Well-Secured Architected

A Model for Safeguarding Architecture

ISAUnited
International Security Architects

ISAUnited

The CORE4 Model

Well-Secured-Architected

A Model for Safeguarding Architecture

ISAU-FAM-108-v1.2024-CORE4

www.isaunited.org
info@ISAUnited.org
Houston, TX

About ISAUnited.org

As a growing professional organization, ISAUnited.org® is striving to be a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISAUnited equips security professionals with the knowledge, credentials, education, and community to advance their careers and transform their organizations. ISAUnited leverages the expertise of its community engaged professionals in information and cyber security, governance, assurance, risk, and innovation. ISAUnited promotes its global presence with its headquarters in the United States.

Disclaimer

ISAUnited has designed and created the ISAUnited Well-Secured-Architected® 2024. This Model is not a rigid structure but an adaptable framework that allows organizations' business units, management, and architectural design practitioners to commit to collaboration and cohesiveness in designing and protecting the organization's architecture. Security architect designers will better understand how to systematically manage architecture security and continuously measure progress to improve overall architecture security posture. This methodology was created to seamlessly integrate into any existing organization's IT architecture maturity and any security frameworks or methods administered by the security team (the "Work").

ISAUnited does not claim that using any Work will ensure a successful outcome. The Work should not be considered inclusive of all proper information, procedures, and tests or exclusive of other information, procedures, and tests reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure, or test, enterprise governance of information and technology, assurance, risk, and security professionals should apply their professional judgment to the specific circumstances presented by the systems or information technology environment.

Copyright

ISAUnited.org

1923 Washington Ave
Houston, Texas 77007.
Website: www.isaunited.org
Email: info@isaunited.org

Abstract

The evolving digital landscape poses a significant challenge for architecture practitioners, particularly security architecture designers, as they navigate the complexities of hybrid on-premises and cloud architectures. With the vast array of components and systems requiring design, maintenance, and security measures, practitioners struggle to establish their organization's digital footprint effectively. The absence of or the use of an unstructured comprehensive framework leaves security architects without clear direction and guidance, hindering their ability to address the intricate demands of securing modern IT infrastructures.

The "Well-Secured-Architected" framework presents a comprehensive and structured approach to designing, implementing, and maintaining secure cloud architectures, tailored specifically for the unique challenges and opportunities of cloud computing.

This whitepaper introduces the four core pillars of the Well-Secured-Architected framework: Enterprise Security Architecture, Cloud Security Architecture, Security Architecture Design, and Security Standards and Controls. Each pillar encompasses a set of strategies, planning processes, execution methodologies, and deployment best practices, providing a holistic and defense-in-depth approach to security architecture.

The Enterprise Security Architecture pillar focuses on developing a strategic security blueprint aligned with organizational goals and risk tolerance while establishing strong organizational security foundations through policies, procedures, and governance structures. The Cloud Security Architecture pillar equips organizations with the expertise and controls necessary to leverage cloud services securely and mitigate cloud-specific risks.

The Security Architecture Design pillar emphasizes the importance of secure design principles, defensible patterns, and resilient architectures, integrating security from the outset rather than as an afterthought. Finally, the Security Standards and Controls pillar ensures adherence to relevant regulations, industry standards, and best practices, providing compliance and security assurance framework.

By following the Well-Secured-Architected methodology, organizations can streamline designing, implementing, and maintaining secure architectures, foster cross-functional collaboration, and implement continuous improvement mechanisms. This whitepaper explores the benefits of adopting the Well-Secured-Architected framework, including comprehensive security coverage, effective risk mitigation, enhanced compliance, increased stakeholder trust, and potential cost savings.

As cyber threats evolve, the Well-Secured-Architected framework offers a robust and adaptable approach to securing cloud architectures. It empowers organizations to stay ahead of emerging risks and maintain a resilient security posture in an ever-changing threat landscape.

www.isaunited.org
info@ISAUnited.org
Houston, TX

Contents

www.isaunited.org
info@ISAUnited.org
Houston, TX

The CORE4 Model

Well-Secured-Architected

A Model for Safeguarding Architecture

Introduction

Problem Statement

The statement 'The absence of or the use of an unstructured comprehensive framework leaves security architects without clear direction and guidance, hindering their ability to address the intricate demands of securing modern IT infrastructures,' encapsulates the challenges and problems faced by security architects when lacking a well-defined, structured framework for enterprise security architecture, as perceived by ISAUnited.

