The Foundational Enterprise Security Architecture Framework

Table of Contents

List of Figures

List of Tables

Why Foundational Enterprise Security Architecture?

This publication was developed to aid and enable security (and IT) professionals who may not have the expertise, background or budget needed to develop a comprehensive Enterprise Security Architecture. To address this need, The Rubicon Advisory Group has developed a robust set of templates to aid in and support developing an entry level foundation for those who want to ensure or gain effective and efficient enterprise security for their organization.

All too often organizations, both large and small, both public and private, tend to struggle with understanding the need and value of Enterprise Security Architecture. While often seen purely as a bureaucratic paper-exercise, we can tell you this is far from the truth when you're actively engaged in an incident, attempting to troubleshoot a network issue, or planning for a digital transformation to revolutionize the organization.

It's true – as an industry, we're more than a bit loosey goosey when it comes to keeping accurate, relevant, and sorely needed information (doubt us, tell us about your asset inventory!). We understand that work is hard, and we are by no means publishing this framework as a reason to make "busy work." What we're attempting to do is prepare you for when you get that call at 2:12 on a Monday afternoon, asking why Brian Krebs is reaching out to the CEO for an official response to why you've been compromised, or for when a customer can no longer access their data and the round robin of blame between infrastructure, systems and application are pointing fingers at each other (we've all seen that) or because your leadership has made the decision to implement something new and valuable.

This publication is designed to complement existing architecture models. It serves as a starting point to highlight the value of understanding the interconnected information technology systems our enterprises depend on and underscores the importance of safeguarding the assets entrusted to us by our stakeholders.

Intended Use & General Disclaimer

The goal of this publication is to provide information technology and security professionals with a starting point, along with example deliverables, to support your Enterprise Security Architecture efforts. The templates provided need to be tailored and should act purely as a foundation for those who are looking at maturing and formalizing their enterprise's security architecture.

This publication is intended purely for the purpose of taking a practical approach to Enterprise Security Architecture. Buckle up, it's about to get weird! The templates provided need to be tailored to each organization specifically and are not intended to be a "one-size fits all." Instead, they are intended to be used to drive further discussions, considerations, and activities to ensure proper security alignment with the enterprise's strategy and goals.

This was written in collaboration and cooperation between: a full-stack hacker (Nicholas), a professional social engineer and business technology consultant (Rachel), an application security developer who gets enterprise security (Charles), a number of highly skilled and talented security executives (Kelvin, Pablo, Eric, and Tracy), a polymath AI, planet-scale information security & Cloud Guru (Kyle), some very talented folks from various government agencies (Brandon & Nick), an enterprise security architect (Sean), a bona fide physical security expert goddess like seriously she wrote a book and breaks into all the places (Valerie), a seasoned, veteran IT auditor who specializes on compliance (Jason) and the industry leader in Enterprise Governance (Mark) – and then there is the Iowa Farm Boy (Ed).

Acknowledgements

This publication could not have been created without the help, insight, expertise, and support of the following who have volunteered the most valuable of things, their time:

- Kelvin Arcelay, Owner/Principal – AALimited, Atlanta, Georgia
- Brad Barret. Security Advisor, Optiv, Louisville, Kentucky
- Pablo Breuer, President, Orthogonal Insights, Washington DC/Baltimore, Maryland
- Charles Burke, Enterprise Security Professional, BITCON, Lawrenceville, Georgia
- Eric F. Crist, Director of Security, Walleye Capital, LLC
- Sean Davis, DevSecOps Executive, Stealth Startup, Sarasota, Florida
- Nicholas Hinsch, InfoSec Consultant, The Rubicon Advisory Group, Ohio
- Laurie Jameson, Senior Advisor, Security Architecture, Transunion, Louisville, Kentucky
- Tracy Janes, vCISO, JMerak Consulting, Jacksonville, Florida
- Jason Lannen, Managing Director, Turnkey Compliance, Roswell, Georgia
- Hilary McCabe, Chief Administrative Officer, Brandenburg, Kentucky
- Brandon McCrillis, Independent Consultant, Qualified Cyber, Augusta, Georgia
- Yvonne Rivera, CISO, CyberMyte, Florida
- Rachel Schutt, InfoSec Consultant, The Rubicon Advisory Group, Columbus, Ohio
- Nick Suttle, Director of Security, Pillsbury Law, Nashville, Tennessee
- Kyle Stone, Chief Technology Officer, NetThunder, Louisville, Kentucky
- Mark Thomas, President Escoute, Phoenix, Arizona
- Valerie Thomas, Independent Cybersecurity Consultant, Washington DC/Baltimore, Maryland

Then there is Ed, he's a weird – eccentric - perchance, odd – definitely, strange – at times, but all in all he really tries to be a good person (as long as you don't give him sweet tea).

I want to thank everyone who contributed and invested their time into bringing this publication to be. Without these folks, this would never have been done. I truly appreciate the feedback, comments, discussions, and challenges that resulted in the Foundational Enterprise Security Architecture framework.

And to my wife Hilary – a special thank you for being my constant anchor and guiding light, especially during the toughest of times. Whether it was helping us navigate the hundreds of recommendations, language revisions, and "conscious streams of thought" to standing by me through my cancer diagnosis, you've always been there to keep me grounded, on task and target, and hopeful. Your strength and encouragement have been a source of resilience I can't put into words, and I feel endlessly grateful to have you by my side. Your work, even behind the scenes, is truly appreciated.

Sincerely,

Ed

Who is this framework for?

This framework is for those up-and-coming IT & cybersecurity practitioners entering the field, those who are working with organizations that may not be big enough to warrant a full-time security architect or hire a firm to do this for you. This framework is for all of you who have walked into the trials of "on the job training" and were told, "just figure it out." This framework is for those professionals who are charged with wearing many or in some instances all of the hats – maybe you're one of the many systems administrators trying to answer a 100-page questionnaire so your company can win a contract; maybe you're the only one responsible for IT, security, and compliance, who has just been told to "review our cybersecurity insurance policy." Whatever your station or status, we hope this framework helps you on your journey.

What is the Foundational Enterprise Security Architecture Framework?

At its core the Foundational Enterprise Security Architecture ("FESA") Framework is a structured and systematic approach to security that goes beyond the deployment of security technologies. It encompasses and includes the following key elements:

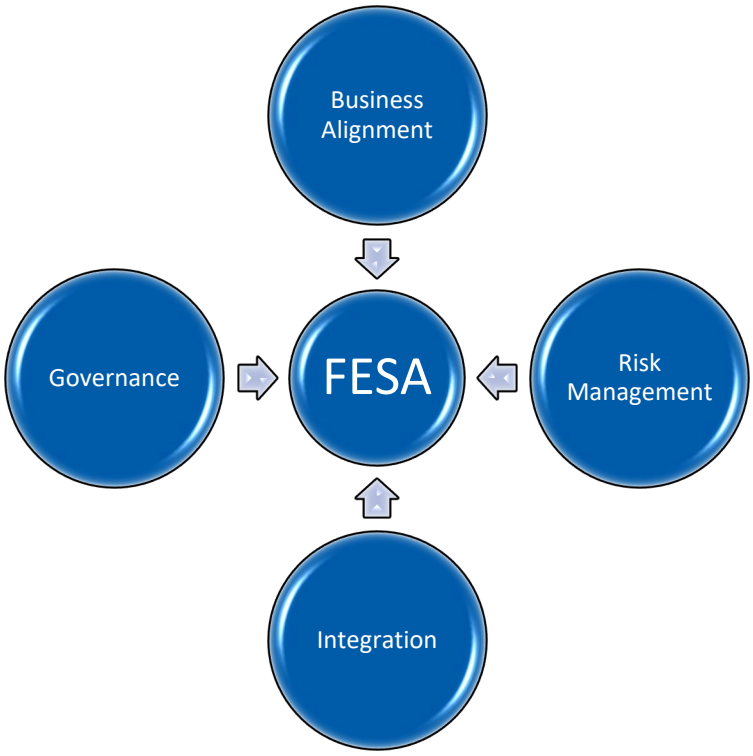


Figure 1 – The FESA Framework

Framework It provides a structured outline for designing and implementing security capabilities, policies, and controls that are tailored to the organization's unique needs, risks, and goals. Keyword here "***tailored***" – this is not meant to be a one and done, cookie-cutter approach. You're going to have to "tailor" this framework to meet the needs of your organization.

Alignment FESA intends to align security strategies with the organization's business objectives, ensuring that security measures are not just cost centers but strategic enablers. Since resources are limited, we need to ensure proper alignment of those resources to provide the most value to the enterprise.

Risk Management FESA focuses on identification, analysis, evaluation, assessment, and response to business risks. This is to ensure we protect critical assets, ensure business continuity, and maintain trust. If you noticed the term "business risk" – all risks are business risks, if you're hoping this will elevate the status of "Cyber Risk" – you're potentially going to be disappointed.

Cyber is just a subset of an enterprise's Operational Risks and that is one of many risks organizations face.

Integration FESA promotes stakeholder involvement for cohesive and effective integration of security solutions and processes across the organization. Integration means operationalizing as part of the normal business processes, not slapping a new control in and checking a box.

Governance FESA demonstrates the proper utilization of enterprise resources, optimizing risks and rewards, to the benefit of the enterprise. This approach guards against overinvestment, misplaced priorities, and a misleading sense of security. It strikes the necessary balance between performance and compliance to achieve meaningful results.

Which architecture is right for my organization?

How do you know which of the several Enterprise Security Architecture frameworks available is the "right one?" We've included a list of pros and cons in Appendix H that may help in selecting a framework. The choice of framework often depends on your specific industry, the size and needs of the enterprise, the maturity and most importantly the culture. As previously mentioned, the Foundational Enterprise Security Architecture framework isn't meant to replace existing architectures. Rather, it should be viewed and used to quick-start security architecture efforts. That being said, let's review some of the more common frameworks.

Open Enterprise Security Architecture (O-ESA)

The Open Group's Enterprise Security Architecture is an open and adaptable framework emphasizing collaboration and integration. It is suitable for diverse industries and organizations of varying sizes.

Pros:	Open and adaptable, encourages collaboration.
Cons:	Customization required.
Common Industry:	Diverse industries.
IT Staff Size:	Varies, often moderate.
Standards Body:	The Open Group promotes and maintains the framework.
Website:	https://pubs.opengroup.org/security/o-esa/

Department of Defense Architecture Framework (DoDAF)

The DoDAF is tailored for the defense industry and government agencies, offering a structured approach to security architecture.

Pros:	Well-structured for defense and government.
Cons:	Limited applicability outside defense and government sectors.
Common Industry:	Defense, Government.
IT Staff Size:	Moderate to large.
Standards Body:	The U.S. Department of Defense (DoD) promotes and maintains the framework.
Website:	https://dodcio.defense.gov/library/dod-architecture-framework/

SANS SEC549: Enterprise Cloud Security Architecture:

Focusing on cloud security architecture, crucial in today's cloud-driven landscape, SANS SEC549 is applicable across industries and adopted by organizations of various sizes who consume cloud services.

Pros:	Addresses cloud security needs.
Cons:	Specific to cloud security.
Common Industry:	Various industries adopting cloud technologies.
IT Staff Size:	Varies, often moderate.
Standards Body:	SANS promotes and maintains the framework.
Website:	https://www.sans.org/cyber-security-courses/enterprise-cloud-security-architecture/

The Open Security Architecture (OSA)

The Open Security Architecture is an open-source, adaptable framework that emphasizes (and relies on) community contributions. It is versatile and can be applied to different industries and organizations.

Pros:	Open-source, adaptable, versatile.
Cons:	Resource and support availability.
Common Industry:	Diverse industries.
IT Staff Size:	Varies, often moderate to small.
Standards Body:	The Open Security Architecture promotes and maintains the framework
Website:	https://opensecurityarchitecture.org

SABSA (Sherwood Applied Business Security Architecture)

SABSA aligns security strategy with business objectives and creates a direct traceability and linkage between business needs and risks and the implementation of the various controls, making it suitable for enterprises in highly regulated industries like finance, legal, healthcare, or government.

Pros:	Business-aligned security, adaptable.
Cons:	Complexity and may require specialized expertise.
Common Industry:	Finance, Healthcare, Government.
IT Staff Size:	Moderate to large.
Standards Body:	The SABSA Institute promotes and maintains the framework.
Website:	https://sabsa.org/

What about NIST and ISO, aren't those Enterprise Security Architecture Frameworks too?

No, no they are not. NIST's Cybersecurity Framework provides a tactical and descriptive approach to security, where ISO/IEC 27001 offers a systematic approach to information security management, to include a set of controls, risk management processes, and certification options.

These frameworks, when properly employed and aligned, can contribute to a well-rounded Enterprise Security Architecture by providing guidance on aligning security with business goals, managing risks, and implementing effective security controls. However, by themselves they are not considered to be an "enterprise security architecture."

NIST CSF (Cybersecurity Framework)

NIST's Cybersecurity Framework is flexible for managing cybersecurity, applicable to various industries and organizations of varying sizes. It is not considered an Enterprise Security Architecture framework when compared to other frameworks. While the NIST Cybersecurity Framework is valuable for improving cybersecurity and managing risks, it does not provide the level of detail or architectural guidance that is provided in traditional Enterprise Security Architecture frameworks.

Pros:	Flexible, applicable to various industries.
Cons:	Customization may be required.
Common Industry:	Various industries.
IT Staff Size:	Moderate to large.
Standards Body:	The U.S. National Institute of Standards and Technology (NIST) promotes and maintains the framework.
Website:	https://www.nist.gov/cyberframework

ISO 27001 & 27002

ISO 27001 is globally recognized for information security management, adaptable to different industries and enterprise sizes, with ISO 27002 providing detailed information on the various security controls. While ISO 27001 is a valuable standard for managing information security, it is not primarily focused on defining the architecture of an organization's security infrastructure. Instead, it provides a framework for establishing policies, processes, and controls to manage information security risks effectively.

Pros:	Globally recognized, adaptable.
Cons:	Certification process can be time-consuming and costly.
Common Industry:	Various industries.
IT Staff Size:	Moderate to large, due to the rigor of the certification process.
Standards Body:	The International Organization for Standardization (ISO) promotes and maintains the framework.
Website:	https://www.iso.org/standard/27001

Enterprise Security Architecture frameworks are more concerned with designing and accounting for the overall security architecture of an organization, ensuring alignment of security efforts and controls with the needs of the business objectives, providing comprehensive architectural guidance. The NIST and ISO frameworks tend to address the broader aspects of enterprise security, including how security fits within the larger enterprise architecture, technology infrastructure, and business processes.

What Enterprise Security Architecture Is Not

Enterprise Security Architecture is more than just implementing the latest security tools or technologies in isolation. It is not about buying the latest and greatest "mystical non-circle[1]"; doing so only creates a procurement exercise rather than demonstrating responsible financial stewardship of our organization's resources. Nor is it a mere collection of isolated security measures and controls[2].

Enterprise Security Architecture is not a one-size-fits-all solution. It must remain highly adaptable, tailored to align with the organization's specific strategy, requirements, and unique risks.

Moreover, Enterprise Security Architecture is not purely a technical initiative. It encompasses people, processes, and technology—intentionally in that order—to create a holistic security strategy that supports the organization's needs, balancing performance and compliance to deliver true value.

And last, but most importantly not least…

Enterprise Security Architecture is not just a Microsoft Visio Diagram!

[1] To avoid a lawsuit, we will avoid using the term "magic quadrant" as someone, who will remain nameless, might get litigious about it.

[2] That is what we in the industry call "a hot mess."

We know people are easily impressed by pretty diagrams, and their enthusiasm is so noted. However, all too often those diagrams fail to capture the appropriate level of detail, nor provide sufficient context to be of any real intrinsic value. Technical diagrams and data flows play their part, but they are only that - a part of security architecture.

If you are dead set on wanting to impress people with your mastery of Visio and your ability to build pretty pictures (while important) of clouds of computers and multi-color connectors that illustrate “secure” vs. “insecure” transmission pathways, this framework is probably not what you’re looking for.

Enterprise Security Architecture should be woven into the fabric of an organization’s goals, engineering practices, and operational activities; not just relegated to being a gatekeeping function. True security asks questions not to create roadblocks, but to manage risk management efforts to protect revenue.

ESA is in the business of "know," not "no." Its purpose is to design and implement business controls, policies, and procedures that mitigate risks and vulnerabilities while aligning with the organization’s goals.

The Goals of Enterprise Security Architecture

In today's rapidly evolving digital landscape, the need for robust security measures has never been more crucial. Enterprise Security Architecture (ESA) stands as the linchpin that not only safeguards an organization's valuable digital assets but also plays a pivotal role in enabling business growth and innovation. It ensures that security isn't a roadblock but rather a facilitator to help businesses achieve their objectives. Let's dig into the primary goals of ESA that make it an indispensable component of modern business operations.

The primary goals of why an organization should pursue ESA include:

> Business Enablement ESA aims to secure the organization's digital assets while enabling business growth and innovation. It ensures that security is a facilitator, not a hindrance, to achieving business objectives.
>
> Structured Governance It creates strong governance frameworks that uphold the consistent enforcement of security policies and controls, supporting compliance and risk mitigation while enabling optimal performance. ESA governance does not operate in isolation; instead, it documents and monitors risk-related decisions in alignment with organizational objectives.

Relationship with Business Enablement

Enterprise Security Architecture is integral to business enablement in several ways; however, it requires knowing the roles and responsibilities of your organization’s key stakeholders. For ease

of use, we have put together generalized RACI charts that can be tailored to your organization (see Appendix G). ESA facilitates and promotes the following:

Security as an Enabler By aligning security with business objectives, ESA helps organizations make informed decisions that enhance business capabilities while managing risks effectively.

Innovation and Agility A well-structured security architecture supports innovation by allowing organizations to confidently explore new technologies and business opportunities.

Customer Service "We are all a provider to someone else[3]" if your customers aren't happy with how you're handling (or mishandling) their data, they won't be customers for long. Proper Enterprise Security Architecture ensures consideration and accounting for the various expectations, statutory and regulatory requirements which our customers expect from us. Additionally, it allows our organizations to innovate and differentiate themselves in the market.

Stakeholder Confidence If you're not a good steward of your organization's resources, be that people, systems, or budget; or if you fail to deliver the value that you have promised, confidence and trust begin to erode[4].

Drivers for Enterprise Security Architecture

There are internal and external influences which drive the adoption of Enterprise Security Architecture:

Internal Drivers These include things like organization's strategic goals, risk appetite, tolerance & capacity, the need to protect assets, customer data, and intellectual property.

External Drivers External factors such as evolving threat landscapes, regulatory requirements, and contractual agreements for data protection and privacy also drive organizations to adopt ESA.

Routine Business Operations

It is our belief that Enterprise Security Architecture should be a fundamental part of routine business as usual operations, and not for the reasons you may think. Enterprise Security Architectures:

- help organizations assess and manage business risk as part of their everyday business activities.

[3] Mark Thomas, President Escoute

[4] In the event of losing stakeholder trust and confidence, end up playing a risky game of "Trust Me If You Can" – not a game that ends well for anyone.

- provide a structured framework for responding to security incidents, ensuring that the organization can recover swiftly and effectively, and in an efficient manner.

- assist in maintaining compliance with regulations and industry standards as a continuous, ongoing process.

Value

In today's constantly and rapidly evolving digital landscape, organizations face a multitude of complex security challenges. All too often organizations rely on ad-hoc, reactive security measures, this is neither effective nor efficient. The Foundational Enterprise Security Architecture proves its value to organizations looking to quick-start and mature their capabilities.

Security architecture results in answering the four foundational questions asked by Governance and aligning the value stream in the context of risk management, specifically the reduction of risk to an organization.

Figure 2 – Value of Enterprise Security Architecture

To help ensure our organization's efforts are aligned, effective, and valuable, we need to not only think about what we do, but *how* we do it and *why* it matters. We need to have a clearly defined understanding of how our day-to-day tasks support the big picture.

> **Are we doing the right things?** This question addresses **Strategic Alignment**, ensuring initiatives support organizational objectives. It focuses on making sound investment decisions, reducing risks, and meeting compliance requirements. For example, governance ensures that measures align with business goals through frameworks like NIST CSF or strategic roadmaps.

Are we doing them the right way? This question reflects **Process Integrity**, operationalizing strategy through mature processes and structured methodologies. Governance ensures that accountability is upheld and activities are assigned to the appropriate individuals under proper oversight. Using frameworks like COBIT ensures that governance standards are consistently applied.

Are we getting them done well? This question focuses on **Performance Management**, ensuring that initiatives meet defined standards and achieve measurable outcomes. Efficient operations within defined risk appetite and tolerance are critical. Governance frameworks, such as COBIT 2019 and ISO 27001, enable organizations to monitor and improve execution quality.

Are we getting the benefits? This question is related to **Value Delivery**, ensuring our organization derives actual benefits from investments. Governance focuses on balancing the right mix of skilled personnel and resources to operate efficiently within risk criteria. Metrics and KPIs provide clear evidence of the value delivered.

The goal of this framework is to provide practitioners who may be struggling with any number of constraints with a structured and holistic approach to security, aligning it with an organization's business objectives. By tailoring and adopting FESA your enterprise can achieve several key benefits:

Strategic Alignment Designed to close the gap between business and security strategies, it enables organizations to identify and prioritize security objectives that directly support core business goals. This alignment ensures that security investments are purposeful and risks are effectively managed, positioning the organization for greater efficiency, scalability, and consistency.

Risk Management Allows organizations to systematically identify, assess, and mitigate risks. It helps in fostering a risk-aware culture and ensures that security measures are proportional to the actual threats and vulnerabilities an organization faces.

Flexibility and Adaptability This approach was designed to be tailored, flexible and adaptable. It can be customized to fit the unique needs and requirements of any organization, regardless of size or industry. This adaptability ensures that the security architecture remains relevant and effective as the threat landscape evolves.

Communication and Collaboration Using this approach to Enterprise Security Architecture should foster open collaboration among different departments and stakeholders, both internal and external, to the organization. Our goal is to provide a common language and framework for discussions about security (and by extension business risks), enabling more effective communication with all participants who play a role in enterprise security.

Compliance and Governance Most organizations have some driver to meet regulatory compliance requirements, this requires us to establish strong governance structures. This framework should support the development and maturation of security policies, procedures, and controls that are in line with industry standards and legal mandates.

Return on Investment Ultimately, we must act as responsible stewards of our organization's trust, resources, and finances. Leveraging this framework to initiate Enterprise Security Architecture should help optimize the use of security resources, ensuring that security investments are cost-effective, provide a clear return on investment and deliver tangible value. This approach helps prevent overspending on unnecessary security measures and focuses attention on what truly matters.

This framework should not be viewed solely as a *security thing* or an *Information Technology thing*; it's a strategic enabler. It empowers organizations to create a robust, adaptable, and most importantly a risk-aware security architecture that enhances their overall resilience and competitiveness. By aligning security with business objectives, managing risks more effectively, and promoting collaboration, FESA can be an indispensable tool for modern organizations seeking to secure their digital assets and ensure long-term success.

Difference between Business, Information Technology and Security Architectures

To ensure we properly level set expectations, let's quickly understand the differences between Enterprise Business Architecture, Enterprise IT Architecture, and Enterprise Security Architecture. It is these three essential aspects working together which result in ensuring effective and efficient operations within an organization, bringing about a proper balance between performance and conformance and delivering value.

Enterprise Business Architecture

The Enterprise Business Architecture focuses on the bigger picture, looking at the overall structure and organization of a business. Enterprise Business Architecture aims to align the business's strategic goals, processes, and functions to ensure efficiency and value delivery. It's all about optimizing the way a business operates, streamlining processes, and ultimately enhancing performance.

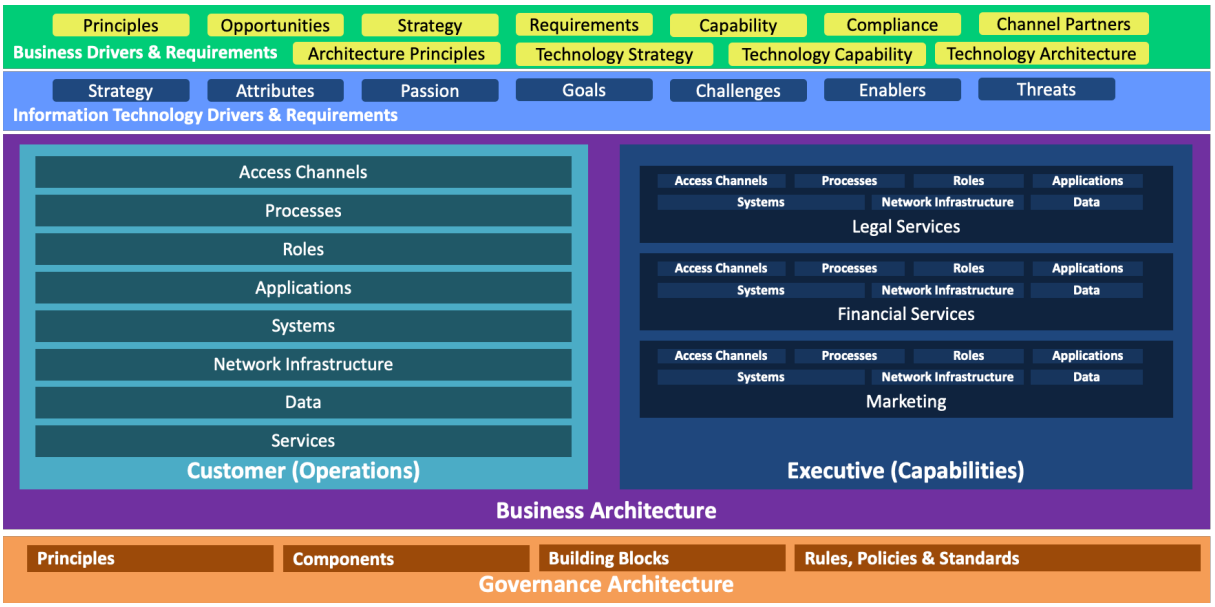


Figure 3 – Enterprise Business Architecture (example only)

Enterprise Business Architecture primarily focuses on the organization's business processes, strategies, and objectives. It aims to align business activities with the organization's goals and mission.

It serves as a strategic planning and management tool to ensure that the organization's business functions are optimized and efficient.

Enterprise Business Architecture includes components like business processes, organizational structure, roles and responsibilities, and business capabilities.

The goal of Enterprise Business Architecture is to improve business performance, enhance agility, and facilitate innovation by providing a clear understanding of how the organization operates and how it can achieve its objectives.

Enterprise Information Technology Architecture

IT Architecture is closely aligned with business architecture, focusing on the design and composition of an organization's technology infrastructure. This encompasses networks, servers, databases, and software applications. The goal of IT Architecture is to ensure that technology solutions are integrated with the business's needs and objectives, providing a robust technological foundation to effectively support the organization.

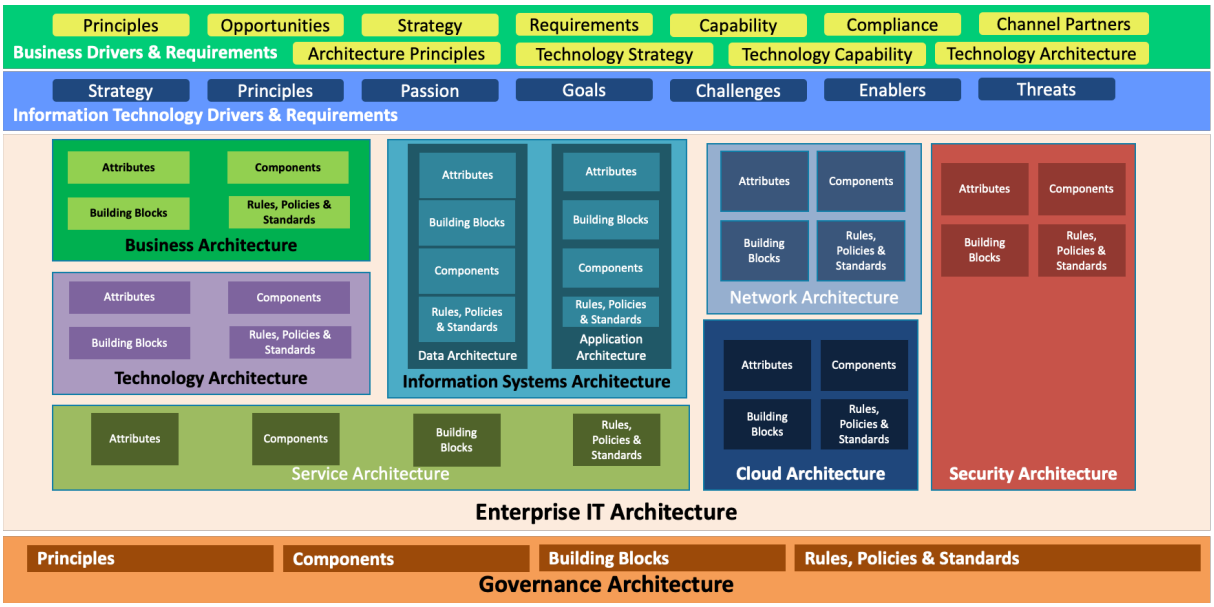


Figure 4 – Enterprise Information Technology Architecture (example Only)

Enterprise Information Technology Architectures tend to concentrate on the technology infrastructure and systems that support an organization's business operations. It encompasses the management of hardware, software, networks, and data.

Its purpose is to design and maintain an efficient and coherent IT environment that aligns with the organization's business needs. Leveraging existing IT capabilities to maximize returns while delivering core services.

Enterprise IT Architecture includes components like application architecture, infrastructure architecture, data architecture, and technology standards.

The goal of Enterprise IT Architecture is to ensure that the IT systems and solutions enable and support the organization's business processes, enhance productivity, gain efficiencies, and provide a foundation for innovation.

Enterprise Security Architecture (ESA)

Enterprise Security Architecture concentrates on safeguarding the organization. This involves identifying potential threats and their associated risks, defining security policies, and implementing reasonable and appropriate business controls[5]. While the primary focus is protecting data and systems ESA is often crucial for audit and compliance purposes as well.

