standards and regulations. Based on the results of this assessment, the customer develops a mitigation plan using Business Intelligence and Analytics tools to develop an effective strategy. The final step is continuous monitoring and evaluation of risks with a Document Management and Collaboration System, which allows customers to monitor the implementation of mitigation plans and evaluate their effectiveness. This monitoring ensures that risks remain under control and corrective action can be taken if necessary. By using these tools, organizations can effectively manage IT security risks and ensure compliance with applicable regulations.

Security Policy Development, a business architecture scheme on Security Policy Development.

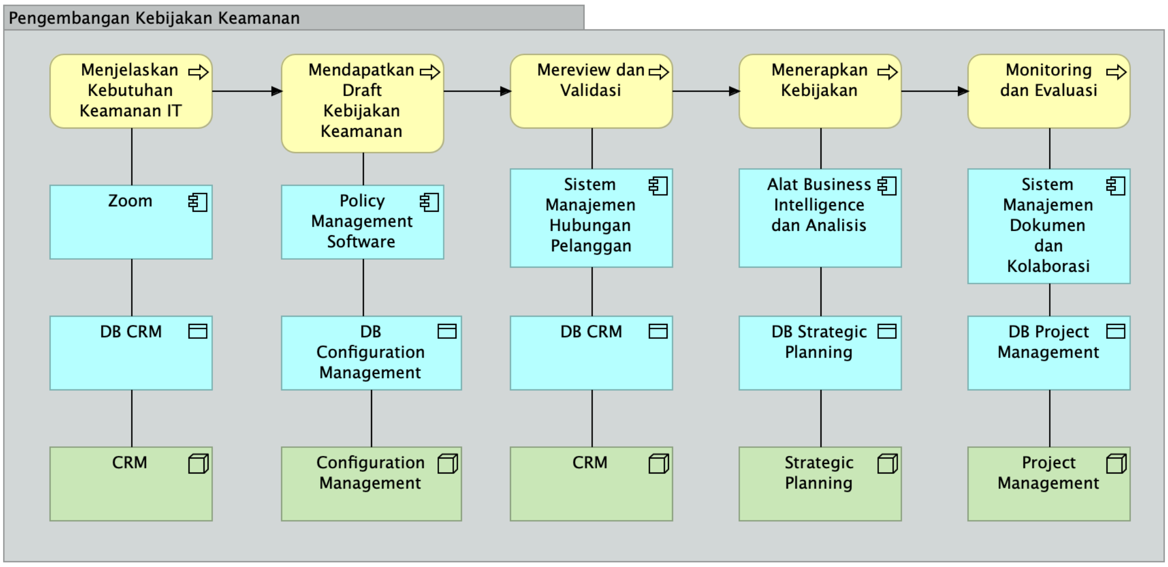

Pengembangan Kebijakan Keamanan
Menjelaskan Kebutuhan Keamanan IT
Mendapatkan Draft Kebijakan Keamanan
Mereview dan Validasi
Menerapkan Kebijakan
Monitoring dan Evaluasi
Zoom
Policy Management Software
Sistem Manajemen Hubungan Pelanggan
Alat Business Intelligence dan Analisis
Sistem Manajemen Dokumen dan Kolaborasi
DB CRM
DB Configuration Management
DB CRM
DB Strategic Planning
DB Project Management
CRM
Configuration Management
CRM
Strategic Planning
Project Management

Figure 8. Security policy development business architecture

The security policy development process begins with the customer explaining their IT security needs via the Zoom app or an in-person meeting to ensure a clear understanding of the security requirements. After that, customers get a draft security policy through the Policy Management Software application which helps in the preparation of policies that are in accordance with the specific needs of the organization. The next step is to review and validate this draft policy through the Customer Relationship Management System, which allows customers to provide feedback and make necessary adjustments. Once the policy is approved, the customer implements the policy using Business Intelligence and Analytics tools to ensure the policy is implemented effectively and in accordance with the planned security strategy. The final stage is continuous monitoring and evaluation of policies through the Document Management and Collaboration System, which allows customers to monitor the implementation of policies and evaluate their effectiveness in dealing with evolving security threats. This monitoring ensures that policies remain relevant and effective in maintaining the security of the organization's IT.