Absence of a comprehensive framework:
The lack of a comprehensive, overarching framework for security architecture design and implementation leaves security architects without a clear roadmap or set of guidelines. This absence creates ambiguity and uncertainty, making it difficult for architects to navigate the complexities of modern IT infrastructures effectively.

Use of an unstructured framework:
Even if a framework exists, it can be equally problematic if it is unstructured or lacks a cohesive approach. An unstructured framework may provide fragmented or disjointed guidance, failing to address the interconnected nature of security concerns across different domains and technologies.

Lack of clear direction and guidance:
Security architects lack the direction and guidance to make informed decisions and consistently implement best practices without a comprehensive, structured framework. This absence of clear guidance can lead to ad hoc or inconsistent approaches, potentially introducing vulnerabilities or inefficiencies in the security architecture.

Hindering the ability to secure modern IT infrastructures:
Modern IT infrastructures are increasingly complex, spanning on-premises, cloud, and hybrid environments, with many components and systems to secure. The absence of a comprehensive framework hinders security architects' ability to effectively address the intricate demands of securing these infrastructures, as they lack a structured approach to navigate the various security considerations and requirements.

ISAUnited aims to highlight the critical need for a comprehensive and structured framework that provides security architects with clear direction, guidance, and best practices for designing, implementing, and maintaining robust and adaptable security architectures in today's complex IT landscapes.

www.isaunited.org
info@ISAUnited.org
Houston, TX

Background

Cloud providers typically utilize "well-architected" as a framework. A well-architected framework serves as a blueprint or reference model that organizations can follow when architecting solutions on the cloud provider's platform. It guides various dimensions such as operational excellence, security, reliability, performance efficiency, and cost optimization.

Cloud providers offer a well-architected framework as a resource to help their customers design and implement cloud architectures that align with industry best practices and effectively leverage the capabilities of their cloud platform. While the specific implementation may vary slightly between cloud providers, the core principles remain consistent.

Overview of the Well-Architected Framework in Cloud Security

ISAUnited has embraced this framework, tailoring it to suit security architecture needs. The well-architected framework is valuable for organizations seeking to design, deploy, and manage cloud-based solutions, prioritizing reliability, security, efficiency, and cost-effectiveness.

1. **Enterprise Security Architecture:**
   This pillar would encompass the holistic, organization-wide approach to security architecture, aligning IT security with the overall business strategy and objectives. It would incorporate elements from ISAUnited's existing frameworks, such as the Defensible Architecture Design Methodology and Security-by-Design principles.
2. **Cloud Security Architecture:**
   This pillar would focus on the principles, best practices, and controls for securing cloud-based infrastructure, applications, and data. It would leverage guidance from cloud providers' well-architected frameworks while addressing multi-cloud and hybrid cloud environments.
3. **Security Architecture Design:**
   This pillar would cover the design principles, patterns, and methodologies for creating secure and defensible architectures. It would draw from ISAUnited's Security Design Operations (SDO) framework and other design-focused resources.
4. **Security Standards and Controls:**
   This pillar would encompass the various security standards, frameworks, and control sets that organizations must adhere to, such as NIST, ISO, and industry-specific regulations. It would guide in selecting, implementing, and maintaining appropriate security controls.

These four pillars would form the foundation of the Well-Secured-Architected methodology, ensuring a comprehensive approach that addresses enterprise-wide security architecture, cloud-specific security considerations, secure design principles, and compliance with relevant standards and controls.
By aligning with and encompassing ISAUnited's existing frameworks and methodologies, these pillars would consolidate security resources into a cohesive, well-architected system, enabling organizations to streamline the process of building robust and adaptable security architectures.

www.isaunited.org
info@ISAUnited.org
Houston, TX

Core Pillars of the Well-Secured-Architected Framework

The identified four core pillars of the "Well-Secured-Architected" framework appear to provide a comprehensive and structured approach to addressing security concerns within cloud architectures. Each pillar encompasses critical aspects of security architecture, from strategic alignment to practical implementation and ongoing compliance.