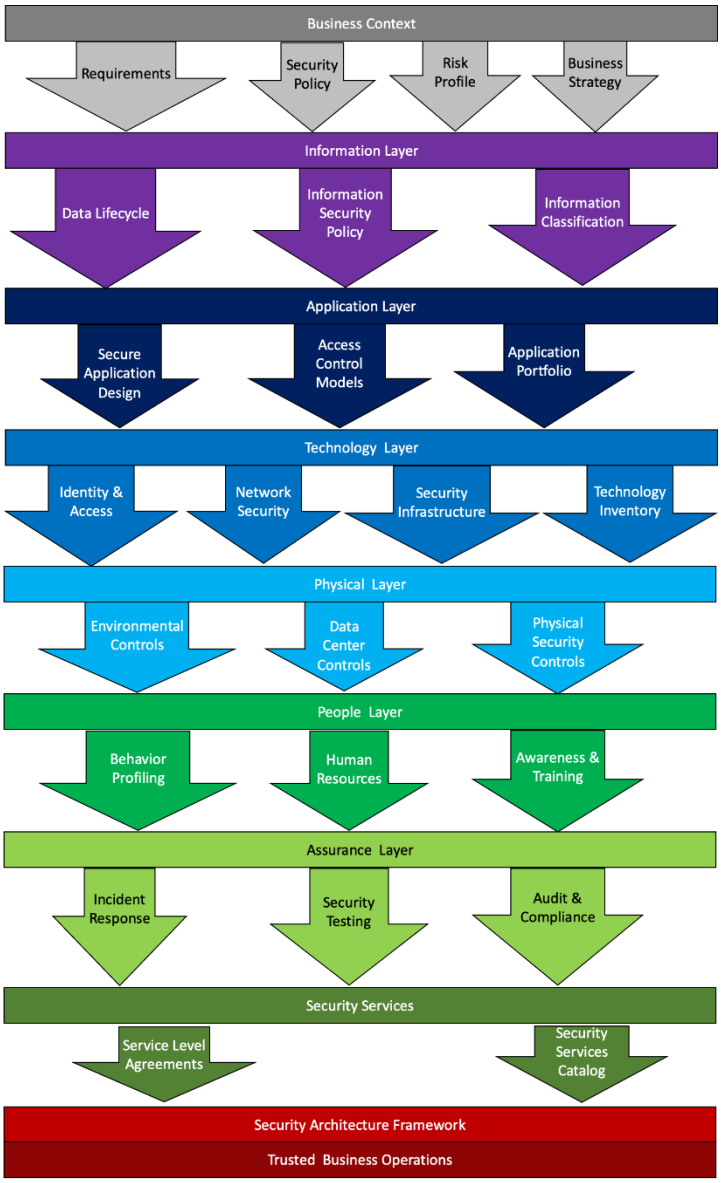


Figure 5 – Bringing it all together with FESA!

Enterprise Security Architecture often blends business and technology, to ensure the proper balancing and optimization of risks and resources in the pursuit of value.

ESA's purpose is to design and implement security (really business) controls, policies, and procedures that mitigate risks and vulnerabilities while aligning with the organization's business goals.

Enterprise Security Architecture includes components from both business (risk management strategies, business context and concepts, policies) and information technology perspectives (access controls, encryption, configuration management).

The goal of Enterprise Security Architecture is to provide a secure and resilient environment that protects sensitive data, ensures business continuity, and minimizes the impact of security incidents.

While these three architectures have distinct focuses, they are closely related and should work together to create a cohesive and effective framework that aligns an organization's business operations with IT capabilities and results in ensuring those capabilities are provided in a secure and efficient fashion to the appropriate stakeholders. These three facets, Enterprise Business Architecture, IT

[5] Each enterprise needs to define what is "reasonable and appropriate" given their industry, customers, geographic location, and jurisdiction.

Architecture, and Security Architectures ideally should operate in harmony with one another and support. When integrated properly, they ensure that the organization's technology infrastructure supports and aligns with broader business goals while maintaining the security and integrity of its operations.

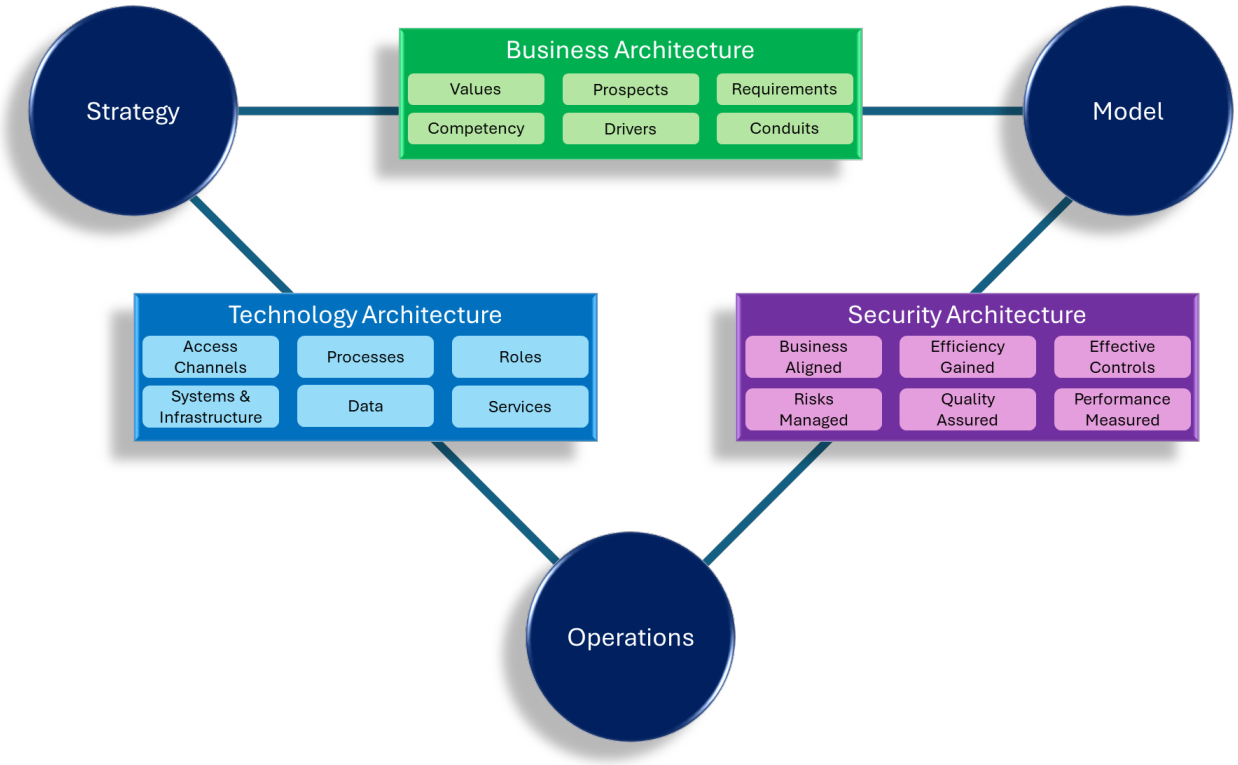


Figure 6 – Harmonizing Architectures

Foundational Enterprise Security Architecture

This publication was developed from observations made while actively engaged with organizations, both big and small, in a variety of capacities across multiple industries – both from internal and external perspectives.

- Audits & Assessments
- Business-IT Alignment Reviews
- Business Process Engineering
- Compliance Assessments
- Digital Transformation Projects
- Incident Response
- Information & Cybersecurity Advisory
- IT Modernization
- Network Operations Management
- Penetration Testing
- Secure Software Development

- Security Architecture
- Solutions Engineering
- Security Operations Management

The common themes and trends observed were predominately derived in context of Incident Response, Digital Transformation, Business Process Engineering, and IT Modernization efforts where fundamental information was not readily available. More concerning was that staff were often unsure or unaware of where or how to get the information.

How the Foundational ESA Aligns Security Strategy to Business Objectives

Adopting the Foundational Enterprise Security Architecture (FESA) safeguards you against your security initiatives being siloed or being done in a vacuum. Instead, it fosters inclusion with the broader business objectives and integrates security into the overall strategy. This integration allows for a proactive, business-driven approach to managing security risks, addressing compliance requirements, and improving operational efficiency.

Governance and Leadership Alignment

From the start, Foundational ESA focuses on governance and business leadership involvement. By establishing a structured framework, Foundational ESA involves key stakeholders and strives to get them actively involved in the security (risk) decision-making process. This framework bridges the gap between security and business teams, enabling security strategies to be directly informed by the organization's strategic goals - not only enhancing communication between security and business units, but also ensuring security investments are prioritized based on their impact on business operations.

Risk Management Tailored to Business Needs

One of the primary functions of FESA is to align security (risk) management with the organization's unique business risks. Traditional security approaches often focus solely on technical vulnerabilities, leaving business risks inadequately addressed. The Foundational ESA, on the other hand (wait for it), facilitates the identification of risks that are directly tied to business-critical processes and assets. By prioritizing risks based on their potential to disrupt key business functions, Foundational ESA ensures that resources are allocated where they will have the greatest strategic impact. What this means is that we're creating a risk (security) management program that not only protects the organization from threats but also supports business continuity and resilience.

Strategic Integration of Security and IT

In adopting, implementing and integrating FESA, security should no longer be viewed as a separate function from IT operations or business development. Rather, it is embedded into the lifecycle of IT systems and business processes (ideally, it should become a "*Business as Usual*" effort). FESA encourages the alignment of IT architecture and business control objectives with broader business goals, ensuring that every technological initiative, from digital transformation projects and cloud adoption to incident response and disaster recovery, incorporates business

risks and considerations from the outset. This integration allows businesses to innovate with confidence, knowing that security is built into their systems rather than bolted on as an afterthought.

Enhanced Compliance and Business Accountability

The Foundational ESA can also be used to address ever-growing regulatory pressures. Not only does FESA align security practices with compliance requirements, as it captures (and demonstrates) claims of conformance in a way that supports the business's operational goals; FESA also traces architectural decisions back to business drivers and enterprise strategy. Many organizations struggle to meet compliance standards in a manner that supports business agility. With FESA, compliance is embedded into the overall security architecture, ensuring that requirements defined by GDPR, HIPAA, PCI DSS, or any other industry-specific requirements are met without sacrificing business efficiency. This not only reduces the risk of regulatory penalties but also enhances the organization's ability to maintain trust with customers and stakeholders.

Continuous Improvement Driven by Business Objectives

The FESA framework incorporates continuous improvement processes, enabling organizations to adapt their security posture in response to evolving business needs and emerging threats. Regular after-action reviews and feedback loops ensure that the security strategy remains aligned with business objectives. This adaptability is crucial in today's dynamic threat landscape, where both business priorities and risks are constantly changing. Continually monitoring and optimizing security practices, FESA ensures that security not only protects the organization but actively enables and supports its long-term growth and success.

FESA facilitates the alignment of security strategy with business objectives by embedding governance, risk management, IT integration, compliance, and continuous improvement into a cohesive framework. This ensures that security is not merely a technical function but a business enabler that supports the organization's strategic vision.

Use Case (FESA in Action): FESA Adoption at Midwest Legal Services

Background

Midwest Legal Services, a regional law firm providing legal representation in areas such as Workers' Compensation, Personal Injury, Employment and Labor Law, Social Security Disability, Estate Planning, Bankruptcy, Foreclosure Defense, and Consumer Law embarked on a digital transformation initiative. The firm sought to modernize its operations by transitioning from on-premises systems to a cloud-based infrastructure, with two SaaS platforms (one for client case management and another for financial management). As part of the digital transformation, the firm adopted a zero-trust network design to secure its growing digital footprint. However, challenges related to compliance, client privacy protection, and integrating security into business operations prompted the firm to evaluate its overall security architecture.

Business Objectives

There were four (4) key business objectives driving digital transformation:

1. **Enhance Client Trust and Confidentiality:** Ensure robust protection of client information, especially given the handling of confidential, sensitive, and personally identifiable information (PII) within their case management and financial systems.

2. **Support Growth and Service Expansion:** Enable the firm's ability to expand beyond their four walls and provide onsite client services which would allow legal practices without compromising security or operational efficiency.

3. **Optimize Operational Efficiency:** Reduce the overhead and technical complexity associated with managing on-premises infrastructure, while improving system reliability, availability, and accessibility by staff and clients.

4. **Ensure Regulatory Compliance:** Maintain compliance with both state and American Bar Association requirements; this included both state-level privacy laws as well as Federal laws like the Health Insurance Portability and Accountability Act (HIPAA), not to mention the requirements for financial data.

Challenges

While the firm's transition to cloud and SaaS services provided operational benefits, it exposed gaps in how security aligned with business objectives:

- **Data Protection:** The firm faced increased risks due to the sensitivity of client data and the potential for breaches that could harm the firm's reputation, erode client trust, result in censures, and potentially disbarred attorneys.

- **Compliance:** The decentralized nature of cloud and SaaS services made it challenging to maintain consistent compliance across multiple regulatory frameworks. Harmonizing business controls became crucial to ensure that requirements were not only designed in but were demonstrable.

- **Security Silos:** Security was treated as an IT responsibility rather than a business priority, which led to insufficient collaboration between the firm's senior leaders, staff employees and the IT team.

Adoption

To address these challenges, *Midwest Legal Services* adopted the Foundational Enterprise Security Architecture (FESA) to align their security strategy with business objectives. FESA provided a structured and flexible approach tailored to the firm's needs, focusing on governance, risk management, and security integration across the organization's operations.

Mapping Security Strategy to Business Objectives

1. **Enhancing Client Trust and Confidentiality**
    - **FESA's Role:** FESA introduced a zero-trust architecture model to support the firm's operations. This ensured that only staff who were authorized could access client data and systems, using thin-clients, hardware multi-factor authentication (MFA), encryption, and real-time monitoring of access points. By embedding security at every layer of the firm's technology stack, FESA helped build stronger data confidentiality controls, which aligned directly with the firm's objective to protect client trust.
    - **Business Alignment:** Through improved access controls and data encryption, *they were* able to demonstrate that sensitive information was securely protected, enhancing their reputation for trustworthiness in legal matters.

2. **Ensuring Regulatory Compliance**
    - **FESA's Role:** FESA's risk management framework included compliance-focused security controls, such as audit trails, policy enforcement, and regular risk assessments. These capabilities were integrated with the firm's case management and financial systems to ensure consistent adherence to HIPAA and state privacy laws.
    - **Business Alignment:** By embedding compliance checks into routine processes, FESA reduced the burden of regulatory audits and helped the firm meet their obligations without interrupting operations, supporting the objective to ensure compliance efficiently.

3. **Supporting Growth and Service Expansion**
    - **FESA's Role:** FESA facilitated the secure scaling of the firm's cloud infrastructure as onsite client services and remote support were added. The architecture design allowed for the incremental adoption of security controls, ensuring that as the firm expanded, security remained proportionate and aligned with the firm's growth strategy.
    - **Business Alignment:** By aligning security with operational scalability, the firm could confidently expand its services, knowing that FESA's security provisions could grow alongside the business without introducing new risks.

4. **Optimizing Operational Efficiency**
    - **FESA's Role:** The architecture also optimized internal processes by automating monitoring, incident response, and access management across the firm's cloud and SaaS services. This automation reduced the burden on the IT team and allowed them to focus on higher-priority tasks, such as system optimization and service reliability.
    - **Business Alignment:** With security embedded into operational processes, the firm achieved greater efficiency in managing its IT resources, lowering operational costs, and ensuring consistent service delivery to clients.

Outcome

The adoption of FESA resulted in a holistic security strategy that fully supported the firm's business objectives. By mapping security initiatives directly to business goals, the firm improved client trust, maintained demonstrable compliance, enabled scalable growth, and optimized its digital transformation efforts.

The firm also realized tangible benefits:

- **Decreased risk of data breaches**, protecting sensitive client information.
- **Improved regulatory compliance**, with fewer compliance gaps and smoother audit processes.
- **Increased operational efficiency**, with more streamlined IT operations.
- **Successful business expansion**, supported by scalable security solutions.

The following table is provided to help illustrate how FESA strives to align with business objectives, from the perspective of the before and after views:

Aspect	Before FESA	With FESA Guidance
Security Governance	Disconnected from business strategy. Security decisions made in silos.	Integrated with executive leadership. Business and security align through governance structures.
Risk Management	Reactive and disjointed. Focus on compliance rather than business risks.	Proactive and business driven. Risk management is aligned with business-critical assets and goals.
Stakeholder Involvement	Minimal engagement from business leaders.	Business leaders actively participate in security strategies and decisions.
Security Operations	Security operates separately from business units, with little collaboration.	Security is embedded in business processes, fostering collaboration between IT, security, and business teams.
Compliance	Compliance is approached in a fragmented manner, increasing risks.	Compliance is integrated into security strategies, meeting regulatory and business objectives.
Incident Response	Incident response is slow and misaligned with business continuity.	Incident response is integrated with business continuity plans, ensuring rapid, business-aligned actions.

Table 1 – Foundational ESA (Before & After perspectives)

Framework Structure

The FESA framework consists of the following eight categories:

- Business Context
- Information
- Application
- Technology
- Physical
- People
- Assurance
- Services

This framework is intended to build and establish Fundamental Enterprise Security Architecture's formal deliverable, using a practical approach to adopting architecture, starting with Business Context and concluding with the delivery and assurance of Security Services.

To illustrate this concept, the following is provided to show each of the Foundational Enterprise Security Architecture respective layers.

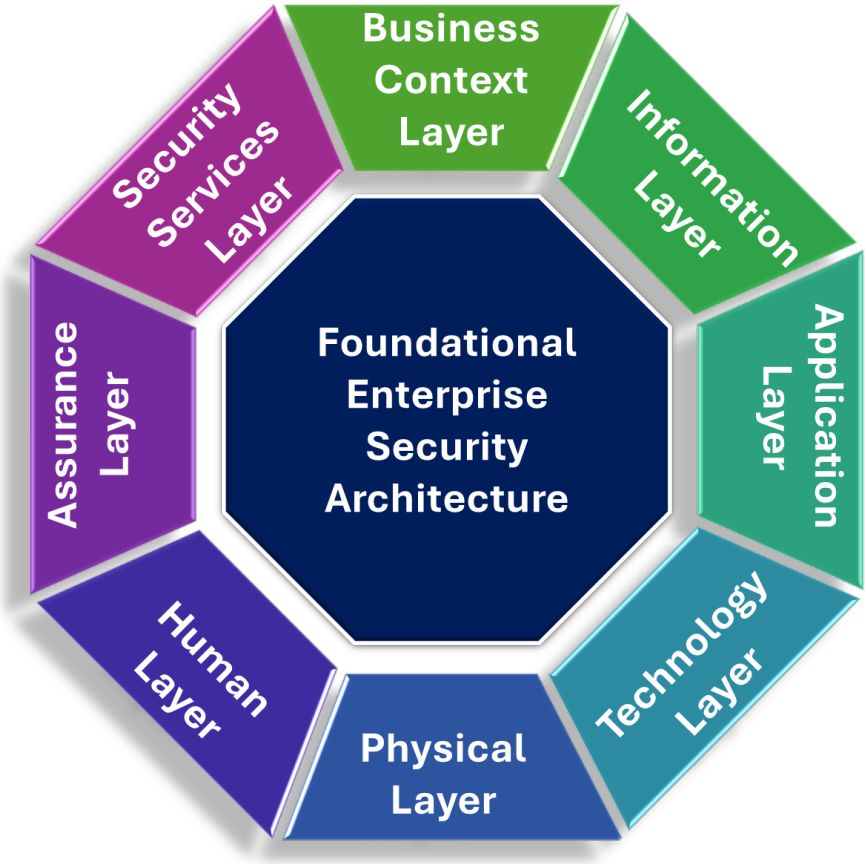


Figure 7 – Foundational Enterprise Security Architecture Model

Rationale behind "Foundational ESA"

Enterprise Security Architecture is so much more than just diagrams (Visio or otherwise) as it encompasses an approach to safeguarding an organization's assets and technology infrastructure. It is the combination of holistic, strategic, and operational views of security by the organization.

Imagine your organization as a fortress and your data and technology systems are the valuable treasures stored inside. You need to protect those treasures from potential threats like criminals, malware, and data breaches. To do this effectively you build strong defenses - our enterprise security architecture. Let's walk through the various components:

Policies & Procedures: Policies represent management's commitment to security, while procedures outline the specific actions needed to achieve security goals. Together, these written rules and activities define how assets are managed, determine access rights, and outline incident response processes. They set expectations for behavior and enable enforcement of security standards.

Perimeter/Boundary Security: This corresponds to 1) knowing where your perimeter and boundaries are, and 2) the security measures that are available in your arsenal to protect your assets. These control who can access your network and how data is handled.

Authentication & Authorization: Access control mechanisms authenticate users and grant permissions based on defined roles and responsibilities. This ensures that only authorized personnel can access data and systems.

Encryption & Data Loss Prevention: The logical controls that are used to safeguard sensitive data and information. These technologies need to be configured so even if your defenses are breached, the attacker can't easily make sense of or exfiltrate data without setting off alarms.

Incident Response & Monitoring: Despite your best efforts, the organization will suffer a breach or other attacks. Just as we have law enforcement who patrols and responds to threats, enterprise security architecture includes incident response plans and continuous monitoring measures to help identify and respond to security incidents swiftly.

Security Awareness & Training: Security awareness and training programs ensure that staff[6] understands the threats that exist, know to follow security policies, how to follow procedures, and can recognize & report threats promptly.

[6] While we say staff, we mean anyone who has access to systems, data, and information. This could be full-time employees, contractors, or other 3rd parties.

Compliance & Risk Management: Numerous laws and regulations may govern our organization's operations, and non-compliance can expose us to unnecessary risks[7]. Therefore, regularly evaluating compliance with industry standards and governmental regulations is essential. Effective risk management involves identifying potential threats, evaluating their impact, and implementing strategies to respond to them.

Security Architecture Governance: Having a leadership structure, which we are responsible and accountable to, provides us with the appropriate governance and oversight. This involves defining responsibilities, assigning roles, and ensuring that the security strategy aligns with the organization's goals. Additionally, this ensures that we maintain continued alignment with the needs of the organization, as we cannot be expected to govern ourselves effectively.

Enterprise Security Architecture Instrumentation & Tooling

Enterprise Security Architecture is truly a multifaceted discipline that combines people, processes, and technologies. As such, as a conductor, it orchestrates various instruments to protect an organization from a wide range of threats and risks. So, what instrumentation and tooling do you need to develop a Foundational Enterprise Security Architecture?

The following table identifies some of the tools we have found to be beneficial[8] in developing, maintaining, and managing Enterprise Security Architecture development efforts:

Tool	Purpose	Examples
Enterprise Architecture Tools	Help create and manage comprehensive architectural models that include security components. They facilitate the documentation and visualization of the ESA.	• Microsoft Word • Rubicon's FESA Templates • Archi – Architecture Modeling • yEd – Process Mapping • Visio – Data Flow Diagrams
Security Policy	Establishes a unified framework to protect an organization's information assets, ensuring compliance, mitigating risks, and promoting a security-conscious culture across all levels.	• SANS Information Security Policy • Information Security Policies Made Easy
Compliance Management Tools	Enable organizations to define, enforce, and monitor security policies and ensure compliance with relevant regulations.	• SimpleRisk • Service NOW (GRC Modules)
Risk Analysis & Management Tools	Assist in managing security risks within the enterprise.	• OpenFAIR • Rubicon's HARM • NIST RMF • RSA Archer

[7] Failing to follow applicable standards can create business problems, even if they don't involve immediate security issues. For example, not meeting PCI requirements could at best mean having to accept higher interchange rates (increased costs) to losing the ability to accept credit cards (loss of revenue).

[8] This is not endorsement or recommendation, only examples.

Tool	Purpose	Examples
Governance Management Tools	Provides a holistic approach to governance, risk, and compliance activities inside the organization. Centralization and automation processes make it easier to assess, track and report on governance.	• COBIT 2019 • ISO 37000 • MetricStream • IBM OpenPages
Documentation & Collaboration Tools	Essential for creating, maintaining, and sharing ESA documentation, collaborating with stakeholders, and maintaining a knowledge repository.	• SharePoint • Confluence • Google Workspace
Project & Portfolio Management Tools	Manage security projects, allocate resources, track progress, and ensure that security initiatives align with the ESA.	• OpenProject • Monday.com • SmartSheet • Microsoft Project • Project365
Communication & Reporting Tools	Generate reports and visualizations to communicate the status of the ESA to various stakeholders effectively.	• R/RStudio • Microsoft PowerBI • Microsoft Word • Tableau • E-Mail

Table 2 – ESA Instrumentation Example

Security Services

Security Services are the combined set of fundamental practices, processes, activities, infrastructure, systems, and applications which play a vital role in protecting information technology assets and sensitive information in various contexts.

The following figure should illustrate the focus of these concepts:

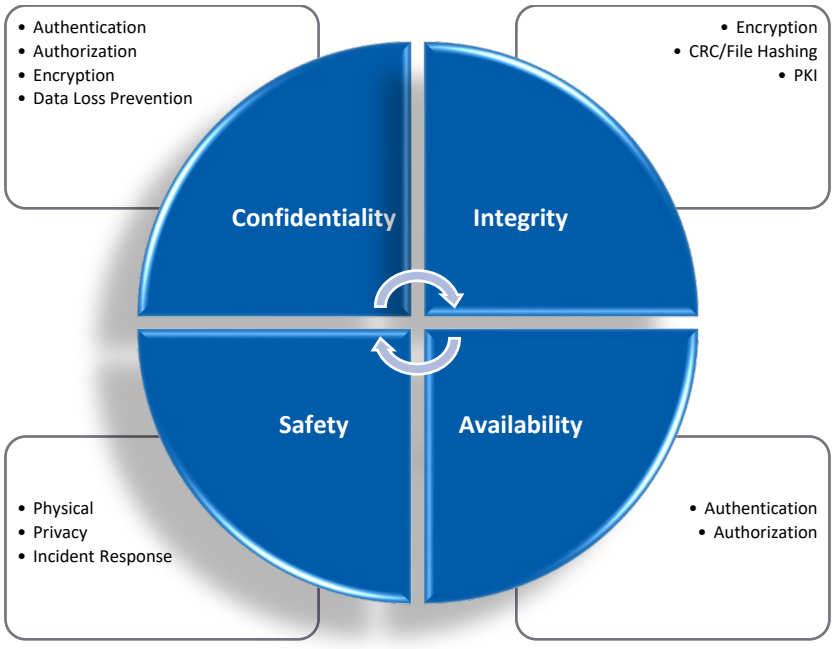


Figure 8 – Logical Security Services CISA Concept Model

These four (4) cores concepts are traditionally universally applicable, regardless of specific organization or industry particular frameworks, and are the desired outcomes of sound security practice.

The following table is provided to offer a more robust listing of Logical Security Services (LSS), mapped to these core concepts of the LSS CISA Concept Model.

Security Service	Primary Function	Secondary Function	Justification and Rationale
Access Control	Confidentiality	Integrity	Ensures confidentiality by restricting unauthorized access, and it also maintains data integrity by preventing unauthorized modifications.
Encryption	Confidentiality	Integrity	Safeguards confidentiality through data encryption. It also contributes to integrity by protecting data from tampering during transmission or storage.
Authentication	Confidentiality	Integrity	Validates user identity, emphasizing confidentiality. It also aids integrity by ensuring that data is accessed and modified by authorized individuals only.
Digital Signatures	Integrity	Authenticity	Verifies that data hasn't been altered. They also enhance authenticity by confirming the sender's identity.
Intrusion Detection and Prevention Systems (IDS/IPS)	Availability	Integrity	Identifies and mitigates threats. It supports integrity by detecting and responding to potentially harmful activities.
Security Information and Event Management (SIEM)	Integrity	Availability	Monitors for security incidents and aids availability by providing insights to maintain system functionality.
Data Loss Prevention (DLP)	Confidentiality	Privacy	Maintains confidentiality by preventing data leaks. It also respects privacy by safeguarding sensitive information.
Single Sign-On (SSO)	Confidentiality	Integrity	Promotes confidentiality through streamlined access. It supports integrity by ensuring users are authenticated for their sessions.
Public Key Infrastructure (PKI)	Integrity	Authenticity	Ensures the integrity of keys and certificates. It also enhances authenticity by verifying the identity of communication parties.
Identity and Access Management (IAM)	Availability	Confidentiality	IAM is vital for availability by efficiently managing user access. It also enforces confidentiality by controlling who accesses what resources.
Firewall	Confidentiality	Integrity	Firewalls aim at confidentiality by blocking unauthorized access. They also protect integrity by filtering out harmful traffic.
Antivirus, Anti-Malware, EDR, MDR, XDR	Integrity	Availability	Antivirus software maintains integrity by detecting and removing malware. It supports availability by preventing malware-induced downtime.

Security Service	Primary Function	Secondary Function	Justification and Rationale
Network Segmentation	Integrity	Confidentiality	Network segmentation enhances integrity by isolating network segments. It enforces confidentiality by limiting access between segments.
Secure Sockets Layer/Transport Layer Security (SSL/TLS)	Confidentiality	Integrity	SSL/TLS primarily secures confidentiality through encryption. It also validates data integrity during secure communications.
Virtual Private Network (VPN)	Confidentiality	Integrity	VPNs protect confidentiality by encrypting data in transit. They support integrity by ensuring data remains intact during transmission.
Penetration Testing	Integrity	Availability	Penetration testing assesses system integrity by identifying vulnerabilities. It ensures availability by mitigating potential threats and weaknesses.
Security Auditing	Integrity	Confidentiality	Security auditing focuses on integrity by monitoring system events. It maintains confidentiality by identifying access breaches and policy violations.
Security Patch Management	Integrity	Availability	Patch management safeguards integrity by applying updates. It ensures availability by preventing exploitation of known vulnerabilities.
Security Information Sharing and Analysis Centers (ISACs)	Availability	Safety	ISACs aim to enhance availability by sharing threat intelligence. They also respect privacy by sharing information responsibly and securely.
Threat Intelligence Services	Availability	Confidentiality	Threat intelligence services enhance availability by providing timely threat data and uphold confidentiality through secure sharing of sensitive information.
Security Policy and Procedure Management	Confidentiality	Integrity	Policy and procedure management ensures confidentiality by defining access rules. It also maintains integrity by specifying standards for secure practices.
Network Monitoring and Analysis	Availability	Integrity	Network monitoring enhances availability by proactively identifying issues. It maintains integrity by monitoring for unusual or unauthorized activities.
Web Application Firewall (WAF)	Confidentiality	Availability	Web Application Firewalls protect confidentiality by preventing web-based attacks. They enhance availability by safeguarding against downtime due to web vulnerabilities.
Secure Code Review	Integrity	Confidentiality	Secure code reviews assess code integrity by identifying vulnerabilities. They support confidentiality by ensuring secure handling of sensitive data.
Disaster Recovery Planning (DRP)	Availability	Safety	Disaster Recovery Planning ensures availability by preparing for and recovering from disasters.

