Information security assurance: Building justified confidence and public trust

Juan Mosso
email: juan.mosso@blacklabel.nz[1]

[1]The Blacklabel company

December 23, 2025

Abstract

This technical essay explores the multifaceted domain of information security and assurance, examining how organizations can build justified confidence in their security measures through standardized approaches, structured methodologies, and systematic validation. The essay investigates the relationship between security implementation and assurance validation, explores the anatomy of assurance cases, and examines practical examples of how assurance principles can be applied in real-world scenarios. Furthermore, it delves into the integration of assurance practices within software and systems development lifecycles, based on the ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 standards, with a particular focus on ISO 15026 workflow alignment and integration. This exploration includes detailed examples of assurance cases, including a network firewall example and a software development use case with specific claims, arguments, and evidence requirements. By understanding the principles, methodologies, and practical applications of information security assurance, organizations can move beyond simply implementing security controls to establishing justified confidence in their effectiveness, thereby supporting strategic objectives such as building and maintaining public trust.

Keywords: Infromation security, assurance, standards, supply chain, cloud.

Contents

1 Introduction

In today's increasingly interconnected digital landscape, organizations face a fundamental challenge: how to establish justified confidence that their information security measures actually work as intended. As systems, attack surfaces, and threats grow more complex, implementing security controls is only half the battle. The other equally important half lies in establishing justified confidence that these controls actually work as intended. This is not merely an academic concern; it has real-world implications for how organizations design, implement, and validate their security programs against strategic outcomes.

Information security and assurance represent two complementary but distinct domains within the broader field of cybersecurity. While security focuses on protecting information through the implementation of controls, assurance provides the grounds for justified confidence that security claims have been or will be achieved. This distinction is crucial for organizations seeking not only to secure their systems but also to demonstrate the effectiveness of their security measures to stakeholders, regulators, and the public.

The concept of assurance exists to provide certainty in an otherwise uncertain environment. At its most basic level, assurance refers to a promise or a statement that inspires confidence. The Cambridge Dictionary defines assurance as "a promise that something is or behaves as expected" or "something that inspires or tends to inspire confidence" (Cambridge University Press, 2023). However, in the context of information security, assurance takes on a more specific and technical meaning, particularly as defined by authoritative standards bodies such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE).

This technical essay explores the multifaceted domain of information security and assurance, examining how organizations can build justified confidence in their security measures through standardized approaches, structured methodologies, and systematic validation. We will investigate the relationship between security implementation and assurance validation, explore the anatomy of assurance cases, and examine practical examples of how assurance principles can be applied in real-world scenarios.

Furthermore, we will delve into the integration of assurance practices within software and systems development lifecycles, based on the ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 standards, with a particular focus on ISO 15026 workflow alignment and integration. This exploration will include detailed examples of assurance cases, including a network firewall example and a software development use case with specific claims, arguments, and evidence requirements.

By understanding the principles, methodologies, and practical applications of information security assurance, organizations can move beyond simply implementing security controls to establishing justified confidence in their effectiveness, thereby supporting strategic objectives such as building and maintaining public trust. This shift from security implementation to assurance validation represents a maturation in organizational security posture, enabling more robust risk management, more effective governance, and ultimately, greater resilience against evolving threats.

2 Building consensus through standardization

In the realm of information security, professionals often face a fundamental challenge when discussing security concepts due to the lack of standardized terminology and shared understanding. This lack of consensus can lead to misaligned definitions, inconsistent approaches, and ultimately, gaps in security posture. To address this challenge, various authoritative bodies have developed standardized definitions and frameworks for assurance, maintaining the core concept of justified confidence while providing specific guidance for implementation.

2.1 General definitions of assurance

At its most basic level, assurance refers to a promise or a statement that inspires confidence. The Cambridge Dictionary defines assurance as "a promise that something is or behaves as expected" or "something that inspires or tends to inspire confidence" (Cambridge University Press, 2023). This general definition captures the essence of assurance as a concept that exists to provide certainty in an otherwise uncertain environment.