Here's a breakdown of each pillar and its significance:

1. **Enterprise Security Architecture**:
    - **Holistic Security Blueprint -** This pillar emphasizes developing a comprehensive security blueprint that aligns with the organization's objectives and risk tolerance. It involves assessing the entire enterprise landscape to identify security requirements and priorities.
    - **Organizational Security Foundations -** Establishing strong organizational security foundations involves defining policies, procedures, and governance structures to ensure consistent and effective security practices.
    - **Strategic Security Alignment -** Strategic alignment ensures that security initiatives are closely aligned with business goals and objectives, enabling security to be viewed as an enabler rather than a hindrance to organizational success.
2. **Cloud Security Architecture**:
    - **Cloud Security Mastery -** This pillar focuses on acquiring the necessary expertise and skills to effectively secure cloud environments, considering the unique security challenges and opportunities cloud computing presents.
    - **Secure Cloud Enablement -** Secure cloud enablement involves implementing security controls and best practices to enable the safe adoption and use of cloud services, ensuring that security is integrated into every aspect of cloud deployment.
    - **Cloud Security Vanguard -** At the forefront of cloud security involves continuously monitoring emerging threats, technologies, and best practices to avoid potential security risks and vulnerabilities.
3. **Security Architecture Design**:
    - **Secure Design Principles -** Secure design principles guide the development of secure architectures from the outset, incorporating security considerations into the design process rather than treating security as an afterthought.
    - **Defensible Design Patterns -** Defensible design patterns help architects and developers build systems inherently resilient to security threats, using proven patterns and techniques to mitigate common attack vectors.
    - **Architecting Resilient Security -** Architecting resilient security involves designing architectures that can adapt and respond to evolving security threats and challenges, ensuring that security remains effective in changing circumstances.
4. **Security Standards and Controls**:
    - **Compliance and Control Frameworks -** Compliance and control frameworks provide a structured approach to meeting regulatory requirements and industry standards, ensuring that security controls are implemented effectively and consistently.
    - **Regulatory Security Guardrails -** Regulatory security guardrails help organizations navigate complex regulatory landscapes by establishing clear guidelines and requirements for achieving and maintaining compliance.

- **Standards-Driven Security Assurance -** Standards-driven security assurance involves implementing security controls and practices that adhere to industry standards and best practices, ensuring stakeholders that security requirements are being met.

These four pillars provide a solid foundation for building and maintaining secure cloud architectures, covering everything from strategic planning and design principles to practical implementation and compliance. Adhering to these pillars can help organizations effectively manage security risks and ensure their cloud-based systems and data's confidentiality, integrity, and availability.

Some of these suggested names aim to capture the essence of each pillar's focus, while others emphasize the desired outcomes or benefits. For example, "Holistic Security Blueprint" and "Strategic Security Alignment" convey the enterprise-wide, strategic nature of the first pillar. In contrast, "Cloud Security Mastery" and "Secure Cloud Enablement" highlight the specialized expertise required for the second pillar.

Similarly, "Defensible Design Patterns" and "Architecting Resilient Security" emphasize the design principles and patterns for creating secure architectures. At the same time, "Compliance and Control Frameworks" and "Standards-Driven Security Assurance" underscore the importance of adhering to industry standards and regulatory requirements.

These catchy names can help make the pillars more memorable and easily recognizable while conveying their respective scopes and objectives within the broader "Well-Secured-Architected" methodology.

Implementing the Well-Secured-Architected Framework

- Analyze existing security frameworks and methodologies.
- Establish Well-Secured-Architected pillars.
- Develop the Well-Secured-Architected methodology.
- Foster cross-functional collaboration.
- Provide assessment and improvement mechanisms.
- Ensure continuous improvement.

Analyze Existing Security Frameworks and Methodologies

- Review the key security frameworks and methodologies currently offered by ISAUnited, such as:
  - Security Design Operations (SDO) framework
  - Defensible Architecture Design Methodology
  - Security-by-Design principles
- Identify common elements, principles, and best practices across these frameworks.

