What Is Enterprise Information Security Architecture?

Mike Tierney

Published: January 18, 2022

Spending on security and risk management is soaring worldwide. But exactly which improvements should you focus on next to best strengthen your cybersecurity program?

For many organizations, building a solid information security architecture should be at the top of the list. Read on to learn how what information security architecture is and how it can help you protect your critical IT assets from security threats with less work and worry.

> **Handpicked related content:**
>
> - [Free Guide] Information Security Risk Assessment Checklist

What is enterprise information security architecture?

A simple way to define enterprise information security architecture (EISA) is to say it is the subset of enterprise architecture (EA) focused on securing company data.

A more comprehensive definition is that EISA describes an organization's core security principles and procedures for securing data — including not just and other systems, but also personnel teams and their roles and functions. This information is provided in the context of organizational requirements, priorities, risk tolerance and related factors, to help ensure the EISA reflects both current and future business needs.

Key elements

Here are the key elements of an EISA and the purpose of each:

- **Business context**— Defines enterprise information use cases and their importance for reaching business goals.
- **Conceptual layer**— Provides the big picture, including the enterprise profile and risk attributes.
- **Logical layer**— Defines the logical paths between information, services, processes and application
- **Implementation**— Defines how the EISA should be implemented.
- **Solutions**— Details the software, devices, processes and other components used to mitigate security vulnerabilities and maintain security for the future.

Benefits of an EISA

Having a solid EISA is invaluable for guiding security planning at all levels. It provides the detailed information required to make the best decisions about what processes and solutions to implement across the IT environment and how to manage the technology lifecycle.

Moreover, a carefully documented and published enterprise information security architecture is vital for compliance with many modern industry standards and legal mandates.

Challenges in creating an EISA

Development of an optimal EISA strategy can be difficult, especially when the following common factors are in play:

- Lack of communication and coordination among various departments or teams when it comes to managing risks and maintaining IT security
- Failure to clearly articulate the goals of the EISA
- Lack of understanding among users and stakeholders about the need to prioritize information security
- Difficulty calculating the cost and ROI of data protection software tools
- Lack of funding to properly address security issues
- Dissatisfaction with earlier security measures that were developed, such as spam filtering that flags valid and critical correspondence
- Earlier failures to meet regulatory requirements or business objectives,
- Concerns about the ineffectiveness of earlier IT security investments

Key tasks in building an EISA

Building an enterprise information security architecture includes the following tasks:

- Identify and mitigate gaps and vulnerabilities in the current security architecture.
- Analyze current and emerging security threats and how to mitigate them.
- Perform regular security risk assessment. Risks to consider include cyberattacks, malware, leaks of personal data of customers or employees, and hardware and software failure events.
- Identify security-specific technologies (such as privileged access management), as well as the security capabilities of non-security solutions (such as email servers), that can be used in the EISA.
- Ensure the EISA is aligned with business strategy.
- Ensure the EISA helps you satisfy the requirements of applicable compliance standards, such as SOX, PCI DSS, HIPAA/HITECH and GDPR.

The 5 steps to EISA success

The following 5 steps will help you develop an effective EISA:

1. Assess your current security situation.

Identify the security processes and standards your organization is currently operating with. Then analyze where security provisions are lacking for different systems and how they can be improved.

2. Analyze security insights (strategic and technical).

Link the insight gained in step 1 with your business goals. Be sure to include both technical measures and strategy context to prioritize your efforts.

3. Develop the logical security layer of the architecture.

To create a logical architecture for your EISA based on security best practices, use an established framework to assign controls where priority is high.

4. Design the EISA implementation.

Turn the logical layer into an implementable design. Based on your expertise, resources and the state of the market, decide which elements to develop in-house and which things should be managed by a vendor.

5. Treat architecture as an ongoing process.

Since the threat landscape, your IT environment, the solution marketplace and best practice recommendations are all constantly evolving, be sure to review and revise your information security architecture periodically.

Choosing modern EISA frameworks

There's no need to start from scratch when building your EISA. Instead, rely on one of the several frameworks developed in the last decade to create an effective EISA. Tailor it as needed to ensure it works for your unique organization.

Here are the EISA main frameworks to choose from:

The Open Group Architecture Framework (TOGAF)

TOGAF provides a set of tools for creating an enterprise security architecture from scratch for the first time. It helps you define clear objectives and bridge the gap between the different layers of your EISA. Moreover, the framework is adaptable to support you as your organization's security needs change.

Sherwood Applied Business Security Architecture (SABSA)

SABSA is a methodology for EA and EISA. It is often used with other processes like COBIT 5.

COBIT 5

COBIT 5, developed by ISACA, is a detailed framework that helps organizations of all sizes manage and secure the IT infrastructure. It covers business logic, risks and process requirements.

Department of Defense Architecture Framework (DoDAF)

The DoDAF is not just for government agencies. Because it links operations with information security, it's ideal for helping multi-company organizations with independent IT networks address interoperability issues. It centers around infrastructure visualization for different stakeholders in the enterprise.