However, in the context of information security, more technical and specific definitions are required to guide practitioners in implementing effective assurance practices. These definitions come from various authoritative bodies, each contributing to a more comprehensive understanding of what assurance means in practice.

2.2 Authoritative definitions from standards bodies

2.2.1 ISO/IEC/IEEE 15026 standard family

The ISO/IEC/IEEE 15026 standard family, focused on systems and software engineering and assurance, provides one of the most comprehensive frameworks for understanding and implementing assurance. According to ISO/IEC/IEEE 15026-1, assurance is defined as "grounds for justified confidence that a claim has been or will be achieved" (ISO/IEC/IEEE, 2019).

This definition introduces several important concepts:

1. **Justified confidence**: Not merely belief or hope, but confidence based on objective evidence and reasoning.
2. **Claims**: Specific statements about system properties or behaviors that can be verified.
3. **Achievement**: The realization of claims, either in the present or future state.

The standard further elaborates on related concepts:

- **Assurance case**: "Reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)."
- **Assurance argument**: "Artifact that links tangible evidence and assumptions to provide a convincing and valid argument of a claim under a given context."

- **Assurance information**: "Information including a claim about a system, evidence supporting the claim, an argument showing how the evidence supports the achievement of the claim, and the context for these items."

ISO/IEC/IEEE 15026-4 provides guidance for integrating assurance practices into systems and software life cycles, emphasizing the achievement of specific assurance outcomes:

- Identifying and justifying assurance claims
- Producing evidence to support these claims
- Ensuring that the required degree of confidence is achieved

The 2021 revision of ISO/IEC/IEEE 15026-4 aligns with ISO/IEC/IEEE 15288 for human-made system's life cycle processes and ISO/IEC/IEEE 12207 for software's life cycle processes, creating a cohesive framework for assurance across different domains (ISO/IEC/IEEE, 2021).

2.2.2 NIST definitions and frameworks

The National Institute of Standards and Technology (NIST) offers complementary definitions of assurance that align with the ISO/IEC/IEEE approach while emphasizing specific aspects relevant to U.S. federal agencies and their partners.

NIST Special Publication 800-37 Rev. 2 adapts the ISO/IEC 15026-1 definition, describing assurance as "grounds for justified confidence that a [security or privacy] claim has been or will be achieved" (Force, 2018). Meanwhile, NIST SP 800-39, drawing from the Committee on National Security Systems Instruction (CNSSI) 4009, defines assurance as a "measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the security policy" (Joint Task Force Transformation Initiative, 2011).

NIST SP 800-160, which provides a framework for systems security engineering, includes assurance as a central element. Volume 1, titled "Engineering of Trustworthy Secure Systems," specifically addresses the relevance of assurance cases, stating that they provide "a basis to formalize a discipline for systems security engineering in terms of its principles, concepts, and activities" and demonstrate "how systems security engineering principles, concepts, and activities can be effectively applied to activities" (Ross et al., 2016).

The NIST System Security Engineering Framework is divided into three parts (Problem, Solution, and Trustworthiness), with trust—a core concept built on top of assurance—playing a central role. NIST SP 800-160 aligns with ISO/IEC/IEEE 12207 for software life cycle processes, further reinforcing the connections between these standards.

2.2.3 NZISM approach to assurance

The New Zealand Information Security Manual (NZISM) describes itself as "the New Zealand Government's manual on information governance, assurance, and information systems security." The manual explicitly recognizes the importance of assurance in its scope, stating that it provides "guidance and specific ICT controls to promote a consistent approach to information assurance and information security across all NZ Government" (Government Communications Security Bureau, 2023).

The NZISM emphasizes the Certification and Accreditation (C&A) process as “a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives confidence” in their information security measures. However, it’s worth noting that the C&A process is highly dependent on risk management activities and lacks the structured and systematic approach to support assurance that is found in standards like ISO/IEC/IEEE 15026.

2.3 The Three Lines of Defense (3LoD) model

The Three Lines of Defense (3LoD) model, updated in 2020, is a corporate risk management framework that assigns responsibility across three distinct functions (The Institute of Internal Auditors, 2020). While it has limitations for the information security domain, the model highlights the necessity of assurance activities to be executed by independent roles in a two-stage approach (internal and external).