Security Solution Implementation, a business architecture scheme on Security Solution Implementation

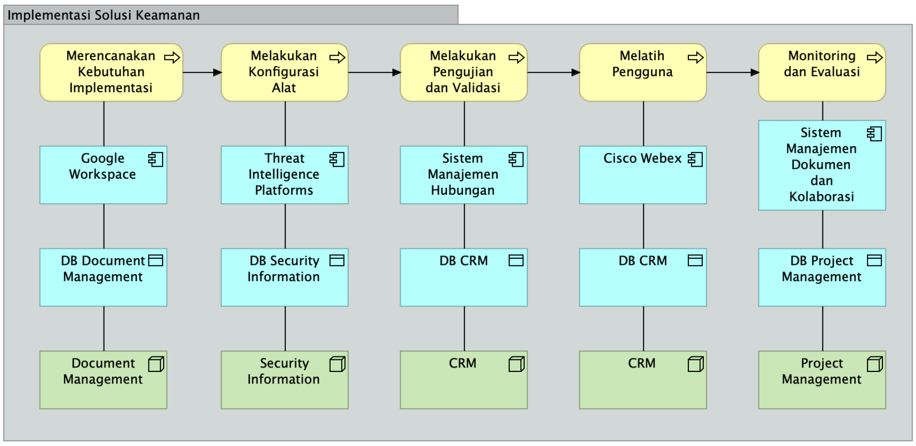

Implementasi Solusi Keamanan
Merencanakan Kebutuhan Implementasi
Melakukan Konfigurasi Alat
Melakukan Pengujian dan Validasi
Melatih Pengguna
Monitoring dan Evaluasi
Google Workspace
Threat Intelligence Platforms
Sistem Manajemen Hubungan
Cisco Webex
Sistem Manajemen Dokumen dan Kolaborasi
DB Document Management
DB Security Information
DB CRM
DB CRM
DB Project Management
Document Management
Security Information
CRM
CRM
Project Management

Figure 9. Security solution implementation business architecture

The security solution implementation process begins with the customer planning their implementation needs through the Google Workspace app, which allows them to plan and document all aspects required for the implementation of the security solution. Next, customers configure the tools using the Threat Intelligence Platforms application, which helps in configuring and setting up security tools according to the specific needs of the organization. Once the configuration is complete, the customer proceeds with testing and validation through the Customer Relationship Management System application to ensure that the security solution is working properly and in accordance with the set requirements. After successful testing, the customer conducted user training through the Cisco Webex application, ensuring that all users involved understood how to use the newly implemented security solution. The final stage is the continuous monitoring and evaluation of security solutions using the Document Management and Collaboration System application, which allows customers to monitor the performance of the solution, identify potential problems, and make necessary adjustments to maintain the effectiveness of the security solution in the long term.

Conclusion

The IT security industry encompasses a variety of important core processes that contribute significantly to the company's bottom line. Based on this research, we focus on the 3 core processes that generate the most revenue, namely the identification and evaluation of security risks, the development of security policies, and the implementation of security solutions. These three core processes have been designed using the Archimate core framework to integrate all elements in the organization effectively. This approach allows companies to achieve targets faster and more efficiently, as well as facilitate information technology implementation planning. Thus, the risk of failure in the information and technology implementation process can be minimized, ensuring that companies in the IT security industry can operate more securely and according to the expected standards.

References

Ali, A. Q., Sultan, A. B. M., Abd Ghani, A. A., & Zulzalil, H. (2019). A systematic mapping study on the customization solutions of software as a service applications. *IEEE Access, 7*, 88196–88217.

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021, April). Enterprise architecture frameworks assessment: capabilities, cyber security and resiliency review. In *2021 1st International conference on artificial intelligence and data analytics (CAIDA)* (pp. 79-84). IEEE. https://doi.org/10.1109/CAIDA51941.2021.9425343

Bernard, S. A. (2012). *An introduction to enterprise architecture*. AuthorHouse.

Coronado Mondragon, A. E., & Coronado Mondragon, C. E. (2018). Managing complex, modular products: how technological uncertainty affects the role of systems integrators in the automotive supply chain. *International Journal of Production Research, 56*(20), 6628–6643. https://doi.org/10.1080/00207543.2018.1424362

de Kinderen, S., Gaaloul, K., & Proper, H. A. (2014). Bridging value modelling to ArchiMate via transaction modelling. *Software & Systems Modeling, 13*(3), 1043–1057. https://doi.org/10.1007/s10270-012-0299-z

Dumitriu, D., & Popescu, M. A. M. (2020). Enterprise architecture framework design in IT management. *Procedia Manufacturing*, *46*, 932-940. https://doi.org/10.1016/j.promfg.2020.05.011

Ellerm, A., & Morales-Trujillo, M. E. (2020). Modelling security aspects with archimate: a systematic mapping study. *2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 577–584. https://doi.org/10.1109/SEAA51224.2020.00094

Gao, R., Wang, Y., Feng, Y., Chen, Z., & Eric Wong, W. (2019). Successes, challenges, and rethinking–an industrial investigation on crowdsourced mobile application testing. *Empirical Software Engineering, 24*, 537–561. https://doi.org/10.1007/s10664-018-9618-5

Gong, Y., Yang, J., & Shi, X. (2020). Towards a comprehensive understanding of digital transformation in government: Analysis of flexibility and enterprise architecture. *Government Information Quarterly, 37*(3), 101487. https://doi.org/10.1016/j.giq.2020.101487

Gulledge, T. R. (2008). Architecture-driven enterprise integration. *International Journal of Management and Enterprise Development*, *5*(3), 265-309. https://doi.org/10.1504/IJMED.2008.017433

Hacks, S., Höfert, H., Salentin, J., Yeong, Y. C., & Lichter, H. (2019). Towards the definition of enterprise architecture debts. *2019 IEEE 23rd International Enterprise Distributed Object Computing Workshop (EDOCW)*, 9–16. https://doi.org/10.1109/EDOCW.2019.00016

Haeckel, S. H. (1999). Adaptive enterprise: Creating and leading sense-and-respond organizations. *Harvard business press*.