Security Service	Primary Function	Secondary Function	Justification and Rationale
			It also prioritizes safety by protecting lives and physical resources.
Backup and Restore	Availability	Integrity	Backup and restore systems are critical for maintaining data availability. They also contribute to data integrity by providing data recovery options.
Incident Response	Availability	Safety	Incident response primarily focuses on restoring availability after an incident. It also respects safety (both privacy & kinetic) by handling incident data with care and conforming to the applicable requirements.
Security Risk Assessment/ inclusive of third parties	Integrity	Confidentiality	Security risk assessment examines system integrity by identifying vulnerabilities and threats. It maintains confidentiality by safeguarding risk assessment data.
Threat Modeling	Confidentiality	Integrity	Threat modeling secures confidentiality by identifying potential risks. It maintains integrity by modeling threats to anticipate and mitigate security concerns.
Network Access Control (NAC)	Availability	Integrity	NAC ensures availability by managing network access. It supports integrity by ensuring devices meet security policy requirements.
Secure File Transfer	Confidentiality	Integrity	Secure file transfer focuses on confidentiality by safeguarding data in transit. It also maintains integrity by ensuring data is transferred securely.
Security Awareness Training	Confidentiality	Safety	Security awareness training enforces confidentiality by educating users on security best practices. It respects privacy by emphasizing responsible data handling.
Secure Email Gateway	Confidentiality	Integrity	Secure email gateways primarily safeguard confidentiality by filtering malicious emails. They also maintain integrity by identifying email-based threats.
Mobile Device Management (MDM)	Confidentiality	Integrity	MDM enforces confidentiality by managing mobile device access. It supports integrity by controlling device security and data protection.
Cloud Access Security Broker (CASB)	Confidentiality	Safety	CASBs focus on confidentiality by securing cloud data and access. They also respect privacy by monitoring and controlling cloud-related activities.
Secure Shell (SSH)	Confidentiality	Integrity	SSH ensures confidentiality by encrypting terminal sessions. It maintains integrity by verifying host authenticity and securing remote connections.
Container & Virtualization Security	Integrity	Confidentiality	Enhances integrity by securing container and/or virtualized environments. It enforces confidentiality by managing access to containerized/virtualized applications.

Security Service	Primary Function	Secondary Function	Justification and Rationale
Security Token Service (STS)	Confidentiality	Integrity	Provides confidentiality by managing access tokens securely. It also supports integrity by ensuring token validity and usage tracking.
File Integrity Monitoring (FIM)	Integrity	Availability	Maintains integrity by monitoring file changes for signs of tampering. It supports availability by identifying issues that might affect data access and usability.
Secure Instant Messaging (SIM)	Confidentiality	Integrity	Secure IM promotes confidentiality by encrypting instant messages. It maintains integrity by ensuring message authenticity and integrity.

Table 3 – Security Services List

First steps into Enterprise Security Architecture

We are often asked “where should we start?” and “How do we implement Enterprise Security Architecture in a practical manner?” Well, it’s really easy - by taking your first step, right? The first step is understanding the goals of the respective layer of the model and capturing them.

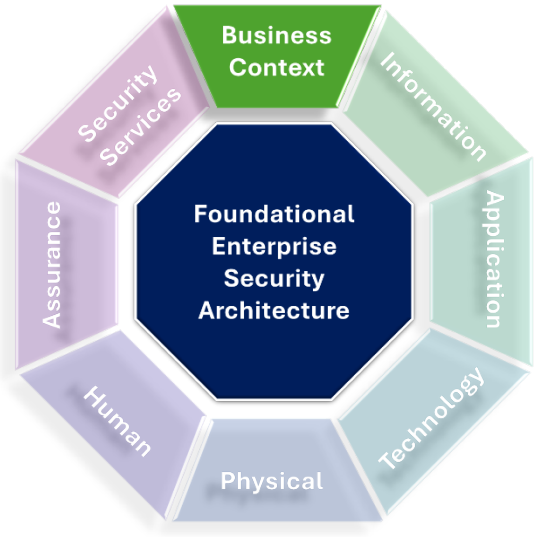
ESA truly is a hydra, as you have roles from Senior Management, the various lines of business (HR, Legal, Operations, etc.), and Information Technology that are attempting to work together towards the same goals for the organization. Understanding the enterprise’s strategy, goals and objectives is key. This is where knowing key stakeholders is vital for program success (see Appendix G for common stakeholder roles and responsibilities).

To achieve this, we’re going to walk through and provide information about each of those layers now and discuss some of the artifacts. This will conclude with another illustration of how these artifacts relate to one another and can be used to demonstrate alignment and justify investments in a fashion that, in the context of the organization, should reduce risk and enable the achievement of the organization’s strategic goals and objectives.

Each layer in this framework plays a very specific role, with the outcome being to build on the insights and information gathered in the previous step to enable and complete each subsequent step of the framework. This approach ensures that a holistic approach, aligned with business objectives, and tailored to the unique needs of the organization. Together, these layers create an inclusive security strategy which not only protects our assets but supports our organization’s mission.

So, with that, let’s begin with understanding the Business Context.

Business Context Layer



The Business Context layer sets the stage for all our efforts. It is within this layer that we collect vital information about our organization's business goals, strategies, and objectives. By understanding the big picture of our business first, we ensure that efforts will align with their goals.

This layer forms our foundation, ensuring that security isn't just a side concern but is embedded in our business strategy, allowing us to protect what matters most. Understanding the strategy and goals of the organization, first and foremost, will allow you to ensure proper alignment of the security practices with what the organization has defined.

As the foundation, we should capture and document the following four (4) artifacts ("deliverables"), which will then be used to guide and inform decisions relating to security practices, controls, and resource commitments:

Business Strategy Alignment: Ensure that the security strategy aligns with the overall business strategy. This artifact will be referenced to guide and inform resource planning and budgetary activities relating to security within the enterprise.

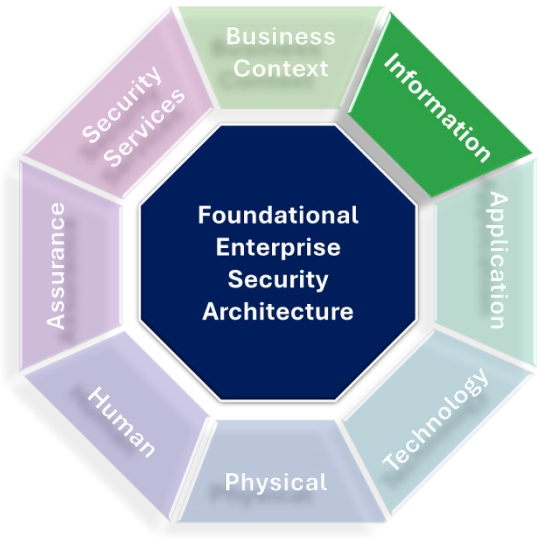
Business Risk Profile: Understand and capture the organization's business risk profile and priorities. This will identify those critical business processes and the IT systems which need to be protected.

Enterprise Security Policy: Establish high-level enterprise security policy and objectives based on business needs. This provides the guardrails we need to remain agile and flexible, as well as setting management's expectations on behaviors.

Business Requirements: Identify specific business requirements that need to be supported by security. Once we understand the business context, we should then be able to capture and verify the specific requirements needed by the business.

These four (4) artifacts, when tailored to the enterprise and completed, should provide sufficient Business Context needed to advance to the next layer.

Information Layer



Once we understand the Business Context, we can start moving around the wheel. Next, the Information Layer dives into the heart of our data and information assets. Here we gain an understanding of what information we have, its value, how it's used, how it needs to be protected and ensure proper handling.

By capturing information on various aspects, such as data sensitivity and classification, we gain the knowledge needed to protect our most critical assets effectively. This layer starts to bridge the gap between the Business Context and the Technical layers, ensuring that security measures are based on understanding our data and information.

This determines how information will be handled, protected and managed, in context of the enterprise and its drivers (both internal and external).

Here we should capture and document the following three (3) artifacts, which will be used to start laying the groundwork for all subsequent security practices, processes, technologies, in addition to assurances to Senior Management that risk is being managed in accordance with the defined enterprise risk profile.

> Information Classification: Classify data and information assets according to their sensitivity and criticality, this defines the business value of the assets. This should be used to establish minimum security controls based upon the respective classification level. The following is an example of data classification. Your mileage will absolutely vary depending on your organization.

Level 1 Public	Level 2 Private	Level 3 Confidential	Level 4 Secret	Level 5 Top Secret
Information intended and released for public use.	Information that may be shared only within the enterprise.	Confidential and sensitive information, intended only for those with a “business need to know."	High-risk information that requires strict controls.	Extremely sensitive information requiring specific controls and isolation from the network.
The enterprise intentionally provides this information to the public.	The enterprise chooses to keep this information private, but its disclosure would not cause material harm.	Disclosure of this information beyond intended recipients might cause material harm to individuals or the enterprise.	Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the enterprise.	Disclosure of this information could cause criminal liability; loss of insurability or employability; or severe social, psychological, reputational, financial,

Level 1 Public	Level 2 Private	Level 3 Confidential	Level 4 Secret	Level 5 Top Secret
				or other harm to an individual or group.
• Published research • Product catalogs • Published staff information • Enterprise directory information • Basic emergency response plans (life & safety) • Enterprise-wide policies • Enterprise publications • Press releases • Published marketing materials • Regulatory and legal filings • Published annual reports • Code contributed to Open Source • Released patents • Plans of public spaces	• Department policies and procedures • Employee web/intranet portals • Enterprise training materials • Pre-release articles • Drafts of research papers • Work papers • Patent applications • Non-public building plans or layouts (excluding L3 or L4 items) • Information about physical facilities (excluding L3 or L4 items) • non-sensitive administrative survey data	• Non-directory student information • Non-published faculty and staff information • UID tied to an individual • Personnel records • Non-public legal work and litigation information • Budget /financial transactions information • Non-public financial statements • Information specified as confidential by vendor contracts and NDAs • Information specified as confidential by Data Use Agreements • General security findings or reports (e.g. SSAE18, SOC2, PCI ROC) • Most enterprise source code • Non-security technical specifications/architecture schema • Sensitive administrative survey data (i.e., such as performance reviews or customer feedback, especially if free text response is permitted.	• Passwords and PINs • System credentials • Private encryption keys • Government issued identifiers (e.g. Social Security Number, Passport number, driver's license) • Individually identifiable financial account information (e.g. bank account, credit or debit card numbers) • Individually identifiable health or medical information • Individually identifiable research/development data • Details of significant security exposures within the enterprise (e.g. vulnerability assessment and penetration test results) • Security system procedures and architectures • Trade secrets • Systems managing critical Industrial & Operational Technology	• Research data classified as Level 5 by the ELT • Information or research under a contract stipulating specific security controls beyond L4

Table 4 – Example Information Classification Matrix

Figure 9 – How to Keep Focus on the Business

Information Security Policies & Procedures: Development of the policies and procedures needed to protect the assets. This is where granularity and focus on controls[9] is needed to protect the information with which we've been entrusted. Each control needs to be linked back to a defined risk, based on Information Classification and business value.

It can be very appealing to focus on the technical aspects of architecture – but that's just one aspect! As professionals, we need to focus on ensuring we keep sight of the business elements, properly aligning with and enabling the organization to achieve their strategy!

Data Lifecycle Management: Understanding and capturing how data is created, stored, processed, and disposed of should inform us of the best location to apply controls, the types of controls to be used (i.e., preventative, detective, corrective, etc.), based on the enterprise's defined Information Classification standard in accordance with jurisdictional[10], statutory and regulatory requirements.

[9] We define "control" as follows: "*The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature.*"

[10] We are not your lawyer, but we can introduce you to one if you need.

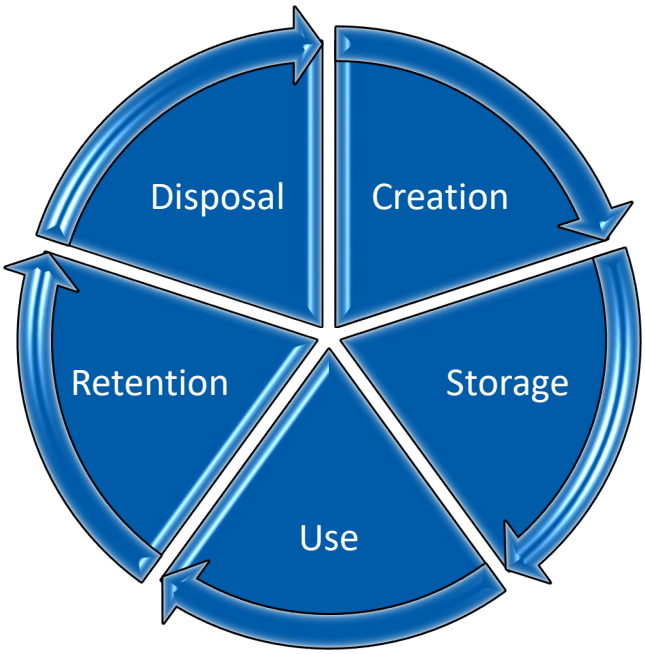


Table 5 – Data Lifecycle Management

The following illustrates the role each artifact provides in relationships and support of understanding the Business Context:

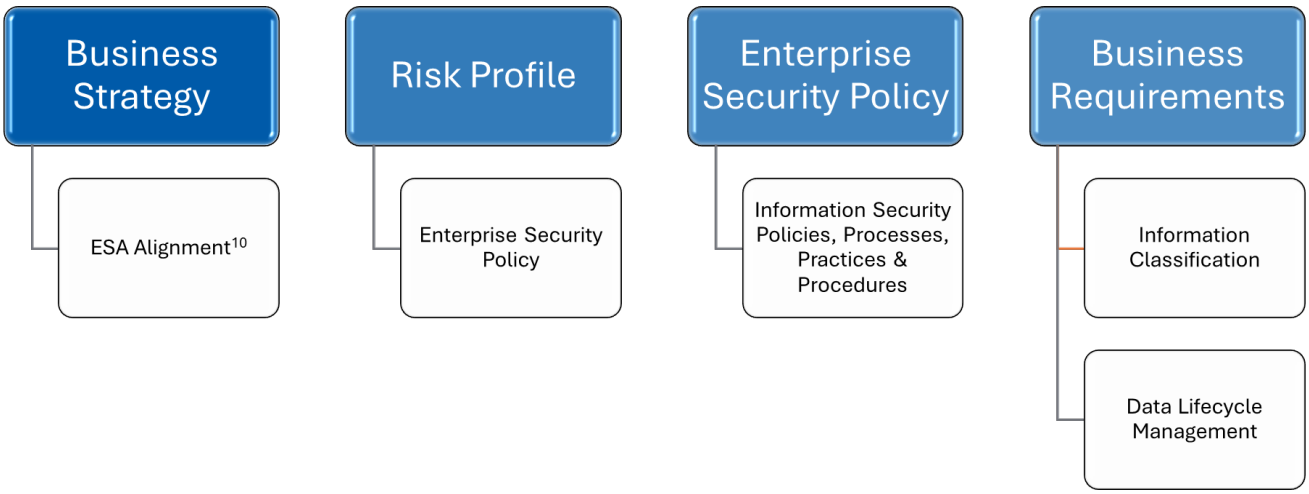


Figure 10 – Business Context Relationship with Information

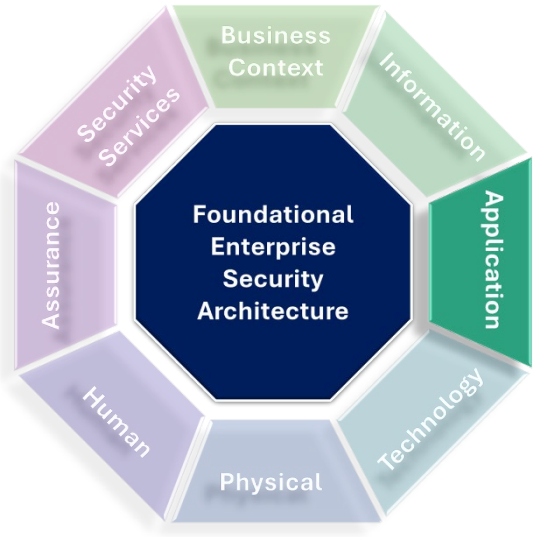
With regards (and to clarify) to the Enterprise Security Policy, no this is not a mistake (although it does appear to be a self-licking ice cream cone); in order to develop a suitable Enterprise Security Policy, it is strongly encouraged to align the policy with the enterprise's risk management program. Failure to do so may otherwise lead to ineffective or inefficient use of enterprise resources.

[11] ESA Alignment is an ongoing process

It is often debated as to whether the Enterprise Security Policy can be (or in most cases, has been) developed independent of the enterprise's risk management program, this process should be carefully reviewed and scrutinized. It has been our experience that when developed independently, the policy tends to be misaligned, in direct conflict and requires revisions to bring into alignment.

We know historically that operating independently or in a "vacuum" works out so well at the end of the day, right? We need to take every measure to prevent a siloed approach to security, as a "simple change" can have a wide-reaching range of impacts to the organization.

Applications Layer



As we continue around the wheel, our next layer is the Applications Layer. Here we focus on the software systems that are used to drive our business processes, automate and batch repetitive & mundane tasks, and increase efficiencies. This layer involves collecting information about and understanding our applications, their functionality, and how they handle data.

By understanding the applications that support our business, we can design security measures that align with specific or unique requirements and the challenges of our software systems.

At this layer, you should capture and document the following three (3) artifacts, which will be used to address subsequent security practices, processes, technologies needed to protect the information we've been entrusted with, wherever it is stored, processed, transmitted/shared, or accessed.

Application Portfolio: Inventory and assess the organization's applications in terms of security requirements.

Access Control Models: The access control mechanisms used for our applications. These can be either Mandatory Access Controls (MAC), Discretionary Access Controls (DAC), or Role-Based Access Controls (RBAC). The following provides a summary of each of these models.

Feature	Mandatory Access Controls (MAC)	Discretionary Access Controls (DAC)	Role-Based Access Controls (RBAC)	Attribute-Based Access Controls
Access Determination	Based on security labels and levels.	Determined by data owners or administrators.	Based on user roles and responsibilities.	Policies evaluate attributes of users, resources, and environments for access decisions.
User Discretion	No user discretion: system enforced.	User/administrator has discretion.	Limited discretion based on role.	User defined policies
Access Control Mechanism	Security labels, clearances, and sensitivity levels.	Access Control Lists (ACLs) and object ownership.	User roles and associated permissions.	Policies based on attributes (e.g., user roles, resource classifications, environmental factors) determine access.
Complexity	Can be complex due to strict adherence to security labels.	Moderately complex, as it requires manual management of ACLs.	Simplifies access management by grouping permissions.	ABAC allows for the creation of complex access control rules that are tailored to an organization's security needs and compliance requirements.
Use Cases	Government, military, highly secure environments.	General business applications, small to medium-sized organizations.	Medium to large organizations, access delegation.	Fine-grained access control scenarios where access needs are based on multiple dynamic factors.
Example	A top-secret document can only be accessed by users with a top-secret clearance.	A file owner can grant read access to specific users.	Users in the HR role can access employee records.	A user with a "Manager" role can access financial data only during office hours from a company device.

Table 6 – Access Control Models

Secure Application Design: Define secure coding practices and design principles to be followed when developing applications. The common key principles associated with protecting both data and systems are described as follows:

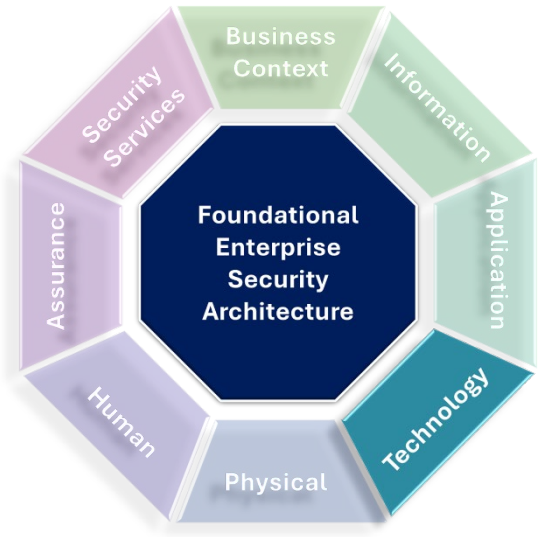
Principle	Description	Reference
Least Privilege	Limit access and permissions to the minimum necessary. Use RBAC.	*NIST SP 800-53* *OWASP Application Security Verification Standard* *ISO 27001 – A.9.2 – User access management* *CIS Top 18 CSC - #6 Access control management*
Defense in Depth	Implement multiple layers of security controls.	*NIST SP 800-53* *NIST SP 800-160* *OWASP Application Security Verification Standard* *ISO/IEC 27002* *MITRE ATT&CK Framework*
Secure by Default	Configure applications and systems to be secure by default.	*NIST SP 800-53* *OWASP Application Security Verification Standard* *Microsoft Security Development Lifecycle (SDL)*
Data Encryption	Encrypt sensitive data at rest and in transit.	*FIPS 140-2* *NIST SP 800-53* *NIST SP 800-175* *OWASP Cryptographic Storage Cheat Sheet* *OWASP Transport Layer Protection Cheat Sheet* *PCI DSS v4.0*
Input Validation and Sanitization	Validate and sanitize all user inputs to prevent vulnerabilities.	OWASP Developer Guide OWASP Top 10 *OWASP Application Security Verification Standard* SAFECode Guidelines
Authentication and Authorization	Use strong authentication and implement proper authorization.	*NIST SP 800-63* *OWASP Authentication Cheat Sheet* *OWASP Application Security Verification Standard*
Secure Coding Practices	Follow secure coding guidelines and avoid hardcoding sensitive data.	*OWASP Secure Coding Practices Quick Reference Guide* *OWASP Developer Guide* *SEI CERT Coding Standards*
Error Handling and Logging	Implement proper error handling and secure logging practices.	OWASP Logging Cheat Sheet OWASP Application Logging Vocabulary Cheat Sheet
Threat Modeling	Conduct threat modeling to identify potential security threats.	NIST SP 800-154 OWASP Threat Modeling Cheat Sheet
Secure APIs	Secure APIs and web services with authentication and encryption.	NIST SP 800-92 OWASP API Security Top 10 OWASP REST Security Cheat Sheet

Principle	Description	Reference
Secure File and Resource Handling	Prevent insecure file operations and limit access to system resources, validate any included remote assets/libraries from 3rd parties or content delivery networks (CDNs).	OWASP File Upload Cheat Sheet OWASP Path Traversal Cheat Sheet
Session Management	Use secure session management techniques to prevent session-related attacks.	NIST SP 800-63 OWASP Session Management Cheat Sheet
Privacy by Design	Prioritizes the inclusion of privacy features and protections from the outset	ISO/IEC 29100 NIST Privacy Framework ISACA Privacy by Design and Default Primer

Table 7 – Secure Application Design Principles

URLs to the references are provided in *Appendix D – Secure Application Design Resources*.

Technology Layer



This layer builds upon the previous layers and dives into our technology infrastructure. Here we collect information about the hardware, networks, and systems that underpin the enterprise's operations. This knowledge helps us secure our technology assets effectively.

By ensuring the security of our IT environment, we create a solid and robust foundation for improved security posture. After all, we can only protect what we know about.

In this level, we capture and document the following four (4) artifacts, which not only identifies the systems where data and information reside within the enterprise[12], but also the available controls & standards present, security management and identities of those who access those systems, data, and information assets.

> Technology Inventory: Identifying and assessing the organization's technology infrastructure is crucial for effective IT Asset Management. This process involves creating a comprehensive inventory of all hardware, software, network components, and data repositories. Classifying assets based on their criticality to business operations and data sensitivity ensures that the most important assets are prioritized for protection.

[12] Understanding that when we use the term "enterprise" we are defining this as "the boundaries of our organization's operations and are inclusive of data centers, mobile devices, WFH, and cloud environments.

Maintaining an up-to-date and accurate inventory is vital for Configuration Management. This involves keeping records of asset configurations (e.g., versions, patch levels, and dependencies), and storing this data – ideally in a Configuration Management Database (CMDB). Continuous monitoring and reporting tools are also necessary to not only track assets but to capture performance, availability, and security status, providing regular reports to offer visibility into the environment's health and security posture.

Security Infrastructure Design: Developing and ensuring the requirements are formalized for establishing, implementing, maintaining, and improving security infrastructure is critical for managing security operations effectively. This involves defining security requirements for all technology components based on business needs, regulatory requirements, and risk assessments, covering aspects such as confidentiality, integrity, availability, and compliance.

Adopting a security architecture framework (like FESA) helps guide the design and implementation of security infrastructure, ensuring alignment with the organization's overall enterprise architecture. Standardization of technology components is also vital, ensuring consistency and interoperability across the IT environment. Documenting security policies, procedures, and guidelines is necessary for managing operations effectively.

Network Security Architecture and Controls: Defining network security architecture and controls to protect the organization's network from threats and vulnerabilities is essential. This involves designing the network to segment critical systems and data from less sensitive areas, using VLANs, subnets, and firewalls to enforce segmentation. Deploying robust perimeter defenses, such as firewalls, intrusion detection/prevention systems (IDS/IPS), a
nd DDoS protection, helps protect against external threats.

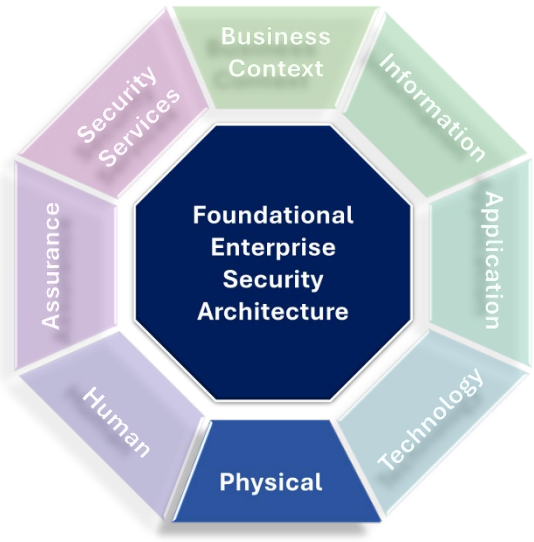
Internal security controls, such as network access control (NAC), VPNs, and endpoint security solutions, are also necessary to safeguard internal network traffic. Regularly monitoring internal network traffic for signs of malicious activity or policy violations helps identify potential threats early. Enforcing strict access control policies for network devices and systems, using role-based access control (RBAC) and least privilege principles, minimizes the risk of unauthorized access.

Identity and Access Management: Establishing unique identifiers for user and device authentication, authorization, and management processes is crucial for ensuring secure access to systems and data. Implementing multi-factor authentication (MFA) for all user accounts, especially those with elevated privileges, enhances security. Strong, unique passwords should be enforced and mandatorily changed if there is any evidence of compromise.

Defining and enforcing access policies based on user roles and responsibilities ensures that users only have access to the resources they need. Regularly reviewing and updating access permissions helps keep them current and appropriate. Maintaining a centralized directory service to manage user identities, access and automating the provisioning and de-provisioning of user accounts, ensures timely and accurate access management.

Implementing device authentication mechanisms ensures that only authorized devices can access the network. Using Mobile Device Management (MDM) and Endpoint Detection and Response (EDR) solutions help manage and secure devices, providing additional layers of protection for the organization's IT environment.

Physical Layer



This layer takes us from the logical environment into the physical world, where our business operates. Here, we collect the relevant information about our facilities, locations, and assets that house our technology.

Understanding the physical security requirements ensures that we protect our infrastructure and data from threats that may originate from the physical world.

At this layer, the following three (3) artifacts are captured and documented, this is to ensure physical security is not forgotten.

Physical Security Controls: Defines the physical security measures used to protect facilities and assets.

Data Center Security: Security mechanisms used to secure data centers and physical infrastructure.

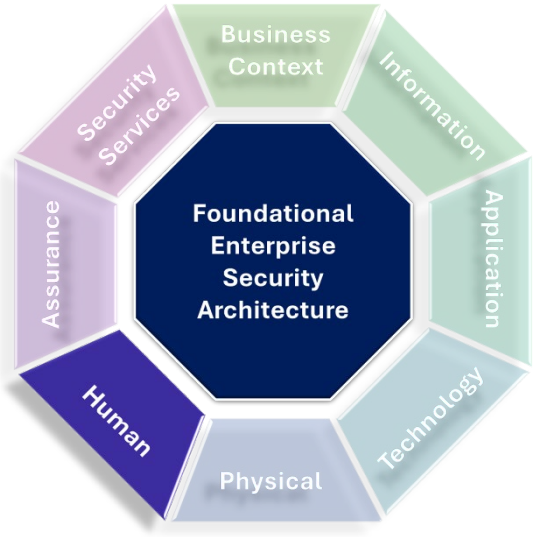
Environmental Controls: Ensure appropriate environmental conditions are maintained and properly managed for technology equipment.

Even though most operations reside within the realm of Information Technology systems, we cannot forget the following considerations:

1) People, being tactile in nature, still like to print things out.

2) People are human, and will cause an incident (e.g., spilling coffee on laptops[13], leaving coffee-soaked laptops on planes, etc.).
3) Criminals are going to criminal; they are just as likely to exploit a vulnerability in a website the same as walking in and stealing a coffee-soaked laptop.

Human Layer



As we continue around, we come to the Human Layer where we focus on the human factors which influence security efforts. This layer involves collecting information about the users of our systems.

By understanding those who interact with our technology and the data and information we are entrusted to protect, we can establish reasonable and appropriate access control mechanisms, aligning security with the specific needs and responsibilities of individuals.

At a foundational level, you should capture the following three (3) artifacts. We will need to ensure that those who have access to information are properly trained, that we're not inviting disaster, and that we proactively ensure abuse is minimized as much as possible.

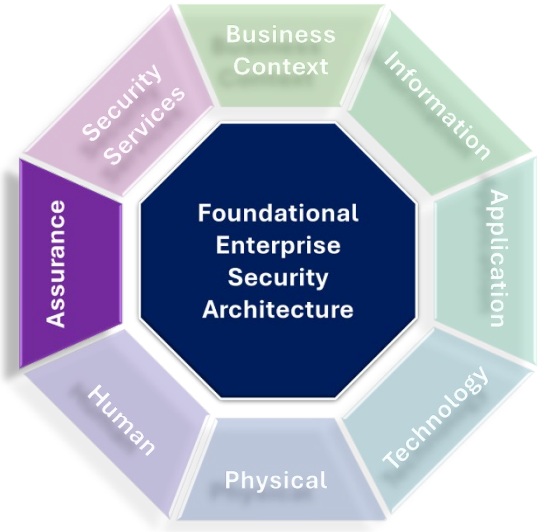
Security Awareness and Training: Develop appropriate audience specific security awareness and training programs for employees.

