ISAUnited
International Security Architects

Know Your Architecture-RP-216

Recommended Principle

Version 1-02.2024

www.isaunited.org

Forward

This guiding principle outlines the integration of 'Know Your Architecture' into your security architecture design. It refrains from prescribing detailed practices or instructions for every specific situation due to the intricate nature of industry and organizational technical architecture designs, encompassing infrastructure, complex networks, and associated components and systems.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.

This guide should be used in conjunction with the practices described in the following ISAUnited standards and publications, when appropriate (use the latest revisions):

1. Security Design Operations Model
2. Defensible Architecture Design Methodology

Contents

Description 4
Scope 5
Terms, Definitions, and Abbreviations 5
Security Culture 6
Process 7
Foundational Considerations for Security Practitioners: 7
Networking Fundamentals and Security Architecture: 7
Informed Decision-Making: 7
Responsibilities 8
Competence, Awareness, and Training 8
Summary 9
References 9

Know Your Architecture-RP-216

Recommended Principle

Version 1-02.2024

Description

Security architecture is a multifaceted discipline that demands a holistic approach to safeguarding an organization's assets. In security design decisions, having an intricate understanding of the organization's infrastructure and network is not merely advantageous; it is fundamental to success. This recommended principle clarifies the critical reasons why security architects shall possess an in-depth knowledge of these foundational elements. Technical architecture with a focus on infrastructure, networks, components, and systems provides a structured approach to designing and organizing the technological elements within an organization, ensuring coherence, efficiency, and optimal performance of the overall IT environment.

Scope

Technical architecture encompasses infrastructure, networks, and associated components and systems. This recommended principle (RP) establishes the base requirements of architecture security for organizations that design, operate, implement, and support architecture for use in on-premises, cloud, and or hybrid. This RP provides security practitioners with an enhanced framework to reveal and manage risk, promote a learning environment, and continually improve architecture security and integrity by using this principle. At the foundation of this RP is the practitioners' existing architecture security posture. The requirements of this RP are comprehensive and define the elements needed to identify and address security for a practitioner's lifecycle. The elements herein comprise what should be done, not how to do it. The document does not explicitly address individual personnel duties and departmental duties, but the elements herein can be applied to those aspects of an employee or operation.

Terms, Definitions, and Abbreviations

Architecture - Technical architecture refers to the structured framework that defines the design, organization, and integration of various technological elements within an IT system or enterprise. It encompasses hardware, software, networks, databases, and other components to create a cohesive and efficient structure that supports the organization's information technology strategy. Technical architecture provides a blueprint for the implementation, maintenance, and evolution of IT systems, ensuring alignment with business goals and optimal functionality.

Infrastructure - encompasses the foundational components, facilities, and systems necessary for the operation and functionality of an organization's information technology environment. This includes hardware, such as servers, data centers, networking equipment, and storage devices, as well as the associated software, middleware, and other supporting elements. Technical infrastructure provides the underlying framework for the deployment, management, and delivery of IT services, ensuring the reliability, scalability, and performance of an organization's technological capabilities.

Network - A network refers to the interconnected system of devices, communication pathways, and protocols that facilitate the exchange of data and information within a computer or telecommunications environment. It encompasses the hardware components like routers, switches, and cables, as well as the software protocols and configurations that enable seamless communication between computers and other devices. Technical networks are designed to support various functionalities such as data transmission, resource sharing, and access to services, forming the backbone of modern information technology infrastructures.

Components - any part of a system that, by itself, provides all or a portion of the total functionality required of a system. A component is recursively defined to be an individual unit, not useful to further subdivide, or a collection of components up to and including the entire system. A component may be software, hardware, etc.

Systems - a system is made up of one or more components, which may be linked (interact through the same processor) and or tightly coupled.

Security Culture

A favorable security culture is crucial for the security performance of the organization, regardless of its size or complexity. Security culture encompasses the shared attitudes, values, norms, and beliefs among employees and contractor personnel in the security department concerning risk and safety. In a positive security culture, collaboration among staff members is fostered, positive attitudes toward compliance are encouraged, a sense of responsibility for public safety and each other's well-being is instilled, and there is a fundamental belief in non-punitive reporting.

Given the numerous and intricate security activities within the organization, it is imperative to systematically manage security using an agreed framework and cultivate a positive security culture. While a positive security culture can exist independently, an effective SMS cannot thrive without it. Hence, security practitioners should actively strive to enhance and evaluate their security culture.

Sustaining a positive security culture demands ongoing diligence across the security department to address issues such as complacency, fear of reprisal, overconfidence, and normalization of deviance. Indicators of a positive security culture within the organization are provided below.
The organization:

- embraces security (personnel, public, and asset) as a core value,
- ensures everyone understands the organization's security mission, vision, and goals,
- fosters systematic consideration of risk, including what can go wrong,
- inspires, enables, and nurtures change, when necessary,
- allocates adequate resources to ensure individuals can accomplish their [____] recommending principal responsibilities,
- encourages employee engagement and ownership,
- fosters mutual trust at all levels, with open and honest communication,
- promotes a questioning and learning environment,
- reinforces positive behaviors and why they are important,
- encourages two-way conversations about learnings and commits to applying them throughout the organization, and
- encourages non-punitive reporting and ensures timely response to reported issues.