Establish Well-Secured-Architected Pillars

- Define the core pillars or principles that will form the foundation of the Well-Secured-Architected methodology:

www.isaunited.org
info@ISAUnited.org
Houston, TX

  - **Enterprise Security Architecture**
  - **Cloud Security Architecture**
  - **Security Architecture Design**
  - **Security Standards**
  - **Security Controls**
  - **Security Project Management**
  - **Operational Excellence**
- Ensure these pillars align with and encompass the existing ISAUnited frameworks.

Develop Well-Secured-Architected Methodology

- Create detailed, step-by-step guidance for implementing the Well-Secured-Architected approach.
- Develop templates, checklists, and other resources to support implementation.
- Provide case studies and examples demonstrating the application of the methodology.

Emphasize Cross-Functional Collaboration

- Foster collaboration between security architects, IT professionals, and other stakeholders throughout the design and implementation phases.
- Establish strategies for promoting a collaborative environment, such as cross-functional teams, regular meetings, and shared documentation.

Provide Assessment and Improvement Mechanisms

- Develop a self-assessment tool to evaluate the organization's security architecture against the Well-Secured-Architected principles.
- Identify areas for improvement and optimization based on the assessment results.
- Implement iterative enhancements to the security architecture based on the identified improvement areas.

Ensure Continuous Improvement

- Establish processes for regularly reviewing and updating the Well-Secured-Architected methodology.
- Incorporate feedback from users and industry developments to refine the methodology.
- Adapt the methodology to address evolving security threats, technological advancements, and regulatory changes.

By following this Well-Secured-Architected Security Program, security architects can consolidate ISAUnited's various security frameworks and methodologies into a cohesive, well-architected approach. This program provides a structured process for designing, implementing, and continuously improving an

organization's enterprise security architecture, ensuring a robust, resilient, and adaptable security posture.

Benefits of the Well-Secured-Architected Approach

- Comprehensive security coverage
- Risk mitigation
- Compliance and regulatory requirements
- Enhanced trust and confidence
- Cost savings
- Balanced and holistic approach

Security architecture designers can leverage ISAUnited's four core pillars of the "well-secured-architected" framework to establish clear guidance and best practices for strategy, planning, execution, and deployment to secure their enterprise's architecture effectively.

1. **Enterprise Security Architecture**:
    - **Strategy -** Security architects can develop a strategic plan for creating a holistic security blueprint aligned with the organization's business goals and risk tolerance. This involves identifying security requirements, conducting risk assessments, and defining security objectives.
    - **Planning -** Based on the strategic plan, security architects can formulate organizational security foundations by establishing policies, procedures, and governance structures. This includes defining roles and responsibilities, establishing security controls, and implementing security awareness programs.
    - **Execution -** Security architects oversee the implementation of security controls and mechanisms to enforce organizational security foundations. This may involve deploying security technologies, training, and implementing incident response procedures.
    - **Deployment -** Security architects ensure that security measures are effectively deployed across the organization's enterprise architecture, including networks, systems, applications, and data repositories. They collaborate with stakeholders to integrate security into the development lifecycle and ensure compliance with security policies and standards.
2. **Cloud Security Architecture**:
    - **Strategy -** Security architects develop a strategy for mastering cloud security by acquiring relevant skills and knowledge and understanding the unique security challenges and opportunities of cloud computing.
    - **Planning -** Security architects plan for secure cloud enablement by identifying cloud security requirements, selecting appropriate cloud services, and designing security controls for cloud environments.
    - **Execution -** Security architects implement security controls to protect cloud-based assets and data, including identity and access management, encryption, network security, and monitoring.
    - **Deployment -** Security architects ensure that cloud security measures are integrated seamlessly into the organization's cloud deployments, leveraging cloud security best practices and standards to mitigate risks effectively.
3. **Security Architecture Design**:

- **Strategy -** Security architects define secure design principles to guide the development of secure architectures, emphasizing security by design and adopting a proactive approach to security.
- **Planning -** Security architects plan for defensible design patterns by identifying common security threats and vulnerabilities and designing architectures that mitigate these risks effectively.
- **Execution -** Security architects implement resilient security architectures by incorporating security controls, mechanisms, and countermeasures into the design and implementation of systems and applications.
- **Deployment -** Security architects ensure that security architectures are deployed successfully, conducting reviews and assessments to verify that security requirements are met and addressing any gaps or deficiencies.