Human Resource Security: Define hiring, onboarding, and offboarding security procedures, including the organization's security requirements and drivers.

Behavioral Profiling: Monitor and manage user behavior for security purposes.

[13] Yes, it's true – I've had to carefully clean my laptop on multiple occasions because I've attempted to use a laptop prior to being properly caffeinated.

Assurance Layer



After we have addressed the technology and personnel components of the framework, we need to ensure our stakeholders receive the trust and confidence they require. Welcome to the Assurance Layer, which is all about building trust and confidence in the security services in which they have invested. Here, we collect information about compliance, risk management, and assurance frameworks.

This layer helps ensure that our security practices are not only effective, but also in line with regulatory requirements, industry standards and internal drivers.

In the Assurance Layer we capture three artifacts. These can then be leveraged to demonstrate that we're doing the right things, we're doing them well, we are doing them the right way and that as a result, our stakeholders are receiving value (or at the minimum, know that we're doing what is reasonable to protect their information and/or investments).

Audit & Compliance: Establish auditing and compliance monitoring processes.

Security Testing: Define methods for security testing, including penetration testing, vulnerability assessments and technical evaluations. It is important to understand the difference and value each of these, the following is provided to help understand these differences:

Aspect	Penetration Testing	Vulnerability Assessment	Technical Evaluation
Objective	Emulate real-world attacks to identify vulnerabilities and assess the effectiveness of security controls.	Identify and quantify vulnerabilities in systems and networks.	Assess the technical aspects and configurations of security controls.
Focus	Exploit to gain unauthorized access or action on objectives.	Identifying and classifying vulnerabilities without exploiting them.	Examining security configurations and settings to ensure they are aligned with best practices.
Method	Actively seeks to exploit weaknesses to assess system resistance to attacks.	Passively identifies vulnerabilities without exploiting them.	Analyzes security configurations, policies, and technical controls.

Aspect	Penetration Testing	Vulnerability Assessment	Technical Evaluation
Frequency	Typically performed periodically (e.g., annually or quarterly) or in response to significant changes.	Can be performed regularly, even continuously, to detect new vulnerabilities as they emerge.	Conducted as part of security architecture reviews, system upgrades, or when implementing new technologies.
Use Cases	Uncover critical security flaws, test incident response, and assess security posture.	Identify vulnerabilities, prioritize remediation, and monitor for changes.	Ensure security controls are effectively configured and aligned with security policies.
Value	Provides a real-world assessment of an organization's security posture. Helps identify high-risk vulnerabilities and assess security incident response.	Identifies vulnerabilities in a non-intrusive manner, allowing for risk prioritization and remediation planning.	Validates that security controls are properly implemented and configured, reducing the attack surface.
Report Type	Typically includes detailed exploit reports, impact analysis, and recommendations for remediation.	Provides a list of vulnerabilities with severity ratings, remediation suggestions, and ongoing monitoring recommendations.	Offers recommendations and best practices for improving technical controls.
Skills Required	Systems and critical thinking, attention to detail; requires highly skilled and experienced professionals who have deep technical knowledge.	Involves security professionals with vulnerability scanning and assessment expertise.	Systems and critical thinking, attention to detail; requires a thorough understanding of security architectures and configurations.
Regulatory Compliance	Assists in meeting compliance requirements by uncovering vulnerabilities and demonstrating due diligence.	Supports compliance efforts by identifying and addressing vulnerabilities that could lead to non-compliance.	Helps in ensuring that technical controls adhere to regulatory standards.
Budget and Resource Implications	Generally higher costs due to skilled personnel and potentially disruptive testing.	Often more cost-effective, with automated tools used for scanning.	Resource-intensive but helps in minimizing costly breaches by validating controls.
Challenges	May disrupt business operations if not properly planned, and ethical considerations are essential. Often unrealistic scoping (e.g., Silo approach)	May disrupt business operations if not properly planned; generate false positives/negatives, and some vulnerabilities may remain unexplored.	Requires deep technical expertise, and misconfigurations can be missed if not analyzed thoroughly.

Table 8 – Security Testing Comparison

One of the most common questions we are asked after performing these activities (and spending the organization's money to accomplish) is "*who gets these reports?*" Understanding the intended target audience is key. The following table is meant to

illustrate some potential stakeholders who may receive copies of the various reports that are generated. You, however, will need to verify with your leadership and general counsel before sharing anything outside of your organization.

The relationship between business and security operations is critical. Activities like threat modeling, code reviews, penetration tests, and vulnerability assessments identify risks that can lead to financial losses, operational disruptions, and reputational damage. These findings must be presented in terms that business owners can understand and act on as they are responsible for the areas impacted by these risks. By aligning risks with business priorities, organizations can ensure business owners take responsibility, allocate resources for mitigation, and plan for operational impacts.

Target Audience	Rationale/Justification
Network Engineers	Design, implement, and maintain network infrastructure.
System Administrators	Manage servers, endpoints, and IT systems.
Application Developers	Build and maintain software applications.
DevOps Engineers	Integrate security testing into CI/CD pipelines.
Compliance Officers	Ensure alignment with regulatory requirements and industry standards.
Risk Managers	Assess and prioritize security risks.
CEO, CFO, Board Members	Oversee organizational security posture.
General Counsel and Legal Advisors	Provide legal guidance on data protection and privacy laws.
Privacy Officers	Ensure compliance with data protection regulations.
Vendors, Suppliers, and Partners	Request security testing reports as part of contractual agreements or vendor assessments.
Customers and Clients	Inquire about security posture and testing results.

Table 9 – Testing Audience Breakdown

Incident Response: Having an incident response plan and procedures is important. It gives you a playbook and demonstrates forward thinking. Your mileage will vary and there will be different processes for different incident scenarios that will need to be defined, just like in *sportsball* – you will have multiple playbooks to reference. The following is meant to illustrate the foundational elements of Incident Response Management efforts within an enterprise.

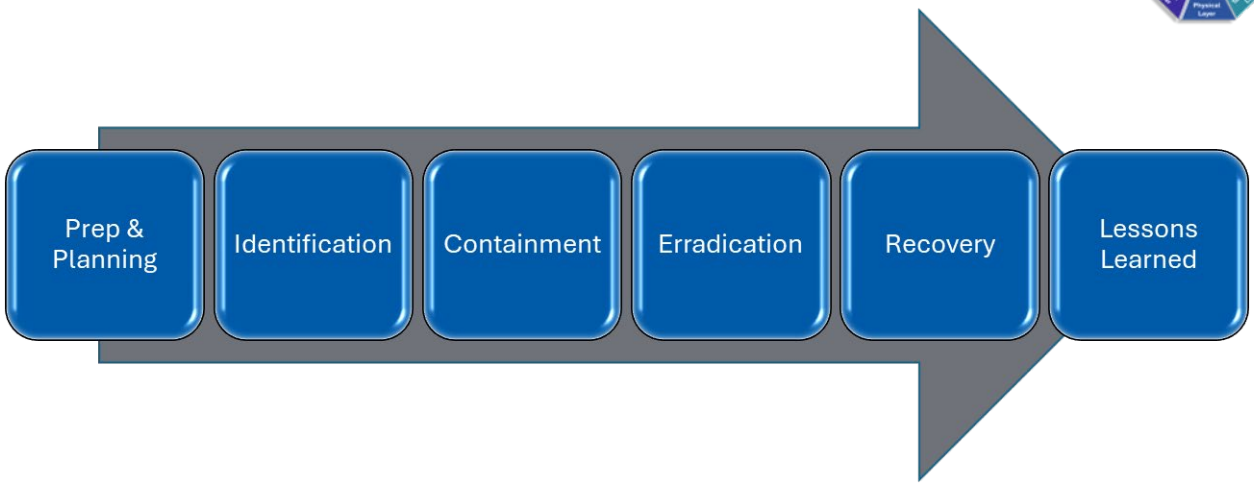
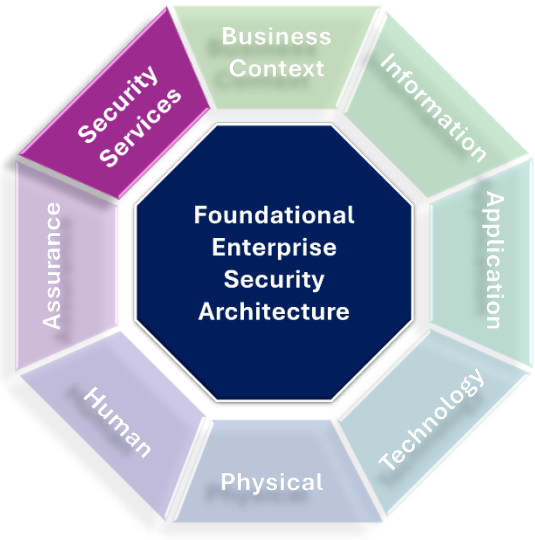


Figure 11 – Incident Response Process (example only)

Also, just to level set expectations, if your organization is not thinking about the future incident that is going to occur on a random Wednesday afternoon at 5pm in April – guess again. Senior Management tends to believe that having an IR plan that is "very high-level" is adequate – ideally your IR documentation should be clear, concise and leave very little to the imagination.

Security Services Layer



We are in the endgame[14] now, Security Services Layer, which is where everything is brought together. At this layer we define the specific security services and controls that are available to protect our enterprise.

By capturing information and documenting these services, we ensure that the appropriate safeguards and countermeasures are in place and available to address the risks and vulnerabilities.

In this final layer, we capture the following three (3) artifacts. Ideally, these will codify the services that the security can and will provide[15], define and formalize the associated response levels and anticipated results, as well as how services will be integrated[16] into the enterprise.

[14] It should be noted that while there were a lot of MCU fans who collaborated on this publication, it is not intended to be an infringement on the MCU's *Avenger's Endgame* movie, nor any Disney trademarks. Don't mess with Mickey, they have lots of lawyers. Just saying. If you really want to know the story, ask the Iowa Farm Boy over an unsweet iced tea sometime.

[15] This is to avoid misunderstandings of capabilities and to establish realistic expectations with the various business units/departments and senior management.

[16] You can implement anything, but you do not receive value until it is properly integrated with business operations.

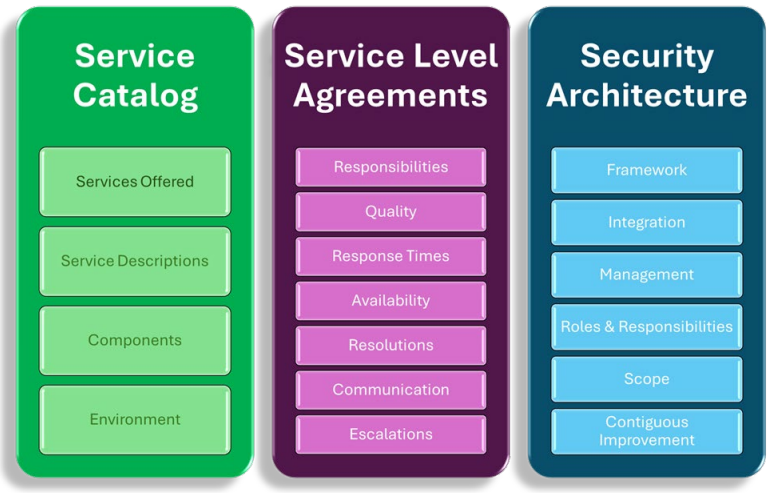


Figure 12 – Security Services Layer

Security Services Catalog: The catalog of defined security services available and provided to the constituents of the organization.

Service-Level Agreements (SLAs): This is used to clearly communicate sufficient information to the constituency so they can understand the expectations.

Security Architecture Framework: With the FESA framework complete, we're now prepared to implement, integrate, and manage security services across the enterprise, bringing everything together cohesively to protect our organization.

Adoption Approach

If you are new to Enterprise Security Architecture, your first instinct may be to jump into the templates and start cranking out documentation and diagrams. Hold up a second young buckaroo! First you really need to learn your organization's strategy, goals, and objectives.

Figure 13 – Adoption Approach

It falls on you to seek out what the organization's strategy is. You will need to understand how that translates into the organization's goals and objectives. You will also need to understand how success is being monitored and how that translates into specific work functions and activities within the organization. Once you have successfully captured these core elements, you can continue down the road to adopt FESA.

Second, know your audience and speak in business appropriate terms. Leave the tech jargon at the door. Understand your organization's culture and identify the formal and informal decision makers and influencers. You will need to gain their buy-in once you have established trust and a rapport with them. Once you have this understanding of the business you can begin efforts in a defensible manner to demonstrate that the goals of security are aligned with the organization. All too often technologists are quick to provide their solution without fully understanding the needs or requirements of the enterprise.

Templates

This framework includes 26 example templates—keyword: example. In our view, these templates represent the minimum viable, foundational elements that should be formally documented and maintained. However, they are by no means an exhaustive solution for proper Enterprise Security Architecture.

The templates provided set the stage for maturing your program and are purely intended to be used as an initial starting point. You will still need to roll your sleeves up, do your homework and tailor the templates to the unique needs, requirements, and culture of your enterprise.

Understanding the Artifacts

So, this is where things can start to get tricky – especially if this is your first-time diving into the fun filled world of architecture; given the nature of business and in context of security, there are a number of interdependencies which exist.

The best way to illustrate this is to think of this like a cherry pie[17], fresh out of the oven and cut into multiple slices. Each slice represents a specific dimension of enterprise security, but underneath that soft flakey crust, it is flowing around all together.

Figure 14 – Cherry Pie Analogy

This may be a bit counter-intuitive, especially if you are a linear thinker. That's because there are a number of interdependences requiring us to treat individual artifacts as living documents, meaning that as you get additional information, it feeds into and updates other artifacts.

We will caution there are a number of common pitfalls that practitioners often don't factor in when adopting an ESA. To help you navigate, we've put together a list of these pitfalls in Appendix I.

Business Layer Artifacts

As these artifacts are outside IT, you will need to work with leadership, management, and various lines of business (i.e., human resources, legal, development, etc.) to understand their individual goals, concerns, and established agreements.

Business Strategy Alignment

Supported by: Business Requirements, Enterprise Security Policy

This artifact ensures we are aligning security efforts with the organization's strategy, goals and overall business objectives and relies on understanding specific business requirements, as well as the establishment of a high-level enterprise security policy to ensure and maintain continued alignment.

[17] To be fully transparent, I'm sitting here and am really hungry. Probably because my YouTube feed recommend that I watch (which I did) Chef John's "*Cherry Pie with Almond Crumb Topping – Cherry Pie Streusel*". Yes, it's 11 years old, but watch and let me know if you're not hungry now too: https://youtu.be/ia9fBs3A3PU

Business Risk Profile

Supported by: Business Requirements, Enterprise Security Policy

The risk profile is established by executive leadership, based on business needs, and should be used to inform the enterprise security policy to help prioritize risks. It is highly encouraged that you also review related sources of information (e.g., business impact assessments, business continuity plans, etc.) to gain additional insight.

Enterprise Security Policy

Supported by: Business Strategy Alignment, Business Risk Profile, Business Requirements

The Enterprise Security Policy should be directed by and in alignment with both the business strategy and the risk profile. This does not need to be overly verbose, instead it should establish the expectations for behavior and establish security as a priority within the organization. Additionally, operational requirements will play a significant role in shaping both this and subsequent (read, granular) policies.

Business Requirements

Supported by: Business Strategy Alignment, Business Risk Profile, Enterprise Security Policy

Business requirements are a critical input to ensure that security measures align with the organization's strategic goals and risk profile. You should consider leveraging any existing and available sources (e.g., business impact assessments, business continuity plans, etc.) to support your understanding of what business requirements exist. These are not always centralized and may require seeking them out from different departments (i.e., human resources, legal, development, etc.).

Information Layer Artifacts

This will require you to have conversations with product teams and business line leadership, as this is not always reflected in diagrams. Additionally, not all data or risk appetites are equal. Work with the appropriate stakeholders to gain clarity and definition on the criticality and sensitivity of the data/information being collected, stored, processed, shared, or transmitted. You should also consider privacy requirements and implications as well.

Information Classification

Supported by: Information Security Policies & Procedures, Data Lifecycle Management

Information classification informs the content of the information security policy and is closely related to data lifecycle management practices. You need to understand what information the organization has been entrusted with, baseline security measures needed to be applied in context of the business value and criticality. This should ensure limited resources are focused on areas which matter the most to the organization and address risks which exceed the defined profile.

Information Security Policies & Procedures

Supported by: Information Classification, Data Lifecycle Management

These policies and procedures are influenced by how information is classified and how it is managed throughout its lifecycle. Additionally, these tend to be more granular in nature, with operational procedures (the required steps to be followed) being developed to ensure a defined policy is enforceable. *Appendix F provides examples of both a policy lifecycle process and policy structure.*

Data Lifecycle Management

Supported by: Information Classification

Data lifecycle management relies on information classification to define how data is created, stored, processed, and disposed of securely. The lifecycle of data is always a tricky topic to tackle, but until you understand the data lifecycle, you will not be able to identify where to place controls in the most effective and efficient manner needed.

Application Layer Artifacts

Application Portfolio

Supported by: Secure Application Design, Access Control Models

The application portfolio informs the design of secure applications, and the access control models required for them. All applications require information. Understanding what information is being stored, processed, accessed, or transmitted allows us to properly identify and recommend the appropriate controls needed to properly protect the information and reduce business risk accordingly.

Access Control Models

Supported by: Secure Application Design, Identity and Access Management

Access control models are needed in the design of secure applications, systems, infrastructure, and data repositories which rely on identity and access management processes. This ensures that account access is properly provisioned and granted only for those accounts with a valid business requirement and that access can be accounted for. Key considerations should be given to those accounts with privileged access to information and the performance of account access reviews.

Secure Application Design

Supported by: Access Control Models, Application Portfolio

The design of secure applications is closely related to defining and implementing access control models for those applications. Secure Application Design ensures that we have identified

potential abuse and misuse of the application, which could result in exposing or allowing unauthorized access to the information which is accessible by the application.

Technology Layer Artifacts

Technology Inventory

Supported by: Security Infrastructure Design

The inventory of technology assets supports the design of the security infrastructure and aids in establishing or capturing technology standards. These should include those assets which the organization relies upon (e.g., mobile, workstation, data center, cloud services). After all, you can only protect what you know about.

Security Infrastructure Design

Supported by: Technology Inventory, Network Security

Designing the security infrastructure is related to the inventory of technology assets and the architecture of network security. This artifact captures existing security controls available within the organization. Additionally, we should capture the security technology standards and develop potential integration strategies to ensure that the appropriate elements of an organization's security infrastructure work together seamlessly.

Network Security Architecture & Controls

Supported by: Security Infrastructure Design

This encompasses all safeguards and countermeasures used to protect the network from threats such as unauthorized access, data breaches, malware, and other network-based attacks. It involves defining network security architecture which may include a variety of controls, such as identity & access controls, access control lists, segmentation, VLANs, intrusion detection and prevention systems, firewalls, and encryption mechanisms.

Identity and Access Management

Supported by: Access Control Models

Establishing mechanisms related to authentication, authorization, and management processes supports access control models. Identity and access management forms the cornerstone of modern enterprise security efforts and is the foundation for access control models. In addition to the technical application of IAM capabilities, it is also required that we manage these processes efficiently, considering jurisdictional authority, geographical requirements, and trans-border operations.

Physical Layer Artifacts

Physical Security Controls

Supported by: Data Center Security, Environmental Controls

Physical security controls are related to securing data centers and ensuring appropriate environmental conditions for technology equipment. We still need to consider our physical security controls to protect IT assets on-prem, as users, visitors, contractors, and other third-parties often access our facilities and efforts to protect the organization need to be considered.

Data Center Security

Supported by: Physical Security Controls, Environmental Controls

Securing data centers relies on physical security measures and the environment in which technology equipment is located. While there is a push for and adoption of "Cloud first" approach to IT, we don't want to forget our traditional data centers (or wiring closets, telco rooms, server under the desk, etc.) where IT systems may still be resident on-premises. This artifact should capture the associated controls needed to physically protect those IT assets.

Environmental Controls

Supported by: Physical Security Controls, Data Center Security

Ensuring appropriate environmental conditions supports physical security controls and data center security. Capturing how the organization protects their IT investments from environmental issues ensure risks are properly accounted for and addressed; after all fire, humidity, temperature spikes or electrical surges can impact the ability to operate just as quickly as a criminal threat.

Human Layer Artifacts

Security Awareness and Training

Supported by: Human Resource Security

Security awareness programs and training are crucial components of human resource security procedures. Because our staff interact with various IT systems, we need to ensure they are properly aware of and know about the various threats our organizations face. Additionally, they need to know what to do when they encounter these threats. Here we capture the organization's Security Awareness & Training program to ensure we are ***proactively*** engaging and elevating staff awareness to the threats we face.

Human Resource Security

Supported by: Security Awareness and Training

Effective human resource security practices rely on comprehensive security awareness programs, training, and robust onboarding and offboarding procedures for staff and contractors. By collaborating with human resources to define, maintain, and apply these practices for

onboarding, internal transitions, and offboarding, we can ensure policy adherence and effectively manage organizational risk.

Behavioral Profiling

Supported by: Audit and Compliance, Security Testing

Behavioral profiling is often part of auditing and compliance monitoring processes and security testing. Here we want to capture the necessary information to detect potential security threats or anomalous activities, which may be indicative of a risk to the organization. Additionally, it should establish the requirement for baselines, allowing for detection of abnormal events, allowing the ability to identify and respond more effectively and efficiently. You must know what good is to find bad.

Assurance Layer Artifacts

Audit and Compliance

Supported by: Security Testing, Incident Response

Audit and compliance processes are closely related to security testing, and they guide incident response activities. This is to ensure that we operate at the appropriate levels of performance and conformance. Operating in a compliant manner does not expose the organization to unnecessary risk. By capturing and understanding the scope of applicable business requirements and drivers (e.g., PCI DSS, HIPAA, SOX, etc.), we can then apply the appropriate controls, mapping back to the business driver and defined requirement.

Security Testing

Supported by: Audit and Compliance, Incident Response

Security testing is essential for assessing and ensuring security compliance and should influence incident response planning. The goal here is to capture the methods and procedures for security testing (e.g., vulnerability scanning, code review, penetration testing, etc.) and should include elements such as defining the objectives, types of testing, and reporting.

Incident Response

Supported by: Audit and Compliance, Security Testing, Risk Profile

Incident response planning is often treated as a checklist or based on a template 'downloaded from the Internet.' Ideally, however, it should be developed over time, informed by business impact analysis, operational requirements, audit and compliance findings, and insights from security testing. Incidents will happen (often at 4:28 p.m. on the Friday before a long weekend), and while the goal is to define processes, roles, and responsibilities for anticipated events, the plan must also allow flexibility for unexpected incidents. Establishing realistic expectations helps ensure a swift and effective response, even for scenarios that may not have been explicitly planned for.

Security Services Artifacts

Security Services Catalog

Supported by: Service-Level Agreements (SLAs)

The security services catalog provides a "menu" of security capabilities to the organization and establishes service-level agreements of those services. We want to capture and publish all the security services that will be made available to the organization; this should be a detailed list of what those services are, an overview of the services, how staff within the organization can engage for those services and business value of those services offered.

Service-Level Agreements (SLAs)

Supported by: Security Services Catalog

SLAs are developed based on the services catalog, ensuring clear terms and conditions for the services being offered and provided to the organization. This artifact will be used to define and formalize the services that security will be providing to the organization, and is inclusive of defining performance metrics, responsibilities, and level-setting expectations about each of those services.

Security Architecture Framework (SAF)

This serves as the overarching structure that integrates and aligns all the other artifacts, ensuring a cohesive and holistic security architecture. Ultimately, the SAF outlines and defines the objectives to be met, key integration points with the business, how risks are to be addressed, and the various security components and services needed. This provides management with assurances that security is aligned with and enabling the business to achieve their strategy, balancing performance, and conformance to deliver value.

The culmination of these interconnected relationships and interdependencies results in leveraging these various artifacts into a Foundational Enterprise Security Architecture framework, a comprehensive, integrated yet practical approach to enterprise security architecture.

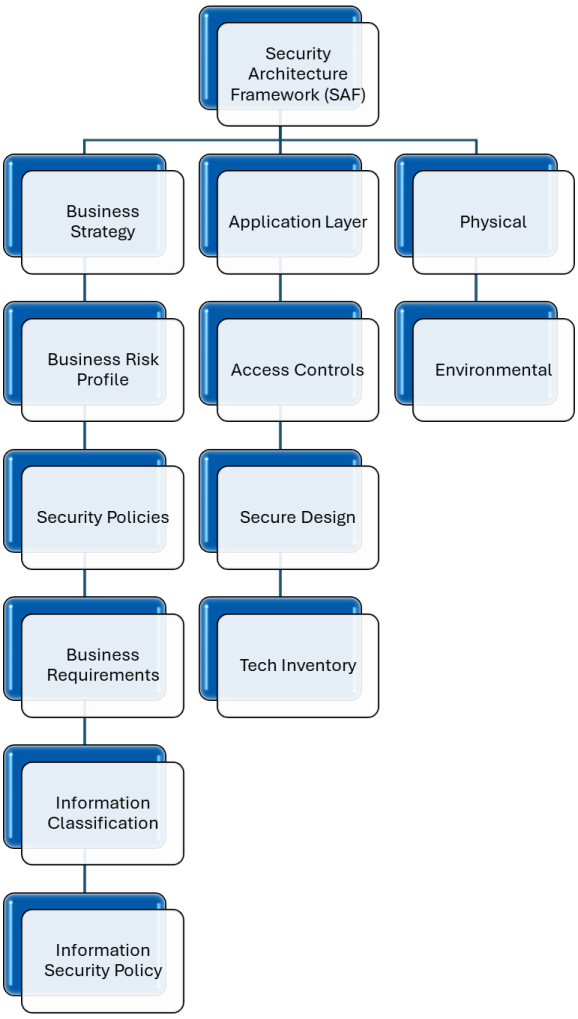


Figure 15 – Security Architecture Framework (components)

Foundational Enterprise Security Architecture Templates

For an aspiring architect, understanding the target audience and how they will derive value from the Foundational Enterprise Security Architecture (FESA) is essential. Rather than creating documentation for its own sake, it should be tailored to meet the organization's needs and provide tangible benefits to stakeholders. To help identify those who typically find value in architecture, the following table maps audience members to the specific benefits and value they receive from FESA.

Target Audience	Rationale	Benefit/Value
IT Operations and Infrastructure Teams ***Management of IT systems and infrastructure***	Integrates security architecture into IT systems design, deployment, and maintenance. Provides insights into existing technology stacks, network configurations, and operational constraints.	Improves resilience, scalability, and efficiency of security solutions, while minimizing disruptions to business operations.
Business Unit Leaders and Stakeholders ***Representation of various departments***	Ensures security architecture addresses specific business needs, requirements, and risk appetites. Provides insights into business workflows, data handling practices, and regulatory obligations.	Prioritizes security investments, aligns security controls with business objectives and fosters a culture of security awareness and accountability.
Executive Leadership and Board Members ***Strategic direction and oversight***	Demonstrates organizational commitment to security. Aligns security architecture with strategic priorities, risk appetite, and budget allocations. Provides support for funding and resource allocation.	Elevates security as a business priority, improves decision-making around security investments, and enhances stakeholder confidence in the organization's ability to manage security risks effectively.
Office Manager ***Management of administrative processes***	Ensures security measures align with administrative policies and procedures.	Facilitates the implementation of security measures within administrative workflows and supports the enforcement of security policies across the organization.
General Counsel ***Legal guidance and compliance oversight***	Provides legal advice on data protection, privacy laws, and regulatory compliance.	Ensures that security measures comply with applicable laws and regulations, mitigating legal risks and liabilities associated with data breaches or non-compliance.
Human Resources ***Management of employee-related matters***	Ensures that security awareness training is provided to employees. Manages access control and personnel security procedures.	Supports the development of a security-aware culture, enhances employee awareness of security risks, and ensures proper handling of personnel-related security matters.
Marketing ***Promotion and communication of brand***	Communicates security-related messages to customers and stakeholders.	Enhances customer trust and confidence by demonstrating the organization's commitment to security and privacy.
Sales ***Engagement with customers and clients***	Addresses security-related concerns and requirements raised by customers.	Demonstrates the organization's ability to meet customer security and privacy requirements, enhancing customer satisfaction and retention.

Business Context Layer

Business Strategy Alignment

Ensure that the security strategy aligns with the overall business strategy.

Business Strategy Alignment Report

Date: [Date]

Executive Summary

This outlines the alignment of the organization's security strategy with its overarching business strategy. The purpose is to ensure that security measures are closely integrated with and supportive of the organization's business objectives.

1. Introduction

Background and context of the organization's business strategy.
Provide an overview of the security strategy alignment initiative.

2. Business Strategy Overview

A summary of the organization's strategy, including key goals and objectives, market analysis, competitive positioning, growth targets, and key business processes and systems.

3. Security Strategy Alignment

Explanation of how the security strategy supports the business strategy.
Identification of key security-related components that align with business goals.
A summary of timely security and privacy incidents and their impact on the business.

4. Security Objectives

Detailed list of security objectives derived from the business strategy, categorized by relevance.
Prioritization of security objectives based on business impact and risk assessment.

5. Risk Assessment

An overview of the organization's risk profile and how it influences business decisions.
Identification of high-priority risks and their impact on business operations.

6. Security Policy Alignment

Description of security policies and procedures aligned with the business strategy.
Highlight key security policies that directly impact business goals.

7. Metrics and Key Performance Indicators (KPIs)
Definition of security related KPIs used to measure alignment effectiveness.
Reporting frequency and mechanisms for tracking KPIs.

8. Budget Allocation
Breakdown of the security budget and resources allocated to support the aligned security strategy.
Justification for resource allocation based on business-critical security needs.

9. Stakeholder Involvement
List of key stakeholders involved in the alignment process.
Roles and responsibilities of stakeholders in implementing the aligned strategy.

10. Conclusion
Summary of the key takeaways from the alignment process.
Next steps and recommendations for ongoing alignment and monitoring.