Hanafi, B., & Purba, R. D. H. (2021). Perancangan Enterprise Architecture Dengan Modified Togaf Adm Pada PT Ilmu Komputercom Braindevs Sistema. *JISICOM (Journal of Information System, Informatics and Computing), 5*(2), 222–231. https://doi.org/10.52362/jisicom.v5i2.603

ISO/IEC. (2018). Information security management systems — Requirements. International Organization for Standardization. ISO/IEC 27001:2013.

Korhonen, J. J., & Halén, M. (2017). Enterprise architecture for digital transformation. *2017 IEEE 19th Conference on Business Informatics (CBI), 1*, 349–358. https://doi.org/10.1109/CBI.2017.45

Kotusev, S. (2018). TOGAF-based enterprise architecture practice: An exploratory case study. *Communications of the association for information systems*, *43*(1), 20. https://doi.org/10.17705/1CAIS.04320

Lankhorst, M. (2009). *Enterprise architecture at work* (Vol. 352). Springer.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Majstorović, M. N., & Terzić, R. M. (2018). Enterprise architecture as an approach to the development of information systems. *Vojnotehnicki glasnik/Military Technical Courier*, *66*(2), 380-398. https://doi.org/10.5937/vojtehg66-15850

Martynov, V. V, Shavaleeva, D. N., & Salimova, A. I. (2018). Designing optimal enterprise architecture for digital industry: state and prospects. *2018 Global Smart Industry Conference (GloSIC)*, 1–7. https://doi.org/10.1109/GloSIC.2018.8570159

Mirsalari, S. R., & Ranjbarfard, M. (2020). A model for evaluation of enterprise architecture quality. *Evaluation and Program Planning, 83*, 101853. https://doi.org/10.1016/j.evalprogplan.2020.101853

Najib, W., Sumaryono, S., Nugroho, L. E., & Putra, G. D. (2018, July). Development of Enterprise Security Framework in SKK Migas Based on Integration of ISO 27000 and SABSA Model. In *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)* (pp. 382-387). IEEE. https://doi.org/10.1109/ICITEED.2018.8534747

Niemi, E., & Pekkola, S. (2020). The benefits of enterprise architecture in organizational transformation. *Business & Information Systems Engineering, 62*, 585–597. https://doi.org/10.1007/s12599-019-00605-3

Pourzolfaghar, Z., Bastidas, V., & Helfert, M. (2020). Standardisation of enterprise architecture development for smart cities. *Journal of the Knowledge Economy, 11*(4), 1336–1357. https://doi.org/10.1007/s13132-019-00601-8

Ross, J. W., Weill, P., & Robertson, D. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard business press.

Sadovykh, A., Bagnato, A., Berre, A. J., & Walderhaug, S. (2020). Archimate as a specification language for big data applications-databio example. *Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment: Second International Workshop, DEVOPS 2019, Château de Villebrumier, France, May 6–8, 2019, Revised Selected Papers 2*, 191–199. https://doi.org/10.1007/978-3-030-39306-9_14

Sales, T. P., Roelens, B., Poels, G., Guizzardi, G., Guarino, N., & Mylopoulos, J. (2019). A pattern language for value modeling in ArchiMate. *Advanced Information Systems Engineering: 31st International Conference, CAiSE 2019, Rome, Italy, June 3–7, 2019, Proceedings 31*, 230–245. https://doi.org/10.1007/978-3-030-21290-2_15

Shanks, G., Gloet, M., Someh, I. A., Frampton, K., & Tamm, T. (2018). Achieving benefits with enterprise architecture. *The Journal of Strategic Information Systems, 27*(2), 139–156. https://doi.org/10.1016/j.jsis.2018.03.001

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security, 90*, 101709. https://doi.org/10.1016/j.cose.2019.101709

The Open Group. (2009). ArchiMate® 2.0 Specification. *Opengrup*.

The Open Group. (2018). Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group. *Opengrup*.

The Open Group. (2023). The TOGAF® Standard, 10th Edition. *The Open Group*.

Varl, M., Duhovnik, J., & Tavčar, J. (2022). Customized product development supported by integrated information. *Journal of Industrial Information Integration, 25*, 100248. https://doi.org/10.1016/j.jii.2021.100248