The model distinguishes between:

1. **First Line**: Operational management that owns and manages risks
2. **Second Line**: Risk management and compliance functions that monitor and facilitate
3. **Third Line**: Internal audit that provides independent assurance

This separation of duties ensures that those implementing controls are not the same as those evaluating their effectiveness, a principle that is fundamental to credible assurance.

2.4 Comparison of different assurance approaches

When comparing these different approaches to assurance, several common themes emerge:

1. **Focus on justified confidence**: All definitions emphasize that assurance is not about absolute certainty but about establishing reasonable confidence based on evidence.
2. **Claim-centric approach**: Assurance revolves around specific claims about system properties or behaviors, rather than general statements about security.
3. **Evidence-based validation**: Confidence must be justified through tangible evidence, not merely assertions or assumptions.
4. **Independence**: Effective assurance often requires separation between those implementing controls and those evaluating them.
5. **Process integration**: Assurance is increasingly viewed not as a separate activity but as an integral part of system and software lifecycles.

However, there are also notable differences in emphasis:

1. **Formality**: ISO/IEC/IEEE standards provide a more formal, structured approach to assurance through assurance cases, while other frameworks may be less prescriptive.
2. **Scope**: Some approaches focus primarily on technical aspects of assurance, while others encompass governance and organizational considerations.

3. **Implementation guidance**: The level of detail provided for implementing assurance practices varies significantly across different standards and frameworks.

By understanding these different approaches to assurance and their commonalities and differences, organizations can develop a more comprehensive and nuanced understanding of what assurance means in practice. This understanding forms the foundation for building consensus around assurance concepts and implementing effective assurance practices that align with recognized standards and best practices.

3 Security and assurance domains

When dealing with information security, there is a key distinction between implementing security controls and proving they work effectively. This distinction forms the basis for understanding the separate but complementary domains of security and assurance. Understanding this distinction is essential for sound security governance and trustworthy risk decisions when developing assurance-specific workflows.

3.1 Distinction between security operations and assurance activities

Security operations focus on designing, implementing, and running controls to protect information. These activities are primarily concerned with the operational aspects of security, such as configuring firewalls, implementing access controls, and monitoring for security incidents. The goal of security operations is to prevent, detect, and respond to security threats in real-time.

Assurance, on the other hand, focuses on validating those controls, testing their effectiveness, and providing confidence that they work as intended. Assurance activities are concerned with evaluating whether security controls meet their objectives, adhere to policies, and provide the expected level of protection. The goal of assurance is to establish justified confidence in the effectiveness of security measures.

This distinction is not merely academic; it has practical implications for how organizations structure their security functions, allocate resources, and make risk-based decisions. By recognizing the different roles and responsibilities of security and assurance domains, organizations can ensure that both implementation and validation receive appropriate attention and resources.

3.2 Security domain characteristics

The security domain is characterized by several key attributes that distinguish it from the assurance domain:

3.2.1 Operational implementation and management

Security controls are implemented and managed by operational teams, such as IT departments and security operations centers. These teams are responsible for the day-to-day operation of security controls, including:

- Designing and implementing security architectures

- Configuring security technologies
- Monitoring for security events
- Responding to incidents
- Maintaining security infrastructure

For example, a firewall is configured by the security operations team to block unauthorized access based on predefined rules. The team is responsible for ensuring that the firewall is properly configured, updated, and monitored for potential breaches.

3.2.2 Technical focus

The security domain emphasizes technical effectiveness, focusing on the proper functioning of security controls from a technical perspective. This includes:

- Technical configuration of security tools
- Integration of security technologies
- Performance optimization
- Technical monitoring and alerting
- Incident response procedures

The primary concern is whether security controls are technically capable of providing the intended protection and whether they are functioning correctly from a technical standpoint.

3.2.3 Continuous operation

Security operations run continuously, providing ongoing protection against threats. This continuous operation involves:

- 24/7 monitoring of security events
- Real-time threat detection and response
- Continuous updates to security configurations
- Ongoing maintenance of security infrastructure
- Regular patching and vulnerability management

The security domain is characterized by its operational nature, with a focus on maintaining continuous protection rather than periodic evaluation.