4. **Security Standards and Controls**:
   - **Strategy -** Security architects develop a strategy for compliance and control frameworks by identifying applicable regulations, standards, and industry best practices.
   - **Planning -** Security architects plan for regulatory security guardrails by mapping security controls to regulatory requirements and defining compliance monitoring and reporting processes.
   - **Execution -** Security architects implement security controls and measures to achieve compliance with regulatory requirements and industry standards, leveraging standards-driven security assurance to demonstrate adherence to security standards.
   - **Deployment -** Security architects ensure that security controls are deployed effectively across the organization, conducting audits, assessments, and reviews to validate compliance and address any non-compliance issues.

By following ISAUnited's four core pillars of the "well-secured-architected" framework, security architecture designers can develop a structured approach to securing their organization's enterprise architecture. This approach enables clear guidance and best practices for strategy, planning, execution, and deployment of security measures. This comprehensive approach helps organizations effectively manage security risks and protect their digital assets in an ever-evolving threat landscape.

Driving Success: The Value Proposition of Embracing Security Architecture Principles

Using the "well-architected" framework primarily for security architecture purposes, such as "well-secured-architected," is a pragmatic and focused approach, particularly in organizations like ISAUnited that prioritize security as a critical aspect of their operations. Security is undeniably one of the most crucial considerations in any IT architecture, especially in today's landscape, where cyber threats are increasingly sophisticated and prevalent.

By adopting the well-architected framework to address security concerns, ISAUnited can ensure that its cloud-based systems are robustly protected against a wide range of threats, including data breaches, unauthorized access, malware, and other cyber-attacks. This focused approach allows them to tailor their architectural decisions, processes, and controls to reinforce security measures effectively.

Here are some potential benefits of using a "well-secured-architected" approach:

- **Comprehensive Security Coverage -** By aligning with the well-architected framework and emphasizing security, ISAUnited can systematically address various security considerations across their cloud infrastructure, applications, and data, ensuring comprehensive security coverage.
- **Risk Mitigation -** A security-focused approach helps identify and mitigate potential security risks early in the design and implementation stages, reducing the likelihood of security incidents and their associated impacts on the organization.
- **Compliance and Regulatory Requirements -** Many industries are subject to stringent data protection and privacy regulations. By incorporating security best practices from the well-architected framework, ISAUnited can better meet compliance obligations and demonstrate adherence to regulatory standards.
- **Enhanced Trust and Confidence -** Demonstrating a solid commitment to security protects ISAUnited's assets and sensitive information and fosters trust and confidence among their stakeholders, including customers, partners, and regulatory bodies.
- **Cost Savings -** Proactively addressing security considerations within the architectural design phase can help avoid costly security breaches and associated remediation efforts, ultimately leading to long-term cost savings**.**

While focusing on security within the well-architected framework is undoubtedly beneficial, ISAUnited must ensure that other architectural aspects, such as reliability, performance, and cost optimization, are not overlooked. Security should be integrated seamlessly with these other considerations to achieve a balanced and holistic approach to cloud architecture that effectively meets the organization's overall objectives.

Conclusion

Summary of the Well-Secured-Architected Framework

The Well-Secured-Architected framework provides a comprehensive and structured approach for organizations to design, implement, and maintain secure cloud architectures. By adapting the principles of the well-architected framework and tailoring it specifically for security needs, this methodology enables robust protection of digital assets and sensitive information.

The four core pillars of the framework—enterprise Security Architecture, Cloud Security Architecture, Security Architecture Design, and Security Standards and Controls—collectively address the critical aspects of establishing a solid security posture. Each pillar contributes to a holistic and defensible security architecture, from strategic alignment and cloud security mastery to secure design principles and regulatory compliance.

Organizations can develop a holistic security blueprint aligned with their business objectives and risk tolerance through the Enterprise Security Architecture pillar. The Cloud Security Architecture pillar equips them with the expertise and best practices to leverage cloud services securely and mitigate cloud-specific risks. The Security Architecture Design pillar emphasizes secure design principles and resilient architectures, while the Security Standards and Controls pillar ensures adherence to relevant regulations and industry standards.

Organizations can streamline designing, implementing, and maintaining secure architectures by following the Well-Secured-Architected framework's structured approach. This includes analyzing existing security frameworks, establishing the core pillars, developing a detailed methodology, fostering cross-functional collaboration, and implementing continuous improvement mechanisms.