11. Appendices
Supporting documents, charts, and data used in the alignment process.
Detailed financial breakdowns, risk assessments, or specific business cases.

Business Risk Profile

Define the organization's business risk profile and priorities.

Business Risk Profile

Date: [Date]

Executive Summary
This Business Risk Profile provides an overview of the key risks the organization is exposed to. It serves as the foundation for risk management and decision-making.

1. Introduction
Background information on the organization and its core business activities.
Purpose and scope of the Business Risk Profile.

2. Risk Categories
Categorization of risks into relevant categories, such as financial, operational, compliance, strategic, and reputation risks.
Explanation of how each category affects the organization.

3. Risk Identification
A comprehensive list of identified risks within each category.
Detailed descriptions of each risk, including potential triggers and sources.

4. Risk Assessment
Quantitative and qualitative assessment of each risk, including likelihood and impact.
Risk prioritization based on the organization's defined risk response matrix.

5. Risk Mitigation Strategies
Description of strategies and controls in place or planned to mitigate each identified risk.
Responsibility assignments and timelines for risk mitigation efforts.

6. Risk Appetite and Tolerance
Clear articulation of the organization's risk appetite and risk tolerance.
Explanation of how these factors influence risk management decisions.

7. Key Risk Indicators (KRIs):
A list of specific metrics and indicators that will be used to monitor and report on identified risks.
Thresholds and alerts triggering further risk management actions.

8. Risk Management Framework
Description of the organization's overall risk management framework.
Roles and responsibilities of key stakeholders in the risk management process.

9. Reporting and Monitoring
Methods and frequency of reporting on risk status to senior management and the board.
Procedures for ongoing monitoring and adjustments to the risk profile.

10. Compliance and Legal Considerations
Any legal or regulatory requirements related to risk management.
Status of compliance measures in place or planned to address established requirements.

11. Conclusion
Summary of the most critical risks and their potential impact on the organization.
Recommended actions and strategies to enhance risk management.

12. Appendices
Supporting data, charts, and risk assessment models.
Historical data on risk incidents and trends.

Security Policy

Establish high-level security policies and objectives based on business needs. The intent of this policy is to establish the requirements for all subsequent requirements for having a comprehensive security program. Specific policies, processes, procedures, and plans will have detailed and amplifying directions based on each organization's requirements.

[Organization Name] Security Policy

Effective Date: [Date]

1. Introduction
Purpose of the Policy: To establish and maintain a comprehensive security program to protect [Organization Name]'s information, assets, and systems.

Scope: This policy applies to all employees, contractors, and third parties who access, use, or manage [Organization Name]'s resources.

2. Information Classification and Handling
Definitions of information classification levels (e.g., public, internal use, confidential).
Standards for classifying and handling data and information, based on its sensitivity.
Procedures for data encryption, storage, and transmission.

3. Access Control
User authentication and authorization standards.
Password management and complexity requirements.
Access request and approval procedures.
Review of user access permissions.
Account termination and deprovisioning processes.

4. Network and Systems Security
Acceptable use of [Organization Name]'s network and systems.
Firewall and intrusion detection/prevention policies.
Firewall and intrusion detection/prevention hygiene/management processes.
Vulnerability assessment and patch management procedures.
System backup and recovery guidelines.
Endpoint protection policies.
Endpoint protection hygiene/management processes.
Mobile Device Management policies.
Mobile Device Management hygiene/management processes.

5. Physical Security
Access control to physical facilities and data centers.

Visitor and guest policies.
Protection of company-owned assets, including laptops and mobile devices.

6. Incident Response and Reporting
Procedure for reporting security incidents.
Incident categorization, triage, and response plan.
Escalation and notification process.

7. Employee Training and Awareness
Security awareness and training requirements.
Acceptable use policy acknowledgment.
Reporting of security concerns.

8. Third-Party Security
Security requirements for third-party vendors and contractors.
Security Risk Assessment.
Compliance checks and audit procedures for third-party agreements.

9. Compliance and Legal Considerations
Applicable laws, regulations, and industry standards.
Procedures for compliance monitoring and reporting.

10. Policy Management
Roles and responsibilities of employees and management.
Consequences for policy violations.
Compliance monitoring and audit processes.
Schedule for policy review and update.
Process for soliciting and incorporating feedback from stakeholders.

11. Glossary
Definitions of key terms and acronyms used in the policy.

12. Document History
Record of changes and updates to the policy, including revision dates and authors.

Business Requirements

Identify specific business requirements that need to be supported by security.

Business Requirements for Security

Date: [Date]

1. Introduction

Purpose: This document outlines the specific business requirements that must be supported by the organization's security strategy.

Scope: These requirements encompass the core business functions, objectives, and initiatives of [Organization Name].

2. Business Objectives

[Business Objective 1]: A clear statement of the first core business objective.

Rationale: Explanation of why this objective is crucial for the organization's success.

Security Implications: How security measures are necessary to achieve this objective.

[Business Objective 2]: A clear statement of the second core business objective.

Rationale: Explanation of why this objective is crucial for the organization's success.

Security Implications: How security measures are necessary to achieve this objective

(Repeat for all core business objectives.)

3. Regulatory and Compliance Requirements

[Regulation 1]: Description of specific regulations or compliance standards affecting the organization.

Compliance Requirements: Explanation of the security requirements to meet regulatory obligations.

Security Measures: How security practices and controls are tailored to meet regulatory needs.

[Regulation 2]: Description of specific regulations or compliance standards affecting the organization.

Compliance Requirements: Explanation of the security requirements to meet regulatory obligations.

Security Measures: How security practices and controls are tailored to meet regulatory needs.

(Repeat for all applicable regulations or standards.)

4. Risk Mitigation and Resilience
Business Continuity and Disaster Recovery: Requirements for ensuring the continuity of critical business operations in the face of disruptions.

Risk Appetite: The organization's defined level as to when a risk is to be either accepted, avoided, transferred, or mitigated.

Risk Tolerance: The organization's criteria for the deviation from established Risk Appetite; specific risks are temporarily categorized as "acceptable" given that impact would not exceed benefits AND exists for a specific, short amount of time.

5. Data Protection and Privacy
Data Classification: Identification of sensitive data and information types and the baseline controls and protection requirements.

Privacy: Requirements for protecting customer and employee data in compliance with privacy laws and contractual requirements.

6. IT and Technology Needs
Technology Infrastructure: Requirements for supporting core technology infrastructure.

Application Security: Specific security needs for critical business applications.

7. Physical Security
Facilities: Requirements for securing physical locations, including data centers, wiring closets and office spaces with information technologies.

Asset Protection: Protection of physical assets.

8. Third-Party Relationships
Vendor and Supplier Security: Requirements for third-party vendors and suppliers to ensure the security of products and services used by the organization.

Contractual Obligations: Terms to include in third-party contracts to meet security requirements.

9. Conclusion

Summary of the critical business requirements that security measures need to support.

A reminder that these requirements will guide the development and implementation of the organization's security strategy.

Information Layer

Information Classification

Classify data and information assets according to their sensitivity and criticality.

Information Classification Policy

Date: [Date]

1. Introduction
Purpose: This policy outlines the framework for classifying information and data assets according to their sensitivity and criticality.

Scope: The policy applies to all employees, contractors, and third parties handling [Organization Name]'s information assets.

2. Information Classification Categories
[Category 1: Public Information]
Description: Information that can be freely disclosed to the public.

Examples: Publicly available marketing materials, press releases.

[Category 2: Internal Use Information]
Description: Information intended for internal use within the organization.

Examples: Non-sensitive internal documents, employee directories.

[Category 3: Confidential Information]
Description: Information that requires protection against unauthorized disclosure.

Examples: Financial data, proprietary business processes.

[Category 4: Highly Sensitive Information]
Description: The most critical information requiring the highest level of protection.

Examples: Personal identification data, trade secrets, customer financial data.

3. Responsibilities
Data Owner: The individual or department responsible for data assets within each category.

Data Custodian: The individual or department responsible for maintaining and protecting data assets.

Users: All employees, contractors, and third parties who handle or access data are responsible for adhering to data classifications.

4. Classification Criteria
Criteria for classifying data into the appropriate categories, including sensitivity, criticality, and regulatory requirements.

Decision-making process for determining the appropriate classification for data assets.

5. Handling Standards
[Category 1: Public Information]
No specific handling requirements.

[Category 2: Internal Use Information]
Access restricted to authorized personnel.
Sharing within the organization only.

[Category 3: Confidential Information]
Access restricted to individuals with a legitimate need.
Encryption requirements for data in transit and at rest.

[Category 4: Highly Sensitive Information]
Strict access control and authentication mechanisms.
Strong encryption for data in transit and at rest.
Mandatory reporting of any breaches or incidents.

6. Data Labeling and Marking
Requirements for labeling data assets with their appropriate classification.
Labeling procedures to ensure clear identification of data sensitivity.

7. Data Lifecycle Management
Guidelines for data retention, archival, and disposal based on classification.
Procedures for securely disposing of data assets when they are no longer needed.

8. Training and Awareness
Employee training requirements on information classification.
Awareness campaigns to inform employees of their responsibilities.

9. Compliance and Monitoring
Periodic assessments and audits to ensure compliance with this policy.
Consequences for policy violations.

10. Review and Revision
Regular reviews of the policy and classification criteria.
Procedures for updating classifications as needed.

Information Security Policy

Develop policies and procedures for protecting information assets.

Information Security Policy

Date: [Date]

1. Introduction
Purpose: This policy establishes the framework for protecting [Organization Name]'s information assets.

Scope: The policy applies to all employees, contractors, and third parties with access to [Organization Name]'s information assets.

2. Information Classification and Handling
Information Classification: Categorization of information into sensitivity levels.

Data Handling: Procedures for the secure handling of information assets based on their classification.

3. Access Control
User Authentication: Requirements for user authentication to access information assets.

Authorization: Procedures for granting and revoking access privileges.

Password Management: Guidelines for creating, storing, and changing passwords.

4. Network and Systems Security
Acceptable Use: Guidelines for the appropriate use of [Organization Name]'s network and information systems.

Firewall and Intrusion Detection: Configurations and monitoring practices.
Vulnerability Assessment: Procedures for identifying and addressing security vulnerabilities.

Data Backup and Recovery: Backup processes and recovery plans for data and systems.

5. Physical Security

Facility Access: Control and monitoring of physical access to data centers and other sensitive areas.

Equipment Protection: Guidelines for securing organization-owned physical assets.

6. Incident Response and Reporting
Incident Reporting: Procedures for reporting and documenting security incidents.

Incident Response Plan: Guidelines for responding to and mitigating security incidents.

Escalation: Procedures for escalating incidents to the appropriate authorities.

7. Employee Training and Awareness
Security Training: Requirements for employee security training.

Security Awareness: Promoting a culture of security among all employees.

8. Third-Party Security
Vendor and Supplier Security: Security requirements for third-party vendors and contractors.

Contractual Obligations: Inclusion of security clauses in third-party contracts.

9. Compliance and Legal Considerations
Applicable Laws and Regulations: A list of laws and regulations relevant to information security.

Compliance Measures: Procedures for monitoring and ensuring compliance.

10. Policy Enforcement and Accountability
Roles and Responsibilities: Explanation of roles and responsibilities related to information security.

Consequences for Policy Violations: Penalties for policy violations.

11. Review and Revision
Policy Review: Schedule for policy review and updates.

Revision Process: Procedure for soliciting and incorporating feedback and changes.

12. Glossary

Definitions of key terms and acronyms used in the policy.

13. Document History
Record of changes and updates to the policy, including revision dates and authors.

Data Lifecycle Management

Define how data is created, stored, processed, and disposed of securely.

Data Lifecycle Management Policy

Date: [Date]

1. Introduction
Purpose: This policy establishes the framework for managing data throughout its lifecycle to ensure data integrity, availability, and security.

Scope: The policy applies to all employees, contractors, and third parties with access to [Organization Name]'s data assets.

2. Data Classification
Data Sensitivity Levels: Categorization of data into sensitivity levels (e.g., public, internal use, confidential, highly sensitive).

Data Handling: Procedures for handling data based on its classification.

3. Data Creation
Data Generation: Procedures for creating and capturing data.

Metadata: Documentation and classification of data elements.

Ownership: Assignment of data ownership responsibilities.

4. Data Storage
Storage Location: Criteria for selecting storage locations based on data classification.

Encryption: Encryption requirements for data at rest.

Backup and Retention: Procedures for data backup, retention, and archiving.

5. Data Processing
Access Control: User authentication and authorization to access and modify data.

Logging and Monitoring: Recording and monitoring data access and changes.

Data Integrity: Ensuring data accuracy and consistency during processing.

6. Data Sharing and Transmission
Secure Data Sharing: Procedures for securely sharing data within and outside the organization.

Encryption: Encryption requirements for data in transit.

Secure Channels: Use of secure communication channels for data transmission.

7. Data Destruction and Disposal
End-of-Life Data: Identification of data that has reached the end of its lifecycle.

Secure Disposal: Procedures for securely destroying and disposing of data.

Data Retention Compliance: Ensuring data destruction complies with legal and regulatory requirements.

8. Data Backup and Recovery
Backup Procedures: Regular backup schedules and procedures.

Recovery Plans: Procedures for data recovery in the event of data loss or system failure.

9. Incident Response
Data Breach Response: Procedures for responding to data breaches.

Incident Documentation: Documentation of incidents, including causes and resolution.

10. Employee Training and Awareness
Training Requirements: Employee training in data lifecycle management.

Security Awareness: Promoting a culture of data security among all employees.

11. Compliance and Legal Considerations
Applicable Laws and Regulations: A list of laws and regulations relevant to data management.

Compliance Measures: Procedures for monitoring and ensuring compliance.

12. Policy Enforcement and Accountability

Roles and Responsibilities: Explanation of roles and responsibilities related to data lifecycle management.

Consequences for Policy Violations: Penalties for policy violations.

13. Review and Revision
Policy Review: Schedule for policy review and updates.

Revision Process: Procedure for soliciting and incorporating feedback and changes.

14. Glossary:
Definitions of key terms and acronyms used in the policy.

15. Document History
Record of changes and updates to the policy, including revision dates and authors.

Application Layer

Application Portfolio

Inventory and assess the organization's applications in terms of security requirements.

Application Portfolio Assessment

Date: [Date]

1. Introduction
Purpose: This document outlines the inventory of [Organization Name]'s applications and assesses them in terms of security requirements.

Scope: The assessment covers all applications used or managed by [Organization Name].

2. Application Inventory
Application Name: The name of each application in use.

Description: A brief description of the application's purpose and functionality.

Responsible Team: The department or team responsible for the application.

Contact Information: Contact details for the application's owner or administrator.

3. Security Assessment
Application Criticality

- Assessment: Evaluation of the application's criticality to the organization's operations.
- Security Implications: How the application's criticality affects security requirements.

Data Sensitivity

- Assessment: Categorization of the data handled by the application in terms of sensitivity.
- Security Requirements: Specific security measures required to protect sensitive data.

Access Control

- Assessment: Evaluation of access control mechanisms in place for the application.
- Authorization: Who has access to the application, and what privileges they have.
- Authentication: Authentication methods used for access.

Data Encryption

Assessment: Evaluation of data encryption practices for data in transit and at rest.

Encryption Standards: Specific encryption standards and practices employed.

Vulnerability Assessment

Assessment: Evaluation of the application for known vulnerabilities.

Patch Management: Procedures for addressing and patching vulnerabilities.

Incident Response Plan

Assessment: Availability of an incident response plan specific to the application.

Response Procedures: Procedures for responding to security incidents related to the application.

4. Compliance and Legal Considerations

Applicable Laws and Regulations: Laws, regulations, or industry standards that impact the application.

Compliance Measures: Procedures for ensuring compliance with relevant requirements.

5. Risk Assessment

Risk Profile: An assessment of the application's risk profile and potential risks.

Risk Mitigation: Measures in place to mitigate identified risks.

6. Conclusion

Summary of the security assessments for each application.

Identification of high-priority security needs and areas for improvement.

7. Recommendations

Specific recommendations for improving security for each application, if necessary.

Prioritization: Suggestions for prioritizing security enhancements based on criticality and risk.

8. Review and Update

Schedule for periodic reviews and updates of the application portfolio assessment.
Procedure for including new applications in the assessment.

9. Glossary
Definitions of key terms and acronyms used in the assessment.

Access Control Models

Design access control mechanisms for applications.

Access Control Models for Applications

Date: [Date]

1. Introduction
Purpose: This document outlines the access control models and mechanisms designed for securing [Organization Name]'s applications.

Scope: The access control models apply to all applications used or managed by [Organization Name].

2. Access Control Models
Role-Based Access Control (RBAC)

Description: Role-based access control assigns permissions to users based on their roles and responsibilities within the organization.

Application Integration: Explanation of how RBAC is implemented within each application.

Role Definitions: A list of roles and their associated permissions.

Role Assignment: Procedures for assigning users to roles.

Attribute-Based Access Control (ABAC)

Description: Attribute-based access control uses attributes (user characteristics, resource attributes, environmental conditions) to determine access.

Attributes: Types of attributes used for access decisions.

Policies: Access control policies and rule definitions.
Attribute Evaluation: Procedures for evaluating attributes and making access decisions.

Discretionary Access Control (DAC)

Description: Discretionary access control allows resource owners to set access controls on their resources.

Resource Ownership: Procedures for defining resource ownership.

Permission Assignment: How resource owners assign and manage permissions.

Access Control Lists (ACLs): Use of ACLs for DAC in applications.

Mandatory Access Control (MAC)

Description: Mandatory access control enforces security labels and access decisions based on labels and classifications.

Security Labels: Labeling of data and resources.

Label Enforcement: Procedures for enforcing access controls based on labels.

3. Access Control Implementation

Authentication and Authorization

Authentication Mechanisms: Methods for user authentication within applications.

Authorization Process: Procedures for authorizing users based on the chosen access control model.

Enforcement Mechanisms

Application Integration: Explanation of how access control models are integrated into applications.

Enforcement Procedures: Mechanisms used for enforcing access controls within applications.

4. Access Control Policy

Policy Definitions

Policy Statements: The specific policies governing access to application resources.

Policy Language: The language used to define access control policies.

Policy Enforcement

Policy Evaluation: Procedures for evaluating access control policies.

Policy Decision: How access control decisions are made.

5. Compliance and Legal Considerations
Applicable Laws and Regulations: Laws, regulations, or industry standards impacting access control for applications.

Compliance Measures: Procedures for ensuring compliance with relevant requirements.

6. Conclusion
Summary of the access control models and mechanisms designed for applications.

Identification of key components and procedures.

7. Review and Update
Schedule for periodic reviews and updates of the access control models and mechanisms.

Procedure for applying access control models to new applications.

8. Glossary
Definitions of key terms and acronyms used in the document.

Secure Application Design

Define secure coding practices and design principles.

Secure Application Design Principles

Date: [Date]

1. Introduction
Purpose: This document outlines the secure application design principles and practices to ensure that [Organization Name]'s applications are built with security as a core component.

Scope: The design principles apply to all applications developed or managed by [Organization Name].

2. Secure Coding Practices
Input Validation

Description: Input validation is essential to prevent input-based attacks, such as SQL injection and cross-site scripting (XSS).

Best Practices: Guidelines for validating and sanitizing user inputs.

Authentication and Authorization

Description: Proper authentication and authorization mechanisms are essential for ensuring that users only have access to the data and functionality they are authorized to use.

Best Practices: Guidelines for secure user authentication and authorization.

Data Encryption

Description: Data encryption is crucial for protecting data at rest and data in transit.

Best Practices: Recommendations for encrypting sensitive data and communications.

Secure Configuration

Description: Proper configuration of application components, frameworks, and libraries is essential to minimize security vulnerabilities.

Best Practices: Guidelines for secure configuration practices.

Session Management

Description: Secure session management is crucial for maintaining user sessions and protecting against session hijacking.

Best Practices: Recommendations for secure session handling.

3. Design Principles

Principle of Least Privilege

Description: Users and processes should have the minimum necessary privileges to perform their tasks.

Implementation: How the principle of least privilege should be implemented in application design.

Defense in Depth

Description: Security should be implemented in multiple layers to provide redundancy and depth of protection.

Implementation: How defense in depth principles should be incorporated into application architecture.

Secure Error Handling

Description: Error messages should not reveal sensitive information and should be logged securely.

Implementation: Guidelines for secure error handling practices.

4. Secure Design Review

Design Review Process

Description: Procedures for conducting secure design reviews before development begins.

Roles and Responsibilities: Roles and responsibilities of individuals involved in design reviews.

5. Compliance and Legal Considerations

Applicable Laws and Regulations: Laws, regulations, or industry standards impacting secure application design.

Compliance Measures: Procedures for ensuring compliance with relevant requirements.

6. Conclusion

Summary of the secure application design principles and practices.

Identification of key components and procedures.

7. Review and Update

Schedule for periodic reviews and updates of the secure application design principles.

Procedure for applying secure design principles to new application development.

8. Glossary

Definitions of key terms and acronyms used in the document.

Technology Layer

Technology Inventory

Identify and assess the organization's technology infrastructure.

Technology Inventory Assessment

Date: [Date]

1. Introduction

Purpose: This document outlines the technology inventory assessment, providing an overview of [Organization Name]'s technology infrastructure.

Scope: The assessment covers all resources [18]used or managed by [Organization Name].

2. Hardware Inventory

Servers

Description: A list of all servers, including physical and virtual servers.

Specifications: Hardware specifications, configurations, and operating systems.

Workstations and End-User Devices

Description: An inventory of all workstations, laptops, and mobile devices used within the organization.

Specifications: Hardware specifications, configurations, and installed software.

Network Equipment

Description: A list of network devices, including routers, switches, and firewalls.

Specifications: Device details, configurations, and firmware versions.

3. Software Inventory

Operating Systems

Description: An inventory of all operating systems used across the organization.

Licensing: Licensing details, including the number of licenses and expiration dates.

Application Software

Description: A list of all applications used, including commercial, open-source, and custom applications.

[18] These assets include, but are not limited to, hardware, software, data and information, networking equipment, and cloud services.

Licensing: Licensing details and compliance for commercial software.

Versions: Application versions and update status.

4. Security Tools and Systems
Antivirus and Endpoint Protection
Description: Antivirus and endpoint protection solutions used.

Update Status: Update frequency and protection status.

Firewalls and Intrusion Detection/Prevention Systems
Description: Firewalls and intrusion detection/prevention systems in use.

Configuration: Firewall rules, intrusion detection configurations, and event monitoring.

5. Data Storage and Backup
Data Storage Systems
Description: An inventory of data storage systems, including NAS and SAN devices.

Specifications: Storage capacity, configurations, and data redundancy.

Backup and Recovery Systems
Description: An inventory of backup and disaster recovery solutions in use.

Backup Schedules: Backup schedules, procedures, and retention policies.

6. Cloud Services
Cloud Service Providers
Description: A list of cloud service providers used by the organization.

Services: Cloud services, subscriptions, and configurations.

7. Compliance and Legal Considerations
Applicable Laws and Regulations: Laws, regulations, or industry standards impacting technology inventory and management.

Compliance Measures: Procedures for ensuring compliance with relevant requirements.

8. Conclusion
Summary of the technology inventory assessment.
Identification of key technology assets and configurations.

9. Review and Update
Schedule for periodic reviews and updates of the technology inventory assessment.
Procedure for including new technology assets and resources in the assessment.

10. Glossary
Definitions of key terms and acronyms used in the document.

Security Infrastructure Design

Develop security infrastructure and technology standards.

Security Infrastructure Design

Date: [Date]

1. Introduction
Purpose: This document outlines the design of [Organization Name]'s security infrastructure and technology standards.

Scope: The design covers all security-related technology and infrastructure used or managed by [Organization Name].

2. Security Infrastructure Components
Network Security
Description: Overview of network security components and technologies.

Firewall Configuration: Firewall rules, configurations, and segmentation.

Endpoint Security
Description: Overview of endpoint security components and technologies.

Antivirus and Malware Protection: Endpoint protection solutions and configurations.

Patch Management: Procedures for patching and updating endpoints.

Intrusion Detection/Prevention Systems (IDS/IPS)
Description: Overview of IDS/IPS solutions.

Configuration: IDS/IPS rule sets, monitoring, and response procedures.

Secure Email and Web Gateway
Description: Overview of email and web security components.

Email Filtering: Anti-phishing, anti-spam, and email encryption.

Web Filtering: URL filtering, content inspection, and web application security.

Server Infrastructure

Description: Overview of the security configurations of server infrastructure components and technologies (e.g., physical, virtual, cloud)

Server Hardening: Hardware security features like Trusted Platform Module (TPM) or Hardware Security Modules (HSMs); disabling unnecessary services; minimizing exposed attack surface.

Configuration & Patch Management: Role-based configuration; least privilege enforcement; active monitoring and patching; centralized logging.

Container/Virtualization Security: Isolation mechanisms to prevent access between containers; hardening hypervisors; virtual network segmentation between environments; security orchestration.

Identity and Access Management (IAM)

Description: Overview of IAM components and technologies.

User Authentication: Authentication methods, including multi-factor authentication.

Access Control: Role-based access control (RBAC) and identity lifecycle management.

3. Security Technology Standards

Encryption Standards

Data Encryption: Data at rest and data in transit encryption standards.

Key Management: Procedures for key generation, storage, and rotation.

Authentication Standards

Authentication Protocols: Protocols used for user authentication.

Password Policies: Password complexity requirements and management.

Logging and Monitoring Standards

Log Retention: Procedures for log retention and archival.

Monitoring: Tools and practices for monitoring security events.

Incident Response Standards

Incident Categorization: Categorization of incidents and response procedures.

Escalation Procedures: Escalation paths for incidents.

4. Security Policy Compliance
Policy Enforcement: Procedures for enforcing security policies and standards.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

5. Compliance and Legal Considerations
Applicable Laws and Regulations: Laws, regulations, or industry standards impacting security infrastructure design.

Compliance Measures: Procedures for ensuring compliance with relevant requirements.

6. Conclusion
Summary of the security infrastructure design and technology standards.
Identification of key security components and standards.

7. Review and Update
Schedule for periodic reviews and updates of the security infrastructure design and technology standards.
Procedure for including new security technologies and standards in the design.

8. Glossary
Definitions of key terms and acronyms used in the document.

Network Security Architecture and Controls

Define network security architecture and controls.

Network Security Architecture and Controls

Date: [Date]

1. Introduction
Purpose: This document outlines the network security architecture and controls for [Organization Name] to protect its network infrastructure from threats and vulnerabilities.

Scope: The network security architecture and controls cover all network components and technologies used or managed by [Organization Name].

2. Network Security Architecture

Perimeter Security

Description: Overview of perimeter security components and technologies.

Firewall Configuration: Firewall rules, configurations, and segmentation.

Intrusion Detection/Prevention: IDS/IPS solutions, monitoring, and response.

Internal Network Security

Description: Security controls and technologies used within the internal network.

Network Segmentation: Segmentation practices to isolate network segments (e.g., VLANs, network ACLs, air gapped).

Access Control: Access control lists (ACLs) and network access policies.

Secure Remote Access

Description: Remote access technologies and security measures.

Virtual Private Network (VPN): VPN technologies, configurations, and access policies.

Multi-Factor Authentication (MFA): MFA for remote users and security tokens.

Wireless Network Security

Description: Security controls for wireless networks.

Encryption: Wireless encryption protocols and key management.

Guest Network: Isolation of guest networks and access controls.

3. Network Security Controls

Firewall and Intrusion Detection/Prevention

Firewall Rules: Rules governing traffic and traffic filtering.

IDS/IPS Configuration: Configuration of IDS/IPS systems and response procedures; to include device cut sheets detailing technical configuration.

Access Control

Access Control Lists (ACLs): ACL configurations for network security.

Role-Based Access Control (RBAC): Role definitions and access permissions.

Encryption

Data Encryption: Data at rest and data in transit encryption standards.

Key Management: Key generation, storage, and rotation procedures.

Monitoring and Logging

Log Retention: Log retention policies and archival procedures.

Security Event Monitoring: Tools and practices for monitoring security events.

Incident Response

Incident Categorization: Incident categories and response procedures.

Escalation Procedures: Escalation paths for security incidents.

4. Compliance and Legal Considerations

Policy Enforcement

Procedures for enforcing network security policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

5. Conclusion

Summary of the network security architecture and controls.

Identification of key network security components and controls.

6. Review and Update

Schedule for periodic reviews and updates of the network security architecture and controls.

Procedure for including new network security technologies and controls in the design.

7. Glossary

Definitions of key terms and acronyms used in the document.

Identity and Access Management

Establish user and device authentication, authorization, and management processes.

Identity and Access Management (IAM) Framework

Date: [Date]

1. Introduction

Purpose: This document defines the IAM framework for [Organization Name] to establish robust user and device authentication, authorization, and management processes.

Scope: The IAM framework applies to all users and devices accessing [Organization Name]'s resources and systems.

2. IAM Components and Technologies

User Authentication

Description: Overview of authentication mechanisms to verify user identities.

Password-Based Authentication: Password complexity policies and practices.

Multi-Factor Authentication (MFA): MFA technologies and configurations.

User Authorization

Description: Controls and technologies for authorizing user access.

Role-Based Access Control (RBAC): Role definitions and access permissions.

Attribute-Based Access Control (ABAC): ABAC policies and attributes.

Device Authentication and Management

Description: Technologies and policies for device authentication and management.

Device Enrollment: Procedures for device registration and authentication.

Mobile Device Management (MDM): MDM solutions and configurations.

Single Sign-On (SSO)

Description: SSO solutions for seamless user access to multiple applications.

SSO Integration: Applications and services integrated with SSO.

SSO Authentication Protocols: Protocols used for SSO authentication.

3. IAM Policies and Processes:

User Account Lifecycle

User Onboarding: Procedures for creating new user accounts.

Account Maintenance: Account updates, changes, and access reviews.

User Offboarding: Account deactivation and data removal procedures.

Access Requests and Approval

Access Request Procedures: How users request access to resources.

Approval Workflows: Procedures for access approval and role assignment.

Password Management

Password Policies: Password complexity requirements and change procedures.

Self-Service Password Reset (SSPR): SSPR implementation.

Incident Response

Incident Categorization: Incident categories and response procedures.

Escalation Procedures: Escalation paths for security incidents.

4. Compliance and Legal Considerations

Policy Enforcement

Procedures for enforcing IAM policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

5. Conclusion

Summary of the IAM framework, components, policies, and processes.

Identification of key IAM components and practices.