Federal Enterprise Architecture Framework (FEAF)

The FEAF is the reference enterprise architecture for the US Federal Government. It was developed to help federal agencies recognize priority areas and build common business practices despite their unique needs, goals, operations and activities. It can help both government agencies and private organizations with EISA as well as EA.

Zachman Framework

The Zachman Framework is a high-level framework often used for creating EA, but it can also be translated into a top-down EISA approach. Based on the six fundamental questions — what, how, when, who, where and why — it has six layers: Identification, Definition, Representation, Specification, Configuration and Instantiation.

Frequently asked questions

What is enterprise cybersecurity?

Enterprise cybersecurity refers to the architecture, protocols and tools used to protect enterprise assets, both internal and on the internet, from cyberattacks within and outside the enterprise.

Enterprise cybersecurity differs from general cybersecurity in that modern enterprises have a complex infrastructure that requires a strong security policy, constant assessments, and effective management to avoid security incidents.

What is the security architecture of an information system?

The security architecture of an information system defines the framework, protocols, models and methods required to protect the data the system collects, stores and processes.

Is security architecture a part of enterprise architecture?

Yes. Security architecture is a pillar of enterprise architecture, as it evaluates and improves security and privacy. Without proper security efforts, the whole enterprise infrastructure — and consequently the entire business — is at risk.

Mike Tierney

Former VP of Customer Success at Netwrix. He has a diverse background built over 20 years in the software industry, having held CEO, COO, and VP Product Management titles at multiple companies focused on security, compliance, and increasing the productivity of IT teams.

Data security | Information security | Risk assessment

Show Comments

MORE GREAT READING

Information Security Policy: Must-Have Elements and Tips

Elena Vodopyan February 25, 2021

Improving Security through Vulnerability Management

Yelena Geras May 29, 2020

How to Reduce Cybersecurity Complexity and Successfully Manage Risks

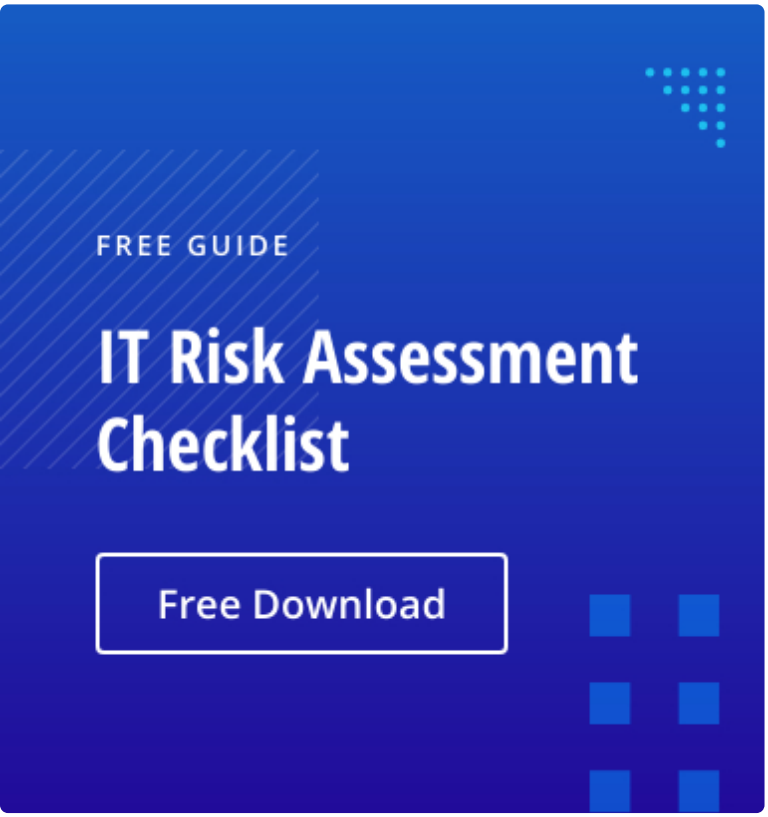
Matt Middleton-Leal December 5, 2019

What is the Principle of Least Access?

Brian Svidergol April 30, 2019

FEATURED TAGS

Active Directory | CISSP | Cyber attack | Data classification | Data governance | Data security | GDPR | Insider threat | IT compliance | IT security | Office 365 | Privileged account management | Risk assessment | SharePoint | Windows Server | ...



FEATURED TAGS

Active Directory | CISSP | Cyber attack | Data classification | Data governance | Data security | GDPR | Insider threat | IT compliance | IT security | Office 365 | Privileged account management | Risk assessment | SharePoint | Windows Server | ...

Webinars
Attack Catalog
How-to Guides
eBooks & Guides
SysAdmin Magazine
Cyber Chief Magazine
Research
Solutions
Active Directory Security
Data Access Governance
Data Governance
Ransomware Protection
Privileged Access Management
Compliance solutions
NIST CSF
CMMC
PCI DSS
HIPAA
ISO
GDPR

Privacy Policy | EU Privacy Policy | EULA | Modern Slavery Statement

Corporate Headquarters: 6160 Warren Parkway, Suite 100, Frisco, TX, US 75034

Phone: 1-949-407-5125 | **Toll-free:** 888-638-9749