Adopting and implementing this recommended principle will strengthen the security culture of an organization. Practitioners, managers, and employees acting to make safety performance and risk reduction decisions over time will improve architecture security as a value, thereby strengthening the security culture of an organization. With this RP, practitioners are provided an enhanced framework to manage and reduce risk and enable continual improvement in architecture security posture. The individual elements, when executed as deliberate, routine, and intentional processes result in improved communication and coordination, which yield a cohesive system and a stronger security culture.

Principle Elements

Foundational Considerations for Security Practitioners:

Comprehensive Inventory: To make informed design decisions, security architects shall maintain a comprehensive inventory of the organization's infrastructure components. This includes servers, databases, storage systems, and any other elements crucial to the functioning of the business. Without this foundational knowledge, architects risk overlooking potential vulnerabilities and may fail to align security measures with the intricacies of the infrastructure.

Interaction Dynamics: Understanding how different components of the infrastructure interact is paramount. The intricate interplay between servers, databases, and network systems significantly influences the overall security posture. Nuanced comprehension allows architects to design security measures that seamlessly integrate with the organization's operational structure, mitigating risks more effectively.

Networking Fundamentals and Security Architecture:

Mapping Network Topologies: The network is the circulatory system of modern organizations. Security architects shall possess a deep understanding of network topologies, including the configuration of routers, switches, firewalls, and other networking devices. This knowledge is indispensable for crafting security designs that account for the nuances of the organization's communication pathways.

Identifying Vulnerabilities: Network vulnerabilities often serve as entry points for malicious actors. Security architects armed with knowledge about network architecture can identify potential weak links and design security measures to fortify these points. This proactive stance is critical for preemptive risk mitigation.

Informed Decision-Making:

Aligning Security Measures: By intimately understanding the infrastructure and network, security architects can align security measures with the specific needs and nuances of the organization. This alignment ensures that security is not an afterthought but an integral part of the organizational fabric, leading to more effective risk management.

Adaptability to Changes: Organizations undergo continuous changes in their infrastructure and network configurations. Security architects, equipped with ongoing knowledge, can adapt their security designs to accommodate these changes seamlessly. This adaptability is essential for maintaining an agile and resilient security architecture.

Responsibilities

Practitioner - The security practitioner shall establish and maintain the recommended principle and build a shared understanding of security culture. The security practitioner shall articulate expectations, including publishing a commitment to security, security responsibilities of personnel at all levels, policies, goals, and objectives. The security practitioner shall improve upon the recommended principle and measure its effectiveness and maturity in accordance with the requirements of this guidance document.

Management - Management shall actively promote, collaborate, communicate, sponsor, and provide support for this recommended principle.

General User – General user or employee shall utilize and integrate this recommended principle into their operations and practices.

RACI - Responsibilities, accountabilities, and authorities in developing, implementing, and continuously improving the security shall be defined, documented, and communicated throughout the architecture practitioner's organization. Accountability for resource allocation shall be assigned to (an) management with appropriate authority.

Competence, Awareness, and Training

The security practitioner shall ensure that personnel whose responsibilities fall within the scope of the RP have an appropriate level of competence in terms of education, training, knowledge, and experience. Where external resources, including contractors, are used to support the RP recommended principle, the security practitioner shall ensure that operating personnel have the requisite competence, skills, and experience.

The security practitioner shall define the need for and provide training to enable the development and implementation of the RP elements. Training shall include refresher training and raising awareness of where executing the safety assurance and continuous improvement sub-elements reveal opportunities to improve processes and procedures. Records of training shall be maintained.

The security practitioner shall establish a training schedule to ensure that personnel and contractors who have accountabilities, responsibilities, and authorities in executing the requirements of the Rp are updated and aware of:

1.applicable elements of the RP recommended principle that affect their job requirements;
2. newly emerging or changing risks, problems in the execution of the RP, and opportunities to improve processes and procedures; and
3. potential consequences of failure to follow processes or procedures.

Summary

Implementing the 'Know Your Architecture' recommended principle strengthens an organization's security culture and posture. The synergy between security architecture and the organization's infrastructure and network is indispensable. The understanding of these foundational elements allow security architects to make better design decisions that are not only robust but also tailored to the unique challenges and dynamics of the organization. The execution of the elements depends on the actions of every individual and organizational unit at all levels of the organization. Each of the RP elements can be expected to contribute to different aspects of the security culture, and these combined aspects reflect the strength of the culture. The RP, with all its discrete elements, supports the culture, and the culture feeds back into the management system in a continuous process, yielding an increasingly mature organization.

References

1. https://csrc.nist.gov/glossary/term/security_architecture
2. https://csrc.nist.gov/glossary/term/architecture
3. https://www.iso.org/standard/51581.html

Revision	Date
Created Date	01-15-2024
Institute Date	01-22-2024
Published Date	01-22-2024

End of document.