6. Review and Update

Schedule for periodic reviews and updates of the IAM framework and policies.

Procedure for including new IAM technologies and practices in the framework.

7. Glossary

Definitions of key terms and acronyms used in the document.

Physical Layer

Physical Security Controls

Define physical security measures to protect facilities and assets.

Physical Security Controls Framework

Date: [Date]

1. Introduction

Purpose: This document defines the physical security controls framework for [Organization Name] to protect its facilities and assets from unauthorized access, theft, and other physical threats.

Scope: The framework applies to all physical security measures used at [Organization Name]'s facilities and assets.

2. Physical Access Control

Access Points

Description: Overview of access points and entryways.

Access Control Systems: Access control technologies, such as card readers and biometric scanners.

Visitor Management: Procedures for managing and controlling visitor access.

Key Management

Description: Key management policies and practices.

Key Issuance: Procedures for issuing and tracking physical keys.

Key Replacement and Revocation: Procedures for replacing lost keys and revoking access.

3. Surveillance and Monitoring

CCTV and Video Surveillance

Description: CCTV and video surveillance systems used for facility monitoring.

Camera Placement: Locations of surveillance cameras and coverage areas.

Data Storage and Retention: Procedures for storing and retaining surveillance footage.

Intrusion Detection

Description: Intrusion detection systems and technologies.

Sensors and Alarms: Types of intrusion sensors and alarm systems in place.

Physical Inventory Management: Label, catalog and inventory all physical assets.

Alerting and Response: Procedures for alerting and responding to intrusions.

4. Security Personnel and Procedures

Security Staffing

Description: Roles and responsibilities of security personnel.

Guard Shifts: Scheduling and shifts for security staff.

Training and Certification: Training requirements and certifications for security personnel.

Emergency Procedures

Description: Procedures for handling emergencies, such as fire, natural disasters, or security incidents.

Evacuation Plans: Evacuation routes and assembly points.

Key Contacts: List of approved [19]contacts (to include law enforcement, regulators, and key service providers) that need to be contacted in the event of an emergency.

Incident Response: Procedures for responding to security incidents.

5. Perimeter Security

Fencing and Barriers

Description: Fencing and barriers to secure facility perimeters.

Security Gates: Access control at entry and exit gates.

Vehicle Access Control: Procedures for controlling vehicle access.

Lighting

Description: Exterior lighting for enhancing visibility, security, and safety.

Lighting Coverage: Areas covered by security lighting.

Maintenance: Procedures for lighting maintenance.

[19] Recommend vetting contact list with general counsel to protect against compliance or legal risks often associated with emergent situations.

6. Compliance and Legal Considerations

Policy Enforcement: Procedures for enforcing physical security policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

7. Conclusion

Summary of the physical security controls framework and measures.

Identification of key physical security components and practices.

8. Review and Update

Schedule for periodic reviews and updates of the physical security controls framework.

Procedure for including new physical security technologies and practices in the framework.

9. Glossary

Definitions of key terms and acronyms used in the document.

Data Center Security

Establish measures to secure data centers and physical infrastructure.

Data Center Security Framework

Date: [Date]

1. Introduction

Purpose: This document defines the data center security framework for [Organization Name] to protect its data centers, physical infrastructure, and the critical assets housed within.

Scope: The framework applies to all data centers and physical infrastructure managed by [Organization Name].

2. Access Control and Authentication

Data Center Access

Description: Overview of access points and entryways to data centers.

Access Control Systems: Technologies used for access control, such as card readers and biometric scanners.

Visitor Management: Procedures for managing and controlling visitor access.

Biometric Authentication

Description: Implementation of biometric authentication for critical access points.

Biometric Technologies: Types of biometric technologies employed for authentication.

User Enrollment: Procedures for enrolling authorized personnel.

3. Surveillance and Monitoring

CCTV and Video Surveillance

Description: CCTV and video surveillance systems used for data center monitoring.

Camera Placement: Locations of surveillance cameras and coverage areas within data centers.

Data Storage and Retention: Procedures for storing and retaining surveillance footage.

Environmental Monitoring

Description: Sensors and monitoring systems for environmental conditions.

Temperature and Humidity: Monitoring and alerting for temperature and humidity.

Fire Detection: Fire detection systems and response procedures.

Fire Suppression: System designed for data center environments with regular testing and maintenance.

4. Access Control and Authorization

Access Control Policies

Description: Policies governing access control within data centers.

Role-Based Access Control (RBAC): Role definitions and access permissions.

Authorization Procedures: Authorization for specific data center resources.

Change Control

Description: Procedures for controlling changes and modifications to data center infrastructure.

Change Request Process: Request, approval, and implementation procedures.

Change Auditing: Auditing and verification of changes.

5. Physical Security Staff and Procedures

Security Personnel

Description: Roles and responsibilities of security personnel dedicated to data center security.

Guard Shifts: Scheduling and shifts for security staff.

Training and Certification: Training requirements and certifications for security personnel.

Incident Response

Description: Procedures for handling security incidents within data centers.

Incident Categorization: Incident categories and response procedures.

Escalation Procedures: Escalation paths for security incidents.

6. Perimeter Security

Perimeter Barriers

Description: Barriers securing the perimeter of data center facilities.

Security Gates: Access control at entry and exit gates.

Vehicle Access Control: Procedures for controlling vehicle access.

Lighting and Alarms

Description: Exterior lighting and alarm systems for enhancing security.

Lighting Coverage: Areas covered by security lighting.

Alarm Configuration: Alarm systems and response procedures.

Cabinet Locks

Description: Secure server cabinets with locks.

Key Inventory: Procedures are in place to ensure only authorized personnel have access to keys.

7. Compliance and Legal Considerations

Policy Enforcement: Procedures for enforcing data center security policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

8. Conclusion
   Summary of the data center security framework and measures.

   Identification of key data center security components and practices.

9. Review and Update
   Schedule for periodic reviews and updates of the data center security framework.

   Procedure for including new security technologies and practices in the framework.

10. Glossary
    Definitions of key terms and acronyms used in the document.

Environmental Controls

Ensure appropriate environmental conditions for technology equipment.

Environmental Controls Framework

Date: [Date]

1. Introduction
Purpose: This document defines the environmental controls framework for [Organization Name] to ensure the appropriate environmental conditions necessary to support technology equipment and infrastructure.

Scope: The framework applies to all areas housing technology equipment and infrastructure managed by [Organization Name].

2. Temperature and Humidity Controls
Temperature Monitoring
   Description: Overview of temperature monitoring systems.

   Monitoring Points: Locations of temperature sensors and monitoring points.

   Threshold Alerts: Temperature threshold alerts and response procedures.

Humidity Control
   Description: Control mechanisms to maintain optimal humidity levels.

   Dehumidification Systems: Dehumidification equipment and configurations.

   Humidity Alarms: Humidity level alarms and response procedures.

3. Fire Detection and Suppression

Fire Detection Systems

Description: Fire detection systems and technologies.

Smoke and Heat Detectors: Types of detectors used for fire detection.

Alarm and Notification: Procedures for alerting and responding to fire incidents.

Testing: Procedures and schedule for testing fire detection are documented and reported on.

Fire Suppression Systems

Description: Fire suppression mechanisms to mitigate fire damage.

Fire Suppression Agents: Types of fire suppression agents used.

Deployment and Activation: Procedures for deploying and activating fire suppression systems.

Maintenance: Procedures and schedule for fire suppression maintenance are defined and reported on, with deficiencies generating corrective action plans as appropriate.

4. Power and Backup Systems

Power Redundancy

Description: Redundant power sources to ensure uninterrupted operations.

Primary and Secondary Power: Sources and configuration of primary and secondary power.

Automatic Transfer Switch (ATS): ATS systems and operation.

Uninterruptible Power Supply (UPS)

Description: UPS systems to provide backup power.

UPS Configuration: UPS configurations, capacity, and runtime.

Battery Testing and Maintenance: Procedures and schedule for battery testing and maintenance are documented and reported on.

5. Security and Access Control

Access Control

Description: Access controls to prevent unauthorized access.

Authorized Personnel: Procedures for granting access to authorized personnel.

Visitor Access: Procedures for managing visitor access.

Environmental Monitoring

Description: Environmental condition monitoring systems.

Data Logging: Data logging and real-time monitoring of environmental conditions.

Alerting and Notifications: Procedures for alerting and responding to environmental alerts.

6. Compliance and Legal Considerations

Policy Enforcement: Procedures for enforcing environmental controls policies and measures.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

7. Conclusion

Summary of the environmental controls framework and measures.

Identification of key components and practices for maintaining appropriate environmental conditions.

8. Review and Update

Schedule for periodic reviews and updates of the environmental controls framework.

Procedure for including new environmental control technologies and practices in the framework.

9. Glossary

Definitions of key terms and acronyms used in the document.

Human Layer

Security Awareness and Training

Develop security awareness programs and training for employees.

Security Awareness and Training Program

Date: [Date]

1. Introduction

Purpose: This document defines the security awareness and training program for [Organization Name] to educate and empower employees to effectively contribute to the organization's security.

Scope: The program covers all employees and contractors within [Organization Name].

2. Training Objectives

Security Awareness Goals

Description: High-level objectives for security awareness initiatives.

Employee Understanding: Ensure employees understand security risks and best practices.

Risk Mitigation: Equip employees to mitigate security threats.

Skills Development

Description: Goals for skill development through training.

Safe Computing: Develop skills in secure computing practices.

Incident Reporting: Empower employees to report security incidents.

3. Training Programs and Modules

General Security Awareness

Description: General awareness programs for all employees.

Security Policies and Procedures: Training in organizational policies and procedures.

Phishing Awareness: Educate employees about recognizing phishing attempts.

Role-Based Training

Description: Specialized training based on employee roles.

IT Staff Training: Specialized training for IT and technical staff.

Management Training: Security leadership and management training.

Compliance and Regulatory Training

Description: Training related to industry-specific regulations.

Data Privacy Training: Compliance with data protection regulations.

Applicable Industry-specific Training: Training for compliance with industry-specific requirements (e.g., PCI DSS, HIPAA, etc.).

Testing and Assessments

Description: Evaluation methods to measure employee knowledge.

Simulated Phishing Tests: Periodic tests to assess email security awareness.

Knowledge Assessments: Periodic quizzes to evaluate understanding.

4. Training Delivery

Training Methods

Description: Methods used to deliver training content.

Instructor-Led Training: In-person or virtual classroom sessions.

Online Learning: E-learning modules and resources.

Frequency

Description: Frequency of training and awareness initiatives.

Initial Training: Training upon employee onboarding.

Periodic Training: Regular intervals for refresher courses.

5. Evaluation and Metrics

Assessment Criteria

Description: Criteria used to evaluate the effectiveness of training.

Knowledge Retention: Assessment of knowledge retention.

Incident Reporting: Measurement of incident reporting rates.

Feedback Mechanisms

Description: Mechanisms for employees to provide feedback.

Anonymous Surveys: Anonymous feedback collection.

Incident Reporting Channels: Reporting channels for incidents and feedback.

6. Compliance and Legal Considerations
   Policy Enforcement: Procedures for enforcing security awareness and training policies.

   Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

7. Conclusion
   Summary of the security awareness and training program.

   Identification of key training programs, modules, and metrics.

8. Review and Update
   Schedule for periodic reviews and updates of the security awareness and training program.

   Procedure for incorporating new training methods and modules.

9. Glossary
   Definitions of key terms and acronyms used in the document.

Human Resource Security

Define hiring, onboarding, and offboarding security procedures.

Human Resource Security Procedures

Date: [Date]

1. Introduction
Purpose: This document defines the human resource security procedures for [Organization Name] to manage the security aspects and obligations of employee and contractor lifecycle, including hiring, onboarding, and offboarding.

Scope: The procedures apply to all employees, contractors, and temporary staff engaged by [Organization Name].

2. Hiring Process
Security Screening
   Description: Procedures for security screening during the hiring process.

   Background Checks: Background check requirements and procedures.

Reference Checks: Reference verification for candidates.

Security Agreements

Description: Agreements and policies communicated during hiring.

Non-Disclosure Agreements (NDAs): NDAs for handling sensitive information.

Acceptable Use Policy (AUP): Acknowledgment of AUP compliance.

Acknowledgements: Procedures are established to capture and maintain all security agreements required by the organization.

3. Onboarding

Security Training

Description: Security training during the onboarding process.

Security Policies: Employee acknowledgment of security policies.

Awareness Training: Training on security awareness and best practices.

Access Control

Description: Procedures for granting access to systems and facilities.

User Account Creation: Procedures for creating user accounts.

Role-Based Access Control (RBAC): Role assignment, access and authorization procedures are defined and validated for all new hires.

4. Promotions/Transfers

Access Control

Description: Procedures for revoking and establishing new access and authorization requirements are defined and followed.

User Account Modification: Procedures for modifying user accounts based on promotion or transfer to new roles are defined.

Role-Based Access Control (RBAC): Role assignment, access and authorization procedures are defined and validated.

5. Offboarding

Access Termination

Description: Procedures for revoking access upon employee departure.

Account Deactivation: Deactivation of system and facility access.

Return of Assets: Procedures for returning organization assets.

Data Removal

Description: Procedures for data removal and protection.

Data Backup: Data backup before account deactivation.

Data Erasure: Secure data erasure and disposal.

6. Reporting Security Incidents

Incident Reporting

Description: Procedures for employees and contractors to report security incidents.

Reporting Channels: Methods for reporting incidents.

Whistleblower Protection: Protection for whistleblowers.

7. Compliance and Legal Considerations

Policy Enforcement: Procedures for enforcing human resource security policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

8. Conclusion

Summary of the human resource security procedures.

Identification of key security measures during the employee and contractor lifecycle.

9. Review and Update

Schedule for periodic reviews and updates of the human resource security procedures.

Procedure for incorporating new security procedures and legal requirements.

10. Glossary

Definitions of key terms and acronyms used in the document.

Monitor and manage user behavior for security purposes.

Behavioral Profiling for Security

Date: [Date]

1. Introduction

Purpose: This document defines the behavioral profiling procedures for [Organization Name] to monitor and manage user behavior for security purposes.

Scope: The procedures apply to all employees, contractors, and users interacting with [Organization Name]'s systems and resources.

2. Behavioral Profiling Objectives

Threat Detection

Description: Objectives for detecting potential security threats.

Anomalous Behavior: Identification of unusual or suspicious behavior.

Insider Threat Detection: Detection of malicious or unintentional insider threats.

Policy Compliance

Description: Objectives for ensuring policy compliance.

User Policy Adherence: Monitoring user adherence to security policies.

Data Access Control: Monitoring access and data handling practices.

3. Data Collection and Analysis

Data Sources

Description: Sources of data for behavioral profiling.

System Logs: The proper configuration [20]and collection of system logs and audit trails.

User Activity Logs: User-specific activity logs.

Data Analysis

Description: Procedures for analyzing collected data.

[20] Maintain adequate configuration to capture access and activities within systems; this is dependent upon the needs and requirements unique to each organization.

Security Baseline Establishment: Methods and frequency in which security baselines are established, validated, and verified. To find bad, you need to know what good looks like.

Anomaly Detection: Algorithms and methods for anomaly detection.

Pattern Recognition: Identification of behavioral patterns.

4. Alerting and Response

Alerting Mechanisms

Description: Procedures for generating alerts based on profiling.

Alert Thresholds: Definition of alerting thresholds and criteria.

Alert Channels: Methods for notifying security teams.

Incident Response

Description: Procedures for responding to detected anomalies.

Incident Categorization: Categorization of behavioral incidents.

Escalation Procedures: Escalation paths for incident response.

5. User Privacy and Legal Considerations

User Consent

Description: Procedures for obtaining user consent for profiling.

Consent Notifications: Notices provided to users who consent to share their data.

Privacy Policy: Policy defining how, what, and why data is being collected, as well as how that data will be protected and retired once it's business use has expired.

Opt-Out Mechanisms: Mechanisms for users to opt out.

Data Protection

Description: Procedures for protecting user data and privacy.

Data Encryption: Encryption of user data in transit and at rest.

Data Retention: Data retention policies and practices.

6. Compliance and Legal Considerations

Policy Enforcement: Procedures for enforcing behavioral profiling policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

7. Conclusion

Summary of the behavioral profiling procedures.

Identification of key measures for monitoring and managing user behavior for security purposes.

8. Review and Update

Schedule for periodic reviews and updates of the behavioral profiling procedures.

Procedure for incorporating new profiling techniques and legal requirements.

9. Glossary

Definitions of key terms and acronyms used in the document.

Assurance Layer

Audit and Compliance

Establish auditing and compliance monitoring processes.

Audit and Compliance Framework

Date: [Date]

1. Introduction

Purpose: This document defines the audit and compliance framework for [Organization Name] to establish auditing and compliance monitoring processes that ensure adherence to organizational policies, industry standards, and legal requirements.

Scope: The framework applies to all business units, processes, and technology systems within [Organization Name].

2. Audit and Compliance Objectives

Regulatory Compliance

Description: Objectives for achieving regulatory compliance.

Industry Standards: Adherence to industry-specific standards.

Legal Requirements: Compliance with relevant legal requirements.

Risk Management

Description: Objectives for identifying and responding to risks.

Security Risks: Identification and mitigation of security risks.

Data Protection: Ensuring the protection of sensitive data and information.

3. Audit Planning and Execution

Audit Planning

Description: Procedures for planning audit activities.

Audit Scope: Definition of the scope and objectives of audits.

Audit Schedule: Scheduling of audit activities.

Audit Execution

Description: Procedures for conducting audits.

Data Collection: Collection of relevant audit data and evidence.

Interviews and Documentation: Interviews with personnel and document review.

4. Compliance Monitoring

Policy Compliance

Description: Procedures for monitoring policy compliance.

Policy Audits: Auditing organizational policies and procedures.

Policy Enforcement: Ensuring policies are enforced.

Incident and Non-Compliance Reporting

Description: Procedures for reporting and addressing incidents and non-compliance.

Incident Reporting: Methods for reporting security incidents.

Non-Compliance Remediation: Procedures for addressing non-compliance issues.

5. Reporting and Documentation

Audit Reports

Description: Content and format of audit reports.

Findings and Recommendations: Presentation of audit findings and recommendations.

Management Response: Management's response and action plan.

Compliance Documentation

Description: Maintenance of compliance documentation.

Compliance Records: Records of compliance audits and findings.

Document Retention: Procedures for document retention.

6. Training and Awareness

Training Programs

Description: Training and awareness programs for audit and compliance personnel.

Audit Training: Training for audit staff.

Compliance Awareness: Awareness programs for employees.

7. Compliance and Legal Considerations

Policy Enforcement: Procedures for enforcing audit and compliance policies and controls.

Compliance Monitoring: Monitoring and audit procedures for policy enforcement.

8. Conclusion

Summary of the audit and compliance framework.

Identification of key audit and compliance measures for maintaining security and adherence to policies and regulations.

9. Review and Update

Schedule for periodic reviews and updates of the audit and compliance framework.

Procedure for incorporating new audit and compliance practices and legal requirements.

10. Glossary

Definitions of key terms and acronyms used in the document.

Security Testing

Define methods for security testing, including penetration testing and vulnerability assessments.

Security Testing Framework

Date: [Date]

1. Introduction

Purpose: This document defines the security testing framework for [Organization Name] to establish methods and procedures for conducting security testing, including penetration testing and vulnerability assessments.

Scope: The framework applies to all technology systems, applications, and network infrastructure within [Organization Name].

2. Security Testing Objectives

Security Assessment

Description: Objectives for assessing the security posture are defined and aligned with business objectives and requirements.

Identify Vulnerabilities: Processes for the identification of vulnerabilities and weaknesses are defined.

Security Enhancement: Recommendations for security improvements are made as part of each test cycle providing actionable insights and corrective action to be taken.

Compliance Validation

Description: Objectives for ensuring compliance with security standards are defined and approved by senior management.

Regulatory Compliance: Compliance with relevant regulations has been identified and is maintained to address regulatory requirements.

Industry Standards: Adherence to industry-specific security standards is tailored in alignment with business requirements and organizational risk appetite.

3. Security Testing Types

Penetration Testing

Description: Procedures for conducting penetration tests are defined and repeatable to ensure consistency and quality of results.

Scope and Targets: Processes are in place to define the scope of testing.

Rules of Engagement: Processes are in place to define the rules and limitations/constraints for conducting specific tests.

Vulnerability Assessment

Description: Procedures for assessing vulnerabilities are defined.

Scanning and Assessment: The methods for scanning and assessment of vulnerabilities are defined and agreed upon by all parties involved.

Risk Prioritization: Prioritizing vulnerabilities is based on risk.

Code Review

Description: Procedures for reviewing and analyzing application code are defined and followed.

Threat Modeling: Procedures are established using an appropriate methodology[21].

[21] Each organization will need to identify their methodology of choice (e.g. Microsoft's STRIDE, persona non gratis, VerSprite's PASTA)

Secure Software Development Lifecycle: Processes are defined for the identification and remediation of vulnerabilities throughout the application's lifecycle.

4. Testing Tools and Resources

Penetration Testing Tools

Description: All software and tools will be documented and approved prior to use in testing. This includes any software associated with discovery, enumeration, probing, payload delivery and reporting used during a test.

Vulnerability Scanning Tools

Description: All software and tools used for the identification and reporting of vulnerabilities (e.g., platform, services, webapp, etc.) will be documented and approved prior to use.

Testing Environment

Description: An environment that mimics production and can be used for testing without impacting production operations. This requires a complete one-to-one match between the two environments (e.g., security controls, application code base, etc.).

5. Test Execution and Reporting

Testing Procedures

Description: Procedures for conducting security tests are defined and documented to ensure consistency and quality of testing.

Test Execution: Processes for the execution of penetration tests and vulnerability assessments are defined.

Test Data Collection: Processes for the identification, collection and management of data collected during testing are defined.

Reporting and Analysis

Description: Content and format of test reports.

Findings & Recommendations: Processes are defined to present the findings and corrective actions identified.

Management Response: Processes are defined to capture management's direction regarding report findings, recommendations and remediation plans originating from the results of testing.

6. Remediation and Follow-Up
Remediation Actions
Description: Procedures for addressing identified vulnerabilities are defined.

Remediation Planning: Planning for vulnerability remediation.

Verification Testing: Re-testing to verify remediation.

7. Compliance and Legal Considerations:
Testing Permissions
Description: Permissions and legal considerations for security testing.

Authorization: Authorization for security testing activities.

Legal Compliance: Compliance with relevant laws and regulations.

8. Conclusion
Summary of the security testing framework.

Identification of key measures for assessing security, enhancing compliance, and addressing vulnerabilities.

9. Review and Update
Schedule for periodic reviews and updates of the security testing framework.

Procedure for incorporating new testing methods and tools.

10. Glossary
Definitions of key terms and acronyms used in the document.

Develop an incident response plan and procedures.

Incident Response Plan

Date: [Date]

1. Introduction
Purpose: This document defines the incident response plan for [Organization Name] to establish procedures for effectively responding to security incidents and minimizing their impact.

Scope: The plan covers all technology systems, applications, and network infrastructure within [Organization Name].

2. Incident Response Objectives
Incident Identification

Description: Objectives for identifying and classifying incidents.

Timely Detection: Prompt detection of security incidents.

Incident Classification: Categorization of incidents by severity.

Incident Containment

Description: Objectives for containing and mitigating incidents.

Rapid Response: Quick containment to prevent further damage.

Minimizing Impact: Actions to minimize the impact of incidents.

3. Incident Classification
Incident Categories[22]

Description: Classification of incidents into categories.

Data Breaches: Incidents involving unauthorized access to data.

Malware Infections: Incidents related to malware or viruses.

Severity Levels

Description: Severity levels assigned to each incident category.

[22] Each organization will need to define their own incident categories, as there are any number of natural, intentional/unintentional, and element-based incidents which may occur.

Low, Medium, High: Classification based on impact and urgency.

4. Incident Response Team

Roles and Responsibilities

Description: Roles and responsibilities of the incident response team.

Incident Management Team: Those individuals who are responsible for managing incidents. This needs to be a cross-functional team from within the organization.

Incident Coordinator: Leadership role in managing the response.

Technical Specialists: Technical experts for triage, forensic analysis, and containment efforts.

Critical Contacts: A list of all key personnel involved needs to be created, maintained, reviewed, and updated as needed on a recurring, periodic basis[23].

Communication Procedures

Description: Procedures for internal and external communication.

Reporting Incidents: How to report incidents to the response team.

Stakeholder Notifications: Communication with relevant internal and external stakeholders.

5. Incident Response Procedures

Incident Triage

Description: Triage procedures for incident assessment.

Initial Assessment: Assessing the nature and scope of the incident.

Determining Severity: Assigning severity levels based on impact.

Containment and Eradication

Description: Procedures for containing and eradicating incidents.

Isolation: Isolating affected systems or networks.

Eradication: Procedures for removing the cause of the incident.

[23] Frequency of review and updates will be based on the size and turnover of organizational IR staff. For environments with low turnover, this may be done annually. For high turnover environments, this should be done quarterly. If the organization uses a third-party provider, quarterly reviews are recommended.

Lessons Learned

Description: Review of how the incident was managed, business efforts recovered and resumed, and what allowed the incident to occur.

Incident Review: Review of the practices, processes and activities associated with incident response efforts to identify efficient and effective gains.

Root-cause Analysis: Identifying what allowed the incident to occur.

6. Reporting and Documentation

Incident Reporting

Description: Procedures for documenting incidents.

Incident Reporting Forms: Forms and templates for incident reports.

Documentation Standards: Standards for documentation.

Post-Incident Review

Description: Procedures for post-incident review and analysis.

Lessons Learned: Identification of lessons learned.

Process Improvement: Recommendations for process improvement.

7. Legal and Regulatory Considerations

Legal Compliance

Description: Procedures for legal and regulatory compliance.

Data Breach Notification: Compliance with data breach notification laws.

Evidence Preservation: Procedures for preserving evidence.

8. Conclusion

Summary of the incident response plan.

Identification of key procedures for incident identification, containment, and documentation.

9. Review and Update

Schedule for periodic reviews and updates of the incident response plan.

Procedure for incorporating new incident handling techniques and legal requirements.

10. Glossary

Definitions of key terms and acronyms used in the document.

Security Services

Security Services Catalog

Define a catalog of security services provided to the organization.

Security Services Catalog

Date: [Date]

1. Introduction

Purpose: This document defines the comprehensive security services catalog for [Organization Name] to provide a detailed list of security services available to support the organization's security needs.

Scope: The catalog covers all security services provided to [Organization Name] and its various business units. It aligns with the Enterprise Security Framework and integrates with business and IT strategies.

2. Catalog Structure

Service Categories

Business Security Services: Services designed to safeguard and enable business processes and assets.

Information Security Services: Services focused on protecting critical information assets.

Technical Security Services: Services for securing the technical infrastructure and platforms.

Service Offerings

Security Architecture Design: Development of security architectures based on the enterprise security framework.

Security Governance and Risk Management: Managing security governance and risk in alignment with enterprise security principles.

3. Service Descriptions

Service Title: Security Architecture Design

Description: Development of security architectures based on the enterprise security framework.

Service Overview: This service entails creating security architectures that align with business requirements and objectives while incorporating the various layers of the enterprise security framework: Business Context, Information, Application, Logical, Physical, and Component. The architectures are designed to support the organization's strategy and risk profile.

Key Features

Business-Driven Security: Aligning security measures with business processes and objectives, as per Business layer.

Risk Management: Incorporating risk management principles and practices in line with guidelines, addressing risk at each layer.

Service Lifecycle

Initiation: Define the security architecture project based on business requirements and risk assessments.

Design: Develop the architecture considering the FESA framework layers and risk assessments.

Implementation: Implement security measures and controls as per the designed architecture.

Monitoring: Continuously monitor the architecture's performance and adapt as needed.

Continuous Improvement: Regularly update the architecture based on evolving business and risk requirements.

Service Dependencies

This service may depend on inputs from risk assessments, business requirements, and the output of security governance processes.

Service Interactions

It interacts with other security services such as risk management, compliance monitoring, and incident response to achieve an integrated and cohesive security posture.

Service Metrics and KPIs

Metrics include alignment with business objectives, risk reduction, and compliance with enterprise security principles.

Service Title: Security Governance and Risk Management

Description: Managing security governance and risk in alignment with framework principles.

Service Overview: This service is designed to establish and maintain effective security governance aligned with the framework principles. It includes the definition of security policies, risk assessments, compliance management, and the continuous monitoring of security controls to ensure they align with the enterprise security framework.

Key Features

Policy Development: Creating security policies consistent with the enterprise security framework, ensuring they are aligned with business objectives.

Risk Assessment Process: Implementing a structured risk assessment process following risk management guidelines.

Compliance Monitoring: Continuously monitoring and ensuring compliance with business-aligned security controls.

Service Lifecycle

Initiation: Define security governance and risk management objectives based on business-aligned principles.

Policy Development: Develop security policies consistent with the framework and business objectives.

Risk Assessment: Conduct risk assessments, identifying, evaluating, and managing risks following enterprise guidelines.

Compliance Monitoring: Continuously monitor and report on compliance with business-aligned controls.

Continuous Improvement: Regularly update policies and risk management strategies based on enterprise requirements.

Service Dependencies

This service may depend on security policies, risk assessments, and inputs from security architecture design.

Service Interactions

It interacts with security architecture design, compliance monitoring, and incident response services to ensure alignment with framework principles and address identified risks.

Service Metrics and KPIs

Metrics include the alignment of security policies with framework principles, risk reduction, and compliance with business-aligned controls.

4. Service Delivery

Service Implementation: Security Architecture Design

Description: Procedures for implementing the service.

Methodology: Implement the framework for designing security architectures, addressing each layer systematically.

Risk Analysis: Conduct risk analysis at each layer following risk management principles and incorporate appropriate controls.

SLAs

Response Time: [Specify Response Time]

Availability: [Specify Availability]

Service Dependencies

Dependencies on risk assessments, policy adherence, and ongoing monitoring.

Service Implementation: Security Governance and Risk Management

Description: Procedures for implementing the service.

Policy Definition: Define security policies aligned with framework principles.

Risk Assessment Process: Implement a structured risk assessment process following risk management guidelines.

Compliance Monitoring: Continuously monitor and report on compliance with business-aligned security controls.

SLAs

Response Time: [Specify Response Time]

Compliance Reporting: [Specify Reporting Schedule]

Service Dependencies:

Dependencies on risk assessments, policy adherence, and inputs from security architecture design.