Embracing the Well-Secured-Architected framework offers numerous benefits, including comprehensive security coverage, effective risk mitigation, enhanced compliance, increased stakeholder trust, and potential cost savings. Moreover, it promotes a balanced and holistic approach to cloud architecture, ensuring that security considerations are seamlessly integrated with other architectural aspects like reliability, performance, and cost optimization.

As cyber threats evolve, the Well-Secured-Architected framework provides a robust foundation for organizations to stay ahead of security risks and effectively protect their digital assets. By adopting this security-focused approach, organizations can confidently navigate the complexities of cloud architectures while maintaining a resilient and adaptable security posture.

Call to Action for Adopting the Framework

In today's digital landscape, where cyber threats are ever-present and constantly evolving, embracing a robust and comprehensive security architecture framework is no longer an option – it's imperative. The Well-Secured-Architected framework offers a strategic and battle-tested approach to securing your organization's cloud infrastructure, applications, and data.

By adopting this framework, you can future-proof your security posture, mitigating risks and safeguarding your digital assets against the most sophisticated cyber threats. The four core pillars—Enterprise Security Architecture, Cloud Security Architecture, Security Architecture Design, and Security Standards and Controls—provide a solid foundation for building secure, resilient, and compliant architectures.

Don't leave your organization's security to chance. Take a proactive stance and leverage the Well-Secured-Architected framework to gain a competitive edge in an ever-evolving threat landscape. Empower your security teams with the tools, methodologies, and best practices to design, implement, and maintain robust security architectures that align with your business objectives and risk tolerance.

Embrace the power of this framework and unlock a world of benefits, including comprehensive security coverage, effective risk mitigation, enhanced compliance, increased stakeholder trust, and potential cost savings. Join the ranks of forward-thinking organizations prioritizing security as a critical enabler of success rather than an afterthought.

The time to act is now. Invest in the Well-Secured-Architected framework and pave the way for your organization's secure and resilient future. Contact our team today to learn more about implementing this game-changing approach and elevating your security posture to new heights.

Future Developments and Enhancements

The Well-Secured-Architected framework represents a robust and comprehensive approach to security architecture, but it is not a static or immutable methodology. As technology evolves and new threats emerge, the framework must adapt and incorporate advancements to remain relevant and effective. ISAUnited is committed to continuously improving and enhancing the Well-Secured-Architected framework, ensuring it remains at the forefront of security best practices and addresses the latest challenges in the ever-changing cybersecurity landscape. Here are some potential areas for future development and enhancement:

- Emerging Technologies: As new technologies such as artificial intelligence, machine learning, and quantum computing become more prevalent, the framework must be updated to address the unique security considerations and risks associated with these advancements.
- Threat Intelligence Integration: Incorporating real-time threat intelligence data into the framework can help organizations avoid emerging threats and proactively adapt their security architectures to mitigate potential risks.
- Automation and Orchestration: Exploring opportunities for automating security processes and orchestrating security controls can improve efficiency, reduce human error, and enhance the overall effectiveness of the framework.
- Continuous Monitoring and Adaptation: Implementing mechanisms for continuous monitoring and automated adaptation can enable the framework to respond dynamically to changes in the security landscape, ensuring that security architectures remain resilient and up to date.
- Industry-Specific Customizations: As the framework gains wider adoption, ISAUnited may consider developing industry-specific customizations or extensions to address various sectors' unique security requirements and regulatory complexities.
- Integration with DevSecOps: Enhancing the framework's integration with DevSecOps practices can streamline the process of incorporating security into the entire software development lifecycle, fostering a culture of "security-by-design."
- Collaborative Evolution: ISAUnited will actively seek feedback and input from the security community, industry experts, and framework users to identify areas for improvement and drive the collaborative evolution of the Well-Secured-Architected methodology.

By continuously enhancing and adapting the Well-Secured-Architected framework, ISAUnited can ensure that organizations can access the most up-to-date and practical security architecture guidance. This will enable them to stay ahead of emerging threats and maintain a robust and resilient security posture in the face of an ever-evolving cybersecurity landscape.

www.isaunited.org
info@ISAUnited.org
Houston, TX

End of Document.