Service Management: Security Architecture Design

Description: Procedures for managing ongoing service delivery.

Architecture Review: Periodic reviews of security architectures to ensure alignment with evolving business needs and compliance with framework principles.

Integration with Projects: Integration of security architecture into ongoing projects and initiatives, applying framework principles.

Alignment with Business Strategy: Ensure that security architectures align with evolving business strategies as per framework's Business Context layer.

SLAs

Review Schedule: [Specify Review Schedule]

Integration Timelines: [Specify Integration Timelines]

Service Dependencies

Dependencies on ongoing risk assessments, policy updates, and business strategy changes.

Service Management: Security Governance and Risk Management

Description: Procedures for managing ongoing service delivery.

Policy Governance: Continuously manage and update security policies in line with business changes, framework principles, and risk assessments.

Ongoing Risk Management: Regularly assess and reassess risks to ensure alignment with changing business objectives and the framework.

Compliance Reporting: Periodic reporting on compliance with business-aligned security controls.

SLAs

Policy Updates: [Specify Update Schedule]

Risk Assessment Frequency: [Specify Assessment Frequency]

Compliance Reporting: [Specify Reporting Schedule]

Service Dependencies

Dependencies on risk assessments, policy adherence, and input from compliance monitoring.

5. Service Benefits

Value Proposition: Security Architecture Design

Description: The value and benefits of the service.

Business-Aligned Security: Security architectures that closely align with business objectives, as advocated by FESA framework's Business Context layer.

Effective Risk Management: Improved risk management based on the framework, ensuring security measures are commensurate with identified risks.

Business Impact Analysis

How the service affects critical business processes, data, and assets.

Incident Response Plan

Overview of the incident response plan for the service, including reporting, investigation, and mitigation procedures.

6. Contact Information:

Service Contact: Security Architecture Design

Description: Contact information for inquiries and service requests.

Lead Architect: [Name]
Architect's Contact: [Contact Information]

Service Contact: Security Governance and Risk Management

Description: Contact information for inquiries and service requests.

Governance Lead: [Name]
Governance's Contact: [Contact Information]
Risk Manager: [Name]
Risk's Contact: [Contact Information]

Service Contact: Incident Response

Description: Contact information for reporting incidents.
Incident Manager: [Name]
Incident Response Contact: [Incident Response Contact Information]

7. Conclusion

Summary of the Comprehensive Security Services Catalog with emphasis on alignment with the services being provided as part of the enterprise security framework and the incorporation of additional elements.

Identification of key service categories, offerings, and contact information.

8. Review and Update

Schedule for Periodic Reviews and Updates

This document will be reviewed and updated bi-annually to ensure its relevance, alignment with the framework, and inclusion of evolving business needs and risk assessments.

Procedure for Incorporating New Services and Adjusting Contact Information

New services or contact adjustments will be evaluated in accordance with principles and organizational objectives.

9. Glossary

Definitions of Key Terms and Acronyms used in the document, including those relevant to the framework.

Service-Level Agreements (SLAs)

Establish SLAs for security services.

Service-Level Agreements (SLAs) for Security Services

Date: [Date]

1. Introduction

Purpose: This document defines the Service-Level Agreements (SLAs) for security services provided by [Service Provider Name] to [Organization Name], outlining the agreed-upon performance metrics, responsibilities, and expectations.

Scope: These SLAs cover the security services provided to [Organization Name] as outlined in the security services catalog.

2. Service Descriptions

Service Title

Description: Name or title of the security service.

Security Assessment: Comprehensive security assessment and testing.

Incident Response: Response to security incidents and breaches.

Service Overview
Description: A brief description of the service.

Security Assessment: Comprehensive assessment of system vulnerabilities.

Incident Response: Rapid response to security incidents.

3. Service Provider Responsibilities
Service Implementation

Description: Responsibilities for implementing the service.

Security Assessment: Scheduling and executing assessments in a timely manner.

Incident Response: Providing 24/7 incident response services.

Service Management

Description: Responsibilities for managing ongoing service delivery.

Security Assessment: Generating detailed reports and offering remediation guidance.

Incident Response: Coordinating with internal teams and external resources for incident handling.

4. Service Metrics and Key Performance Indicators (KPIs):
Security Assessment Metrics

Description: Metrics and KPIs for the Security Assessment service.

Report Delivery Time:	Delivery of assessment reports within [Timeframe].
Vulnerability Remediation Time:	Timeframe for addressing identified vulnerabilities.

Incident Response Metrics

Description: Metrics and KPIs for the Incident Response service.

Incident Response Time:	Timely response within [Timeframe].
Incident Resolution Time:	Resolution of incidents within [Timeframe].

5. Performance Targets

Security Assessment Performance Targets

Description: Agreed-upon performance targets for the Security Assessment service.

Report Delivery Time Target: [Timeframe]

Vulnerability Remediation Time Target: [Timeframe]

Incident Response Performance Targets

Description: Agreed-upon performance targets for the Incident Response service.

Incident Response Time Target: [Timeframe]

Incident Resolution Time Target: [Timeframe]

6. Escalation Procedures

Escalation Contacts

Description: Contacts for addressing issues and escalations.

Primary Contact: [Contact Information]

Secondary Contact: [Contact Information]

Escalation Process

Description: Procedures for escalating issues and handling disputes.

Dispute Resolution: Steps for resolving disputes or performance issues.

7. Reporting and Review

Reporting Frequency

Description: Frequency of reporting and review.

Monthly Performance Reports: Monthly reports on service performance.

Quarterly Review Meetings: Quarterly meetings to review SLAs.

8. Compliance and Legal Considerations

Legal Compliance:

Description: Compliance with legal and regulatory requirements.

Data Protection Regulations: Compliance with data protection laws.

Confidentiality and Non-Disclosure: Protection of sensitive information.

9. Conclusion
   Summary of the Service-Level Agreements (SLAs) for security services.

   Identification of key service metrics, targets, and escalation procedures.

10. Review and Update
    Schedule for periodic reviews and updates of the SLAs.

    Procedure for modifying SLAs to reflect changing security needs or performance requirements.

11. Glossary
    Definitions of key terms and acronyms used in the document.

Security Architecture Framework

Create a framework for the integration and management of security services.

Security Architecture Framework

Date: [Date]

1. Introduction
Purpose: This document defines the Security Architecture Framework for [Organization Name] to create a structured approach for integrating and managing security services, ensuring the organization's security posture is aligned with its objectives.

Scope: The framework encompasses all technology systems, applications, and network infrastructure within [Organization Name].

2. Framework Objectives
Security Integration
   Description: Objectives for integrating security services seamlessly.

      Interoperability: Ensuring compatibility of security solutions.

      Efficiency: Enhancing operational efficiency through integration.

Risk Mitigation
   Description: Objectives for mitigating security risks.

      Threat Detection: Early threat detection and prevention.

      Compliance: Ensuring compliance with industry standards and regulations.

3. Architecture Components

Security Services

Description: Listing of security services available for integration.

Security Assessment: Comprehensive security assessment and testing.

Incident Response: Rapid response to security incidents.

Integration Points

Description: Points at which security services are integrated.

Network Security: Integration with network infrastructure.

Application Security: Integration with software applications.

4. Integration Design

Integration Patterns

Description: Design patterns for service integration.

Layered Security: Integration at multiple security layers.

Data Flow Control: Control points for data flow.

Data Flow Diagrams

Description: Diagrams illustrating data flow and integration points.

Network Data Flow: Visual representation of network data flow.

Application Data Flow: Visual representation of application data flow.

5. Security Service Management

Service Coordination

Description: Procedures for coordinating security services.

Incident Response: Coordination with internal teams and external resources.

Security Assessment: Integration with change management processes.

Monitoring and Analytics

Description: Monitoring and analytics to support service management.

Threat Intelligence: Integration of threat intelligence feeds.

Performance Metrics: Monitoring of service performance.

6. Compliance and Governance

Regulatory Compliance

Description: Ensuring compliance with regulatory requirements.

Data Protection: Compliance with data protection regulations.

Reporting and Auditing: Auditing to demonstrate compliance.

7. Scalability and Adaptability

Scalability

Description: Framework considerations for scalability.

Scalable Design: Design for accommodating growth.

Resource Allocation: Scalable allocation of resources.

Adaptability

Description: Framework considerations for adaptability.

Technology Upgrades: Integration with evolving security technologies.

Framework Flexibility: Adaptation to changing security needs.

8. Conclusion

Summary of the Security Architecture Framework

Identification of key framework components, integration points, and considerations for effective security service management.

9. Review and Update

Schedule for periodic reviews and updates of the Security Architecture Framework.

Procedure for adapting the framework to changing security needs and technologies.

10. Glossary

Definitions of key terms and acronyms used in the document.

Appendix A: Example Business Case for Foundational Enterprise Security Architecture

The following is meant as an example version of a Business Case for introducing and adopting the Foundational Enterprise Security Architecture (FESA) at Acme Corporation. Tailor according to the unique requirements of your organization.

1. Business Case

Acme Corporation recognizes that its digital assets and sensitive information are critical to its operations and growth. However, the organization currently faces various challenges related to security, compliance, and risk management. There is a pressing need to strengthen the security posture and ensure alignment with industry best practices. FESA offers a holistic approach to address these challenges by providing a comprehensive security framework tailored to Acme's business needs, reducing vulnerabilities, and enabling secure business operations.

2. Executive Summary

In today's interconnected and rapidly evolving business landscape, ensuring the safety, security and confidentiality of Acme Corporation's systems is paramount. The adoption of FESA will fortify our organization's defenses against cyber threats, enhance ability to demonstrate compliance, and align security efforts with our strategic goals. It will enable us to protect our assets, ensure data integrity, and maintain a competitive edge in the marketplace.

3. Background

Acme Corporation operates in a highly competitive industry where confidentiality, integrity, and availability of information are crucial. The increasing complexity of IT systems and the growing threat landscape necessitate a structured approach to security. FESA is needed to provide a robust security framework that aligns with the organization's business objectives and risk management priorities.

4. Business Challenges

Presently, there is a disconnect between the revenue generating lines of business, Information Technology and Security Operations. This has resulted in the following:

- Inadequate alignment of security measures with business objectives.
- Lack of a comprehensive security framework.
- Increasing regulatory compliance requirements.
- Rising cybersecurity threats and vulnerabilities.
- Inefficient risk management practices.

5. Gap Analysis & Goal Identification

The organization currently lacks a structured approach to security that aligns with business needs and risk management. The goal of FESA adoption is to bridge these gaps and create an enterprise security architecture that is closely integrated with our business processes, thereby improving risk management, incident response capabilities and ability to demonstrate compliance.

6. Alternatives Considered

The alternatives considered for our enterprise's security architecture included:

- NIST Cybersecurity Framework v1.1
- ISO 27001
- The OpenGroup's O-ESA

However, these alternatives were not selected for the following reasons:

- *NIST Cybersecurity Framework v1.1*: While NIST CSF provides a robust framework for cybersecurity, it is primarily prescriptive in nature and was designed for government agencies and organizations dealing with critical infrastructure. Its extensive scope and level of detail may not be well suited to Acme Corporation's smaller size and cost leadership strategy.

- *ISO/IEC 27001*: While a widely recognized international standard for information security management, its implementation often requires substantial time, resources, and financial investment. Given our organization's size and the desire to exercise cost leadership, ISO 27001 was deemed less practical.

- *The OpenGroup's O-ESA*: The OpenGroup's O-ESA is a valuable framework, but it was not selected as it does not fully align with Acme Corporation's unique business needs and risk profile.

By choosing FESA, we can tailor our security architecture to our business context, ensuring a more effective and efficient alignment with our goals and constraints.

7. Proposed Solution

The Foundational Enterprise Security Architecture (FESA) framework was considered as the best fit for our specific requirements, organization size, maturity, while balancing resources constraints and commitments.

Phase 1 – High-level Pre-planning

1) Executive sponsorship and alignment with business objectives.
2) Identify key stakeholders and establish a governance structure.
3) Initial risk assessment and scoping.

Phase 2- Program Implementation

1) Develop a tailored yet detailed Fundamental ESA framework.
2) Align with IT architecture and compliance initiatives.
3) Define security control objectives.
4) Implement ESA across the organization.

Phase 3- After Action Review & Lessons Learned

1) Gather feedback and data.
2) Identify successes and challenges.
3) Develop recommendations for improvement.
4) Communicate the findings.
5) Develop a plan for continuous improvement.
6) Monitor and evaluate the FESA.

8. Program Scope

The Fundamental ESA framework will cover the entire organization and augment other business programs, including IT architecture, compliance, and risk management.

Figure 16 – High-level FESA Program Scope

The FESA methodology involves interactive workshops with stakeholders to ensure alignment with business objectives. As well as business integration activities, efforts for continuous improvements and definition of appropriate guidance and frameworks.

9. Program Deliverables

The planned outcomes produced by FESA include:

- Aligned security strategy with business objectives.
- Defined security policies, controls, and procedures.
- Improved risk management practices.
- Enhanced compliance with regulatory requirements.
- Strengthened cybersecurity posture.

10. Program Risk

The following are risks to successfully implementing ESA:

- Resistance to change among stakeholders.
- Insufficient funding and resources.
- Inconsistent stakeholder buy-in.
- Evolving cybersecurity threats.

11. Stakeholders

Stakeholders in the program include:

- Enterprise Risk Committee
- IT Executive Committee
- Governance Team
- Compliance Staff
- Local/Business Unit Management
- Information Technology Team
- Application Development Team
- Security Operations Team
- Internal Audit Services.

These stakeholders play a crucial role in providing guidance, setting priorities, and approving value objectives.

12. Cost-Benefit Analysis

Benefits to be realized after successful adoption of FESA include:

- Enhanced security and reduced risk
- Improved compliance and regulatory adherence
- Protection of brand reputation
- Increased operational efficiency
- Reduced cybersecurity incident costs

13. Return on Investment (ROI)

- Initial cost estimates and ongoing operational expenses
- Projected cost savings and ROI calculations

14. Challenges and Success Factors

By addressing these challenges and implementing the corresponding critical success factors, Acme Corporation can better navigate the complexities of FESA adoption and ensure successful implementation.

Challenge	Critical Success Factor
Resistance to Change	• Mitigate through committee structures within the group (to be agreed and constituted). • Ensure that implementation of the life cycle also includes change enablement activities.
Communication Gap between IT and the Business	• Involve all stakeholders.
Cost of Improvements Outweighing Perceived Benefits	• Focus on benefit identification.
Lack of Trust and Good Relationships Between IT and the Enterprise	• Foster open and transparent communication about performance, with links to enterprise performance management.
	• Focus on business interfaces and service mentality.
	• Publish positive outcomes and lessons learned to help establish and maintain credibility.
	• Ensure the CIO maintains credibility and leadership in building trust and relations.
	• Normalize governance roles and responsibilities in the business so accountability for decisions is clear.
	• Identify and communicate evidence of actual issues, risks to be mitigated, and business benefits associated with the proposed improvements.
	• Focus on change enablement planning.
Lack of Understanding of FESA Environment by Those Responsible for the GEIT Program	• Apply a consistent assessment methodology.
Various Levels of Complexity (Technical, Organizational, Operating Model)	• Treat the entities on a case-by-case basis. Benefit from lessons learned and sharing knowledge.
Understanding of FESA Frameworks, Procedures, and Practices	• Train key staff and mentor as needed.
Adoption of Improvements	• Enable empowerment at the practice area and business unit level.
Difficulty in Integrating FESA with the Governance Models of Outsourcing Partners	• Involve appropriate, strategic Third Parties in FESA activities.
	• Incorporate conditions and the right to audit inclusive of compliance, security, and privacy into contracts.
Failure to Realize FESA Implementation Commitments	• Set and manage expectations.
	• Keep it simple, realistic, and practical.
	• Break down the overall project into small achievable projects, building experience and benefits.
	• Apply program and project management principles.
	• Use milestones.

Challenge	Critical Success Factor
Trying to Do Too Much at Once; IT Tackling Overly Complex and/or Difficult Problems	• Prioritize tasks (Pareto principle 80% benefit with 20% effort) and be careful about sequencing in the correct order. Capitalize on quick wins.
	• Build trust and confidence. Have skills and experience to keep it simple and practical.
	• Reuse what is there as a base.
IT in Fire-Fighting Mode and/or Not Prioritizing (Unable to Focus on FESA)	• Apply good leadership skills.
	• Gain commitment and drive from top management so people are made available to focus on FESA.
	• Address root causes in the operational environment (external intervention, management prioritizing IT).
	• Apply tighter discipline over/management of business requests.
	• Obtain external assistance.
Absence of Required IT Skills and Competencies	• Focus on change enablement planning: Development, Training, Coaching, Mentoring, Feedback into the recruitment process, Cross-training.
Improvements Not Adopted or Applied	• Use a case-by-case approach with agreed principles for the entity to ensure practicality. It must be practical to implement.
Benefits Difficult to Show or Prove	• Identify performance metrics.
Loss of Interest and Momentum	• Build group-level commitment, including communication.

Table 10 – Challenges & Critical Success Factors (example only)

Appendix B: Enterprise Security Controls Index

Domain	Control	Category
Network	Application Controls	Network Security
Network	Email Inspection and Controls	Content Security
Network	Web Inspection and Controls	Content Security
Network	Firewall	Perimeter Defense
Network	Firewall	System Segmentation
Network	Intrusion Detection System	Perimeter Defense
Network	Intrusion Detection System	System Segmentation
Network	Intrusion Prevention System	Perimeter Defense
Network	Intrusion Prevention System	System Segmentation
Network	Monitoring & Reporting	Perimeter Defense
Network	Monitoring & Reporting	System Segmentation
Network	Packet/NetFlow Inspection	Perimeter Defense
Network	Packet/NetFlow Inspection	System Segmentation
Network	Geolocation	Network Security
Network	Network Time (NTP)	Network Security
Network	Network Access Controls	Network Security
Network	Application Control (APP FW)	Wireless
Network	Pre-Authentication (802.1x)	Wireless
Network	Guest Network	Wireless
Network	Encryption	Wireless
Network	Network Behavior Analysis	Monitoring
Network	Network Anomaly Detection	Monitoring
Network	Network Forensics	Monitoring
Network	Logging and Monitoring	Monitoring
Network	Monitoring	Managed Services
Network	Management	Managed Services
Network	DDoS Protection	Managed Services
Network	Layer 2 Encryption	Network Encryption
Network	Transport Layer Security	Network Encryption
Network	Virtual Private Network	Network Encryption
Network	Out of Band Networking	Network Security
End-point	Anti-Malware	Endpoint Defense
End-point	Host Firewall	Endpoint Defense
End-point	HIPS	Endpoint Defense
End-point	Application Control Listing	Endpoint Defense
End-point	Disk Encryption	Endpoint Security
End-point	Network Access Control	Endpoint Security
End-point	BYOD Security - Unified Endpoint Management	Endpoint Security
End-point	Remote Access/VPN	Endpoint Security
End-point	Security Configuration Baselines	Endpoint Security
End-point	Build Compliance Checking	Endpoint Security
End-point	Logging and Monitoring	Endpoint Security
End-point	Process Protection	Endpoint Security
End-point	Sandboxing	Endpoint Security
End-point	Memory Protection	Endpoint Security

Domain	Control	Category
Physical	Physical Access Control	Physical Security
Physical	Security Badge/Passes - Identity	Physical Security
Physical	CCTV Monitoring	Physical Security
Physical	Physical Access Control	Physical Security
Physical	Cabinet Locking	Physical Security
Physical	Rack Locking	Physical Security
Web Services	Direct Authentication	Web Security Services
Web Services	Brokered Authentication	Web Security Services
Web Services	Data Confidentiality	Web Security Services
Web Services	Data Origin Authentication	Web Security Services
Web Services	Logging and Monitoring	Web Security Services
Data	Database Encryption	Database Security
Data	Database Assessment	Database Security
Data	Database Activity Monitoring	Database Security
Data	CASB - DLP	Data Security
Data	Storage DLP	Data Loss Prevention
Data	Database DLP	Data Loss Prevention
Data	Physical Media Control	Data Loss Prevention
Data	Network DLP	Data Loss Prevention
Data	Endpoint DLP	Data Loss Prevention
Data	Content Discovery	Data Loss Prevention
Data	Email DLP	Data Loss Prevention
Data	Web Gateway DLP	Data Loss Prevention
Data	File/Folder	Encryption
Data	E-mail Encryption	Encryption
Data	SAN/NAS Encryption	Encryption
Data	Application Encryption	Encryption
Data	Entitlement Management	Access Management
Data	File Activity Monitoring	Access Management
Data	Logging and Monitoring	Data Security
IAM	Directory Replication	Directories
IAM	Directory Authentication and Authorization	Directories
IAM	Role Based Access	Recertification & Toxic Combinations
IAM	Incompatible Role Definitions	Recertification & Toxic Combinations
IAM	Toxic Combination Detection	Recertification & Toxic Combinations
IAM	Access Recertification	Recertification & Toxic Combinations
IAM	Joiners, Movers & Leavers	Provisioning
IAM	Device Identities	Provisioning
IAM	Authoritative Source	Provisioning
IAM	Generic Account Management	Provisioning
IAM	Service Account Management	Provisioning
IAM	Browser Based Federation	Federation
IAM	Web Services	Federation
IAM	Web (Forms, Business Apps, etc.)	Authentication (MFA)
IAM	Enterprise	Authentication (MFA)
IAM	Device Certification	Authentication (MFA)
IAM	Remote Access Authentication	Authentication (MFA)
IAM	Mobile Device Management	Authentication (MFA)

Domain	Control	Category
IAM	Network Authentication (802.1x, PAP, CHAP, etc.)	Authentication (MFA)
IAM	Challenge Response	Authentication (MFA)
IAM	Push Notification Authentication	Authentication (MFA)
IAM	Privileged User Management	IAM
IAM	Logging and Monitoring	IAM
IAM	Authorization	IAM
IAM	DMARC Email Authentication	IAM
IAM	Domain Keys Identified Mail (DKIM)	IAM
IAM	Sender Policy Framework (SPF)	IAM
Virtualization	Access Control	Virtualization
Virtualization	Segmentation Control	Virtualization
Virtualization	Containerization	Virtualization
Virtualization	Resource Utilization Management	Virtualization
Virtualization	Shared Storage	Virtualization
Virtualization	Virtual Networking Security	Virtualization
Virtualization	Logging and Monitoring	Virtualization
Management	SIEM	Security Operations Tooling
Management	Log Investigation and Management	Security Operations Tooling
Management	Security Operations Center Tooling	Security Operations Tooling
Management	Response and Investigation Case Tooling	Security Operations Tooling
Management	Dashboard and Compliance Reporting	Security Operations Tooling
Management	Cyber Threat Intelligence Management Platform	Security Operations Tooling
Management	Penetration Testing Toolset	Vulnerability Management
Management	Vulnerability Scanning Toolset	Vulnerability Management
Management	Patching	System Management
Management	Configuration Management	System Management
Management	Security Incident Management	Security Management
Management	Forensics - Host	Forensics
Management	Forensics - Memory	Forensics
Management	Forensics - Cloud	Forensics
Management	Malware Reverse Engineering	Forensics
Management	Disaster Recovery Testing	Business Continuity
Management	Disaster Recovery Tooling	Business Continuity
Management	Business Continuity Management Tooling	Business Continuity
Management	Service Continuity Management Tooling	Business Continuity
Cloud	Conditional Access	Cloud Security
Cloud	Cloud Access Governance	Cloud Security
Cloud	Information Protection	Cloud Security
Cloud	VPN Gateway	Cloud Security
Cloud	Key Vault	Cloud Security
Cloud	API Gateway	Cloud Security
Cloud	DDoS Protection	Cloud Security
Cloud	Directory Services	Cloud Security
Cloud	Application Gateway	Cloud Security
Cloud	Cloud Firewall Appliances	Cloud Security
Cloud	Adaptive Application Controls	Cloud Security
Cloud	Threat Detection	Cloud Security
Cloud	Disk Encryption	Cloud Security

Domain	Control	Category
Cloud	Just In Time Access	Cloud Security
Cloud	Network Threat Detection	Cloud Security
Cloud	Cloud Hardening	Cloud Security
Cloud	Build Configuration and Control	Cloud Security
Cloud	Logging and Monitoring	Cloud Security
Cloud	Authentication	Cloud Security Access Broker
Cloud	Data Tokenization	Cloud Security Access Broker
Cloud	Encryption	Cloud Security Access Broker
Cloud	Data Loss Prevention	Cloud Security Access Broker
Cloud	Logging	Cloud Security Access Broker
Cloud	Single Sign On	Cloud Security Access Broker
Cloud	Access Control	Cloud Security Access Broker
Cloud	Enforcement	Cloud Security Access Broker
Testing	Web Vulnerability Scanning	Web Application Assessment
Testing	Web Application Testing Tools	Web Application Assessment
Testing	Web Application Testing – Static Analysis	Web Application Assessment
Testing	Web Application Testing – Dynamic Analysis	Web Application Assessment
Testing	Assessment/Testing	Managed Services
Testing	Managed Web Application Firewall	Managed Services
Application	Application - Business Activity Logging	Auditing
Application	Application - Operational Support Activity Logging	Auditing
Application	Application Component Activity Logging	Auditing
Application	ACLs - File System	Access Control - Authorization
Application	ACLs - Database	Access Control - Authorization
Application	Role Based Access Model	Access Control - Authorization
Application	ACLs - Bespoke	Access Control - Authorization
Application	ACLs - Host Based	Access Control - Authorization
Application	Application Logic controlled access control	Access Control - Authorization
Application	Least privilege controls	Access Control - Authorization
Application	Incompatible Role Definition Detection	Access Control - Authorization
Application	Toxic Combination Detection	Access Control - Authorization
Application	Separation of Duties	Access Control - Authorization
Application	Web (Forms, BA, etc.)	User and Application Authentication
Application	Browser based Federation (SAML, ADFS)	User and Application Authentication
Application	Application Federation (Web Services)	User and Application Authentication
Application	Bespoke Authentication	User and Application Authentication
Application	Directory (LDAP)	User and Application Authentication
Application	Unsuccessful Login Controls	User and Application Authentication
Application	Previous Logon Notification	User and Application Authentication
Application	Denial of Service Protection	User and Application Authentication
Application	Single Sign On	User and Application Authentication
Application	Application Encryption	Application-level Encryption
Application	Channel Encryption (TLS, etc.)	Application-level Encryption
Application	Credential Encryption	Application-level Encryption
Application	Session Termination	Session Management
Application	Session Lock	Session Management
Application	Session Auditing	Session Management
Application	Concurrent Session Control	Session Management

Domain	Control	Category
Application	Session Authenticity	Session Management
Application	Tamper Resistance and Detection	Integrity Controls
Application	Memory Protection	Integrity Controls
Application	Input Validation (bounds checking etc.)	Integrity Controls
Application	Input Sanitization (application layer)	Integrity Controls
Application	External Library/Dependency Inventory (SBOM)	Integrity Controls
Application	Code Control	Integrity Controls
Application	Data at Rest integrity controls	Integrity Controls
Application	Application Code Partitioning	Compartmentalizing
Application	Application Partitioning	Compartmentalizing
Application	Security Function Separation	Compartmentalizing
Audit	Assurance of Financial Management & Reporting	Audit
Audit	Assurance in Quality of Management Information	Audit
Audit	Assurance in IT project acquisitions	Audit
Audit	Assurance in IT project implementation	Audit
Audit	Assurance in Information Technology Capabilities	Audit
Audit	Assurance of Key Business Process	Audit
Audit	External Compliance Requirements	Audit
Audit	Internal Compliance	Audit
Audit	Internal Controls	Audit
Audit	Performance Targets	Audit
Audit	Conformance Targets	Audit
Operational	Cloud Monitoring	Operational Security
Operational	Data Loss Prevention	Operational Security
Operational	Build Compliance	Operational Security
Operational	Vulnerability Scanning	Operational Security
Operational	Incident Management	Operational Security
Operational	Protective Management	Operational Security
Operational	Privileged User Management	Operational Security
Operational	Patch Management	Operational Security
Operational	Remote Access Management	Operational Security
Operational	Anti-Malware Management	Operational Security
Operational	Business Continuity Management	Operational Security
Operational	Key Management	Operational Security
Operational	Cloud Security Integrity	Operational Security
Operational	Internal Certificate Management	Certificate Management
Operational	External Certificate Management	Certificate Management
Operational	Security Advisories and Notifications	Intelligence
Operational	Brand Management	Intelligence
Operational	Regulatory Advisories	Intelligence
Operational	Vendor Advisories	Intelligence
Operational	CERT Advisories	Intelligence
Operational	Internal Vulnerability Scanning	Security Testing
Operational	External Vulnerability Scanning	Security Testing
Operational	Infrastructure Penetration Test - Annual	Security Testing
Operational	Infrastructure Penetration Test - Ad-hoc	Security Testing
Operational	Application Penetration Test - Annual	Security Testing
Operational	Application Penetration Test - Ad-hoc	Security Testing

Domain	Control	Category
Operational	Red Team/Adversary Testing	Security Testing
Operational	Blue Team Testing	Security Testing
Operational	Purple Team Testing	Security Testing
Operational	Security Monitoring	Security Operations Center
Operational	Security Incident Management	Security Operations Center
Operational	Continuous Improvement	Security Operations Center
Operational	Threat Hunting	Security Operations Center
Operational	Misuse and Abuse Case Development	Security Operations Center
Operational	Security Test Management	Security Operations Center
GRC	ISO/IEC 27001	Governance and Compliance
GRC	COBIT 2019	Governance
GRC	ITIL Framework for IT Governance	Governance
GRC	VAL IT	Governance
GRC	AS8015-2015 IT Governance Framework	Governance
GRC	COSO	Governance
GRC	ISO/IEC 38500	Governance
GRC	NIST Cybersecurity Framework	Compliance
GRC	PCI DSS v4.0	Compliance
GRC	HIPAA	Compliance
GRC	FISMA	Compliance
GRC	CJIS (Criminal Justice Information Services)	Compliance
GRC	GDPR (General Data Protection Regulation)	Compliance
GRC	CIS Top 18 Critical Security Controls	Compliance
GRC	ISO/IEC 20000	Compliance
GRC	FedRAMP	Compliance
GRC	CMMC	Compliance
GRC	ISO 22301	Compliance
GRC	SOC 2 (Service Organization Control 2)	Compliance
GRC	IT General Controls	Compliance
GRC	Internal Policy	Compliance
GRC	Internal Standards	Compliance
GRC	Internal Guidelines	Compliance
GRC	Internal Patterns Management	Compliance
GRC	Education and Awareness	Compliance
GRC	Security Risk Management	Risk Management
GRC	Privacy Risk Management	Risk Management
GRC	Validation and Maturity	Risk Management
GRC	Secure by Design	Risk Management
GRC	Third Party Risk Management	Risk Management
GRC	Operational Assurance	Risk Management
GRC	Operational Risk Management	Risk Management
GRC	FAIR Analysis	Risk Management
GRC	Holistic Approach to Risk Management (HARM)	Risk Management

Table 11 – Enterprise Security Controls Index

Appendix C: SPENCER: Maintaining Digital Trust Canvas

The goal and purpose of using the Digital Trust Canvas is to aid in modeling, promoting, and ensuring consentient and continuous digital trust with those to whom we provide and deliver services.

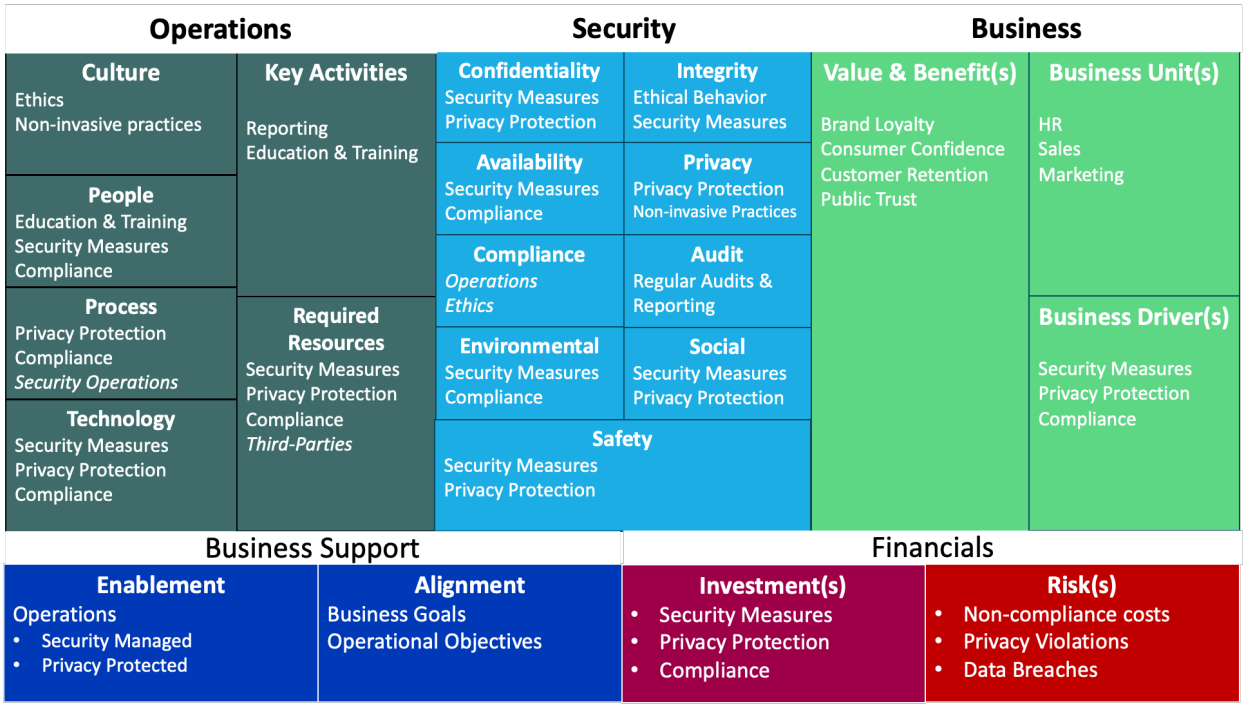


Figure 17 – Digital Trust Modeling Canvas

The primary goal of the Digital Trust Modeling process is to quickly identify, link, visualize and communicate, at a high-level, the various elements associated with a business, information technology, privacy, and information/cybersecurity initiatives within the enterprise.

The goal of using Digital Trust Modeling is not meant to replace Business Cases; rather it is intended to quickly aid in understanding needs and potential impacts of specific initiatives, in a logical and cohesive manner to further build business cases and promote definition of requirements for those initiatives.

For additional information on the Digital Trust Canvas, please feel free to visit and download your copy at the following URL:

www.therubiconadvisorygroup.com/2023/10/12/introducing-the-spencer-framework-a-framework-for-maintaining-digital-trust/

Appendix D: Secure Application Design Resources

Reference Materials	Website
CIS Benchmarks	www.cisecurity.org
CIS Top 18 Critical Security Controls	www.cisecurity.org
ISO 27001 - A.9.2 - User Access Management	www.iso.org/standard/27001
Microsoft Security Development Lifecycle (SDL)	www.microsoft.com/en-us/securityengineering/sdl
MITRE ATT&CK Framework	attack.mitre.org
NIST SP 800-154	csrc.nist.gov/pubs/sp/800/154/ipd
NIST SP 800-160	csrc.nist.gov/pubs/sp/800/160/v2/r1/final
NIST SP 800-175	csrc.nist.gov/pubs/sp/800/175/b/r1/final
NIST SP 800-53	csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
OWASP API Security Top 10	owasp.org/API-Security/editions/2023/en/0x00-toc
OWASP Application Logging Vocabulary Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Logging_Vocabulary_Cheat_Sheet.html
OWASP Application Security Verification Standard	owasp.org/www-project-application-security-verification-standard
OWASP Authentication Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
OWASP Cryptographic Storage Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html
OWASP Developer Guide	owasp.org/www-project-developer-guide/draft/
OWASP File Upload Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
OWASP Logging Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
OWASP Path Traversal Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Laravel_Cheat_Sheet.html#path-traversal
OWASP REST Security Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html
OWASP Secure Coding Practices Quick Reference Guide	owasp.org/www-project-secure-coding-practices-quick-reference-guide
OWASP Session Management Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
OWASP Threat Modeling Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html
OWASP Top 10	owasp.org/www-project-top-ten/
OWASP Transport Layer Protection Cheat Sheet	cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
Payment Card Industry Data Security Standards	www.pcisecuritystandards.org
SAFECode Guidelines	safecode.org
SEI CERT Coding Standards	wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

Appendix E: IT Asset Management Reference Model

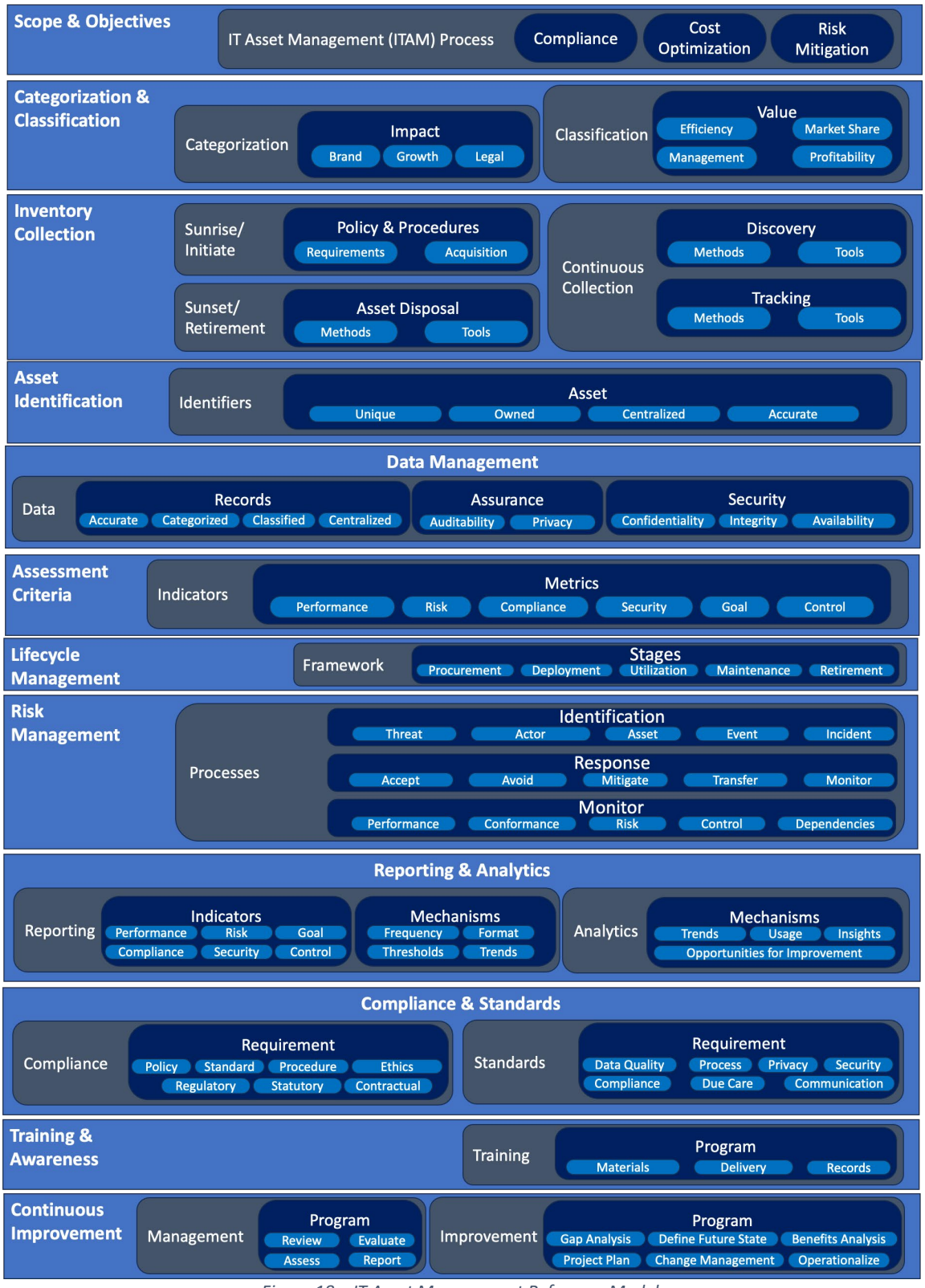
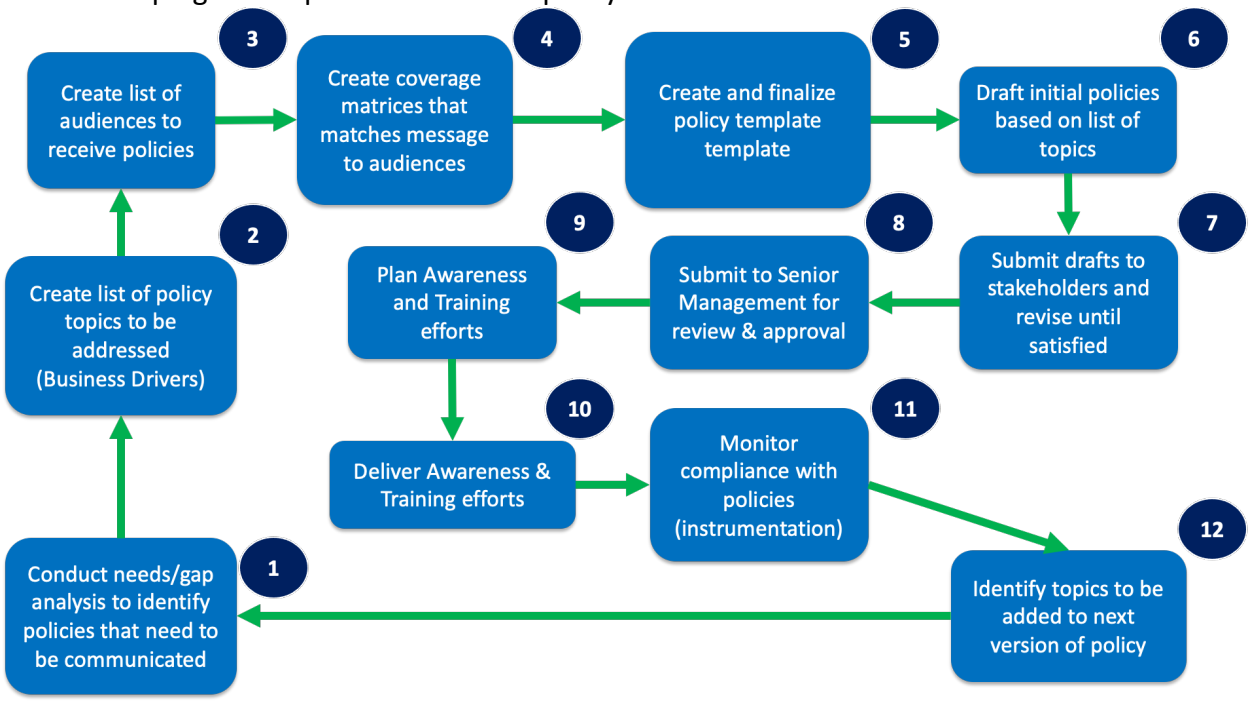


Figure 18 – IT Asset Management Reference Model

Appendix F: Sample Policy Lifecycle & Structure

Policy Lifecycle

The following illustrates a policy lifecycle process that walks through each key step associated with developing and implementation of a policy.



Step 1 – Review existing policies and determine the need or identify any gaps in policy coverage which need to be addressed.
Step 2 – Based on previous step, draft a list of policy topics mapped to their respective business drivers.
Step 3 – Identify a list of personnel that will need to review and approve the policy. This will consist of key stakeholders, appropriate subject matter experts and peer reviewers.
Step 4 – Develop an initial coverage matrix, allowing for the message to be tailored and conveyed in relevant terms that they'll understand.
Step 5 – Draft the policy using existing enterprise policy templates to ensure consistency.
Step 6 – Draft initial policy statements based on topics identified in step 2.
Step 7 – Submit draft policy to the appropriate stakeholders to allow for enhancements, changes, and support of the policy.
Step 8 – Submit draft policy to Senior Management for review, revisions, and approval needed for enforcement.
Step 9 – Develop reasonable and appropriate training materials on the new policy.
Step 10 – Delivery training to applicable audience members the policy applies to.
Step 11 – Monitor performance and conformance with the new policy.
Step 12 – Identify any enhancements to the policy for next version.

Example Policy Structure

[Organization Name]			*Policy Name*		
Policy ID #		Version:		Effective Date:	
Replaces:			Category:		

Policy ID: Uniquely identifies the policy for ease of reference and cross-reference.
Version: Provides the current iteration of the policy.
Effective Date: Date that the policy goes into effect.
Replaces: States which policy is being replaced
Category: Identifies the appropriate category the policy applies to (e.g., Encryption, Governance, Privacy, Mobile Device, Data Protection, etc.) within the organization.

Table of Contents

Purpose

The organization's business driver behind the policy.

Scope

What the policy applies to within the organization.

Policy

The specific statements establishing expected behavior of staff or the functional requirements of the organization which must be adhered to.

Violations

The consequences for deviation from the defined and established policy, in terms of the impact to both the organization and staff member.

Definitions

Clearly describe all unique terms and acronyms used in the policy document.

References

Identify applicable and related sources of information, either internal or external. This can include complimentary policies, standards, statutory, regulatory, or contractual requirements.

Related Documents

Identify relevant documentation that is supported by, in support of, or relies on the policy. This can include sample worksheets (e.g., IT Asset Inventory form, Data Classification Matrix, etc.)

Approval and Ownership

Identify the policy owner, who it was approved by and the date it was approved.

Revision History

Identify and keep current the version, description of changes, dates revision(s) were made, the change author, reviewer and approval accepting the changes.

Appendix G: Layer RACI Charts

Business Context Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Business Strategy Alignment	**A**	R	C	C	C	I	I	C	I	C,I	C,I	I	I
Business Risk Profile	R	**A**	I	C,I	C,I	I	C,I	C,I	I	C,I	C,I	I	I
Enterprise Security Policy	C	C	**A,R**	R,C	C,I	C,I	R,C	C	C	C	C	I	R,C
Business Requirements	C	C	R	**A**	C	C,I	C,I	I	C	R	C	C,I	I

Information Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Information Classification	**A**	C	R	C	C	C	C	R	C	C	I	C,I	I
Information Security Policies	R	C	**A,R**	C	C	C	C	C	C	C	C	I	I
Information Security Procedures	R	C	I	C	C	C	**A**	C	C	C	C	I	I
Data Lifecycle Management	I	R	R	**A**	I	R	R	I	C,I	R	R,C	I	I

Application Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Application Portfolio	I	C,I	I	I	I	I	**A**	C	C	C	C	I	C,I
Access Control Models	I	C	C	**A**	C	C	R	C	C	C	C	--	C,I
Secure Application Design	I	C	C	R	C	R	**A**	R	C	C	C	--	C,I

Technology Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Technology Inventory	I	C,I	I	R	C,I	C	**A**	C	C	R	C	--	C,I
Security Infrastructure Design	I	I	I	C,I	I	C,I	R	I	I	C,I	C,I	--	**A**
Network Security Architecture	I	I	I	C,I	C	C	**A**	C	I	C	C	--	R
Identity and Access Management	I	I	I	C,I	I	C,I	**A**	C,I	I	C	C	--	R

Physical Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Physical Security Controls	I	C	C	**A**	C	C	R	C	C	R	C	I	I
Data Center Security	I	C	C	**A**	C	C	R	C	C	R	C	I	I
Environmental Controls	I	C	C	**A**	C	C	R	C	C	R	C	C,I	I

Human Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Security Awareness and Training	C,I	I	**A**	I	I	R,I	C	--	--	R,C	I	R,C	R,I
Human Resource Security Procedures	I	I	**A,R**	I	I	I	C	--	--	R,I	I	R,C	C
Behavioral Profiling Mechanisms	C	I	**A**	I	I	I	R,C	--	--	R	I	R,C	R,C

Assurance Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Audit & Compliance Monitoring	**A**	I	I	R	I	R,C	R,C	I	--	R,C	R,C	--	R,C
Security Testing Methods	I	I	I	R	I	R	R	I	--	R,C	C,I	--	**A,R**
Incident Response Plans	**A**	C,I	I	R	I	R	R	I	I	R,C	C,I	C,I	R,C

Security Services Layer

Artifact	Executive Leadership	Finance	Human Resources	Product/System Owner	Sales	Project Management	Information Technology	Marketing	Administration	Operations Management	Business Development	Staffing/Recruitment	Architect
Security Policy Framework	**A**	C	I	R,C	I	R,C	R,C	I	--	R,C	I	I	R
Security Awareness Training	I	I	**A,R**	R,C	I	R,C	C,I	I	I	R	I	I	C,I
Access Control Matrix	I	I	R	**A**	I	R,C	R	I	I	R,C	--	--	R,C

Appendix H: Choosing a Framework

Considerations for Choosing the Right Framework

1. Industry Fit: Consider whether the framework is used and recognized by your industry.
2. IT Staff Size and Resources: Frameworks may require specialized expertise and resources, whereas some may be more adaptable and appropriate for smaller organizations; assess your IT staff.
3. Specific Needs: Identify needs and requirements that are specific and appropriate to your organization.
4. Organizational Maturity and Culture: Align the framework with your organization's maturity level and culture. Some frameworks may be more complex and require a higher level of maturity and capability.
5. Adaptability and Customization: Determine how adaptable the framework is to your organization's needs. Some frameworks offer high adaptability but may lack formal support.
6. Business Alignment: Consider how well the framework aligns with your business objectives and processes. The target framework needs to provide a strong alignment between security and business needs.

Framework	Pros	Cons
Foundational Enterprise Security Architecture	Quick start for business aligned security architecture efforts. Flexible, applicable to various industries.	Tailoring and business engagement will be required.
Open Enterprise Security Architecture	Open and adaptable, encourages collaboration.	Customization required.
Department of Defense Architecture Framework	Well-structured for defense and government.	Might be considered overkill for non-government organizations.
SANS Enterprise Cloud Security Architecture	Addresses cloud security needs.	Specific to cloud security.
The Open Security Architecture	Open-source, adaptable, versatile.	Resource and support availability.
Sherwood Applied Business Security Architecture	Business-aligned security, adaptable.	Complexity and may require specialized expertise.

Appendix I: Common pitfalls to be aware of

We feel the following are hazards you should be considerate of when attempting to adopt any enterprise security architecture.

1. **Lack of Alignment with Business Objectives**: Failing to align architecture with the broader strategic goals and objectives of the organization can lead to misalignment of priorities and ineffective security investments.
2. **Overemphasis on Technology**: Placing too much focus on technological solutions without considering broader organizational factors, such as culture, processes, and people, can result in ineffective security implementations.
3. **Ignoring Organizational Culture**: Neglecting to consider the existing culture and dynamics can lead to resistance to security initiatives and poor adoption by staff.
4. **Complexity and Over-Engineering**: Designing architectures that are difficult to understand, implement, and maintain can lead to inefficiencies and increased risk of introducing vulnerabilities into the environment.
5. **Lack of Stakeholder Engagement**: Failing to engage key stakeholders (e.g. senior leadership, business units, IT) throughout the architecture's development and implementation process can result in inadequate buy-in and support.
6. **Poor Communication**: Inadequate communication of security policies, procedures, and requirements for staff can lead to confusion, non-compliance, and increased business risks.
7. **Insufficient Training and Awareness**: Neglecting to provide comprehensive training and awareness programs for staff can result in security gaps due to lack of understanding and adherence to business requirements.
8. **Failure to Adapt to Change**: Architectures that are rigid and inflexible may fail to adapt to evolving threats, technologies, and business requirements, leading to vulnerabilities and gaps in protection.
9. **Lack of Metrics and Measurement**: Failing to establish clear metrics and Key Performance Indicators (KPIs) to measure the effectiveness of architectures can make it challenging to assess performance and identify areas for improvement.
10. **Underestimating Human Factors**: Overlooking the human element of security, including insider threats, social engineering attacks, and human error, can leave vulnerabilities unaddressed and compromise overall security posture.

Appendix J: Glossary of Terms & Acronyms

Access Control

Methods that regulate who can view or use resources within a computing environment, ensuring only authorized entities can access sensitive data.

Application Security

The process of defending applications against vulnerabilities and threats by integrating security measures into the software development lifecycle (SDLC).

Architecture

The structured framework used to manage the design, development, and security of IT systems and their alignment with organizational goals.

Artifact

Any documentation, model, or product created during the process of developing or securing IT systems, used to provide evidence of compliance or analysis.

Artificial Intelligence

The use of algorithms and machine learning to simulate human intelligence for tasks like decision-making, which may involve security threat analysis.

Audit Trail

A chronological record of security events and actions, enabling the traceability of access, changes, or system activities.

Authenticity

The assurance that data, communications, or users are genuine and have not been altered or falsified.

Availability

Ensuring that authorized users have reliable and timely access to information systems and data when needed, often through redundancy and fault tolerance.

Boundaries

The logical or physical limits of a system, network, or data set within which security controls are applied to protect resources from unauthorized access or exposure.

Business Continuity Plan (BCP)

A strategic plan ensuring that critical business functions remain operational during and after a security incident or disaster, minimizing downtime and loss of services.

Compliance

Adherence to legal, regulatory, and organizational security requirements that govern how sensitive data and systems must be managed, accessed, and protected.

Confidentiality

Ensuring that sensitive information is accessible only to authorized individuals.

Control

A safeguard or countermeasure implemented to reduce risk by protecting applications, business processes, people, systems, networks, or data from unauthorized access, modification, or damage.

Cybersecurity

The practice of protecting systems, networks, and data from threats, unauthorized access, and malicious attacks to ensure the confidentiality, integrity, and availability (CIA) of information.

Data Encryption

The process of converting data from a readable format (cleartext) into an unreadable format (ciphertext) to protect it from unauthorized access.

Defense in Depth

A multi-layered security strategy that uses a series of defenses (technical, physical, and procedural) to protect assets and reduce the risk of a single point of failure.

Digital Asset

Any valuable or sensitive electronic information (e.g., intellectual property, personally identifiable information, etc.).

Digital Forensics

The investigation and analysis of electronic devices and data to identify, preserve, and recover evidence of crime, security incidents, or policy violations.

Disaster Recovery (DR)

A subset of business continuity that focuses on the prioritized restoration of IT systems and data following a disruption or disaster, ensuring minimal downtime and data loss.

Enterprise Business Architecture

The structure that aligns an organization's business strategy, processes, and resources to meet its goals and optimize efficiency across all business units.

Enterprise Information Technology Architecture

The overarching framework for managing and integrating IT resources and infrastructure across the organization to support an organization's goals, objectives and processes.

Enterprise Security Architecture (ESA)

A structured approach to managing and securing an organization's processes, systems, and business controls ensuring that security measures align with business objectives and protect critical assets.

Event

Any observable occurrence within a system or network, typically logged for monitoring and analysis.

Framework

A structured set of policies, standards, and guidelines that provide a foundation for managing security risks and achieving objectives within an organization.

Governance

The system of policies, processes, procedures, standards, guidelines, and controls that guide how an organization manages its security, ensuring alignment with regulatory requirements and the organization's goals and objectives.

Identity and Access Management (IAM)

Policies and technologies that ensure only authorized users can access certain resources, maintaining secure authentication and authorization processes.

Incident

A security event that compromises the integrity, confidentiality, or availability of an information system, requiring an immediate response to mitigate harm.

Incident Response

A structured approach to handling and managing security breaches or attacks, aimed at minimizing the damage and restoring normal operations as quickly as possible.

Integrity

The assurance that data is accurate, complete, and has not been altered or tampered with, ensuring its reliability and trustworthiness throughout its lifecycle.

Key Management

The process of administering cryptographic keys in a secure manner, including their generation, storage, distribution, revocation, and destruction, to ensure data protection.

Least Privilege

A security principle that ensures users, applications, or systems have only those access rights necessary to perform their functions, reducing the risk of misuse.

Multi-Factor Authentication (MFA)

A security mechanism that requires users to provide two or more verification factors to gain access to a resource, enhancing the protection against unauthorized access.

Network Segmentation

The practice of dividing a network into smaller, isolated segments to reduce the attack surface and contain potential security breaches to limited areas.

Penetration Testing (Pen Testing)

A simulated attack conducted to identify vulnerabilities and weaknesses in systems, networks, or applications before they can be exploited by malicious actors.

Perimeter

The boundary that separates an internal, trusted network from external, untrusted networks, traditionally guarded by security measures like firewalls.

Privacy

The protection of sensitive personal or organizational information from unauthorized access or exposure, ensuring compliance with legal and regulatory frameworks.

Procedure

A detailed set of instructions and steps to be followed to achieve specific tasks,

Regulatory

The standards which govern how an organization manages and protects data and systems, ensuring legal and ethical practices.

Risk Management

The process of identifying, assessing, and mitigating potential threats to an organization's security, ensuring business continuity and data protection.

Sanitizing

The process of securely removing data from a system, device, or storage medium to ensure that it cannot be recovered or accessed by unauthorized individuals.

Security Awareness Training

A management program designed to educate employees and stakeholders about risks, best practices, and the importance of protecting sensitive information within the organization.

Security by Design

The practice of integrating security considerations into every stage of system development, ensuring that security is a foundational aspect rather than an afterthought.

Security Controls

Measures, policies, or mechanisms implemented to safeguard information systems, reduce vulnerabilities, and mitigate the risk of security breaches or attacks.

Security Frameworks

Structured guidelines or best practices that provide a comprehensive approach to managing and securing an organization’s information systems and infrastructure.

Security Information and Event Management (SIEM)

A technology that provides real-time analysis of security alerts generated by applications and network hardware to detect and respond to potential threats.

Security Operations Center (SOC)

A centralized team responsible for monitoring, detecting, and responding to security incidents in real-time, providing continuous protection and risk mitigation.

Security Policy

A formal document outlining an organization's security objectives, principles, and processes to guide how security controls and practices are implemented.

Stakeholder

Any individual or group with an interest in the security of an organization's systems and data, including employees, customers, partners, and regulatory bodies.

Statutory

Pertaining to laws and regulations that organizations must comply with regarding security, privacy, and data protection, often legally enforced.

Supply Chain Risk Management

The process of identifying, assessing, and mitigating risks to an organization's supply chain, ensuring that suppliers adhere to contractually defined security standards and reduce risk to the organization.

System Hardening

The process of securing an application or system by reducing its surface of vulnerability, often by disabling unnecessary services, configuring security settings, and applying patches.

Third-Party Risk Management

The process of identifying, assessing, and mitigating risks to an organization's supply chain, ensuring that vendors meet contractually defined security standards and don’t introduce any unnecessary risks.

Threat Intelligence

Information which is collected, analyzed, and used to understand potential threats against an organization’s assets, providing insights for proactive defense and mitigation.

Tokenization

A technique that replaces sensitive data (e.g., credit card numbers, social security numbers, etc.) with non-sensitive tokens, reducing the risk of exposure during data processing.

Vulnerability Management

The process of identifying, assessing, remediating, and mitigating vulnerabilities across systems, applications, and networks to reduce risk.

Whistleblower

An individual who reports unethical, illegal, or security-related violations within an organization, often protected by laws to prevent retaliation.

Zero Trust Architecture (ZTA)

An approach to security that assumes no implicit trust within an organization's network and requires continuous verification for access to all resources.

Acronyms

ACL - Access Control Lists

API - Application Programming Interface

ATT&CK - Adversarial Tactics, Techniques, and Common Knowledge

CI/CD - Continuous Integration/Continuous Delivery

CMDB - Configuration Management Database

CSF - Cybersecurity Framework

DAC - Discretionary Access Control

EDR - Endpoint Detection and Response

ELT – Executive Leadership Team

FESA – Foundational Enterprise Security Architecture

FIPS - Federal Information Processing Standards

HIPAA - Health Insurance Portability and Accountability Act

IAM - Identity and Access Management

IR - Incident Response

ISO - International Organization for Standardization

ISACA – Information Systems Audit and Control Association

ISSA – Information Systems Security Association

KPIs - Key Performance Indicators

KRIs - Key Risk Indicators

MAC - Mandatory Access Control

MDM - Mobile Device Management

MFA - Multi-Factor Authentication

NDA - Non-Disclosure Agreement

NIST - National Institute of Standards and Technology

OWASP - Open Web Application Security Project

PCI - Payment Card Industry

PCI DSS - Payment Card Industry Data Security Standard

RBAC - Role-Based Access Control

REST - Representational State Transfer

RMF - Risk Management Framework

ROC – Report on Compliance

SAF - Security Architecture Framework

SANS - System Administration, Networking, and Security Institute

SLAs - Service Level Agreements

SOC2 - Service Organization Control 2

SOX - Sarbanes-Oxley Act

UID - Unique Identifier

VPNs - Virtual Private Networks