3.3 Assurance domain characteristics

The assurance domain has distinct characteristics that set it apart from the security domain:

3.3.1 Evaluation and validation

Assurance activities focus on evaluating and validating the effectiveness of security controls. This involves:

- Assessing whether controls meet their objectives
- Validating compliance with policies and standards
- Evaluating the design and implementation of controls
- Testing control effectiveness
- Identifying gaps and weaknesses

Auditors and assurance professionals do not operate or manage security controls but assess whether they are effective and meet objectives. They focus on policy adherence, effectiveness validation, and identifying systemic weaknesses.

3.3.2 Governance focus

The assurance domain emphasizes governance and compliance, focusing on whether security controls align with organizational policies, regulatory requirements, and industry standards. This includes:

- Evaluating alignment with security policies
- Assessing compliance with regulatory requirements
- Verifying adherence to industry standards
- Reviewing governance processes
- Assessing risk management practices

For example, an external ISO 27001 audit verifies whether firewall policies meet international security standards, focusing on governance aspects rather than technical configuration details.

3.3.3 Independent assessment

Assurance activities provide independent validation through audits, assessments, and reviews conducted by parties not directly involved in security operations. This independence ensures:

- Objective evaluation of control effectiveness
- Unbiased identification of gaps and weaknesses
- Credible reporting to stakeholders
- Separation of duties between implementation and evaluation
- Reduced risk of conflicts of interest

The highest level of confidence comes through independent assessments of security claims, using formalized assurance cases, audit findings, and external validations such as ISO 27001 certification.

3.4 Key differences and complementary roles

Several key differences distinguish the security and assurance domains, while also highlighting their complementary roles:

3.4.1 Operational vs. evaluative

Security domains focus on operational implementation and management, while assurance domains focus on evaluation and validation. Security teams implement and operate controls, while assurance teams verify their effectiveness against policies.

3.4.2 Implementation vs. verification

Security teams implement and operate controls, while assurance teams verify their effectiveness against policies. This separation ensures that those responsible for implementing controls are not also responsible for evaluating their effectiveness, providing a necessary check and balance.

3.4.3 Continuous operation vs. periodic validation

Security operations run continuously, while assurance activities often occur at defined intervals. This difference reflects the different nature of these domains: security provides ongoing protection, while assurance provides periodic validation that this protection is effective.

3.4.4 Technical focus vs. governance focus

Security domains emphasize technical effectiveness, while assurance domains emphasize governance and compliance. This difference ensures that both technical and governance aspects of security receive appropriate attention.

3.4.5 Self-assessment vs. independent assessment

Security domains may conduct self-assessments, but assurance domains provide independent validation. This independence is crucial for establishing credible assurance, as it ensures that evaluations are objective and unbiased.

Despite these differences, the security and assurance domains are complementary, each playing a vital role in an organization's overall security posture. Security operations implement and maintain controls, while assurance activities validate their effectiveness. Together, they provide a comprehensive approach to information security that addresses both implementation and validation.

By understanding and respecting the distinct roles and responsibilities of these domains, organizations can ensure that both security implementation and assurance validation receive appropriate attention and resources. This balanced approach leads to more effective security governance, more informed risk decisions, and ultimately, greater confidence in the organization's security posture.

4 Developing assurance-specific workflows

To effectively demonstrate that security controls work as intended, organizations need structured approaches for building and evaluating assurance. This section explores the anatomy of assurance cases, methodologies for their development, and considerations for their effective implementation.

4.1 Anatomy of an assurance case (ISO 15026)

By systematically linking claims, arguments, and evidence, assurance cases provide a comprehensive framework for validating security controls. The ISO/IEC/IEEE 15026 standard family provides a formal structure for assurance cases, consisting of three primary components:

4.1.1 Claims: Statements about security requirements

Claims, the foundation of assurance cases, are specific statements asserting that a security requirement has been or will be met. According to ISO/IEC/IEEE 15026-1, a claim is a "true-false statement about the limitations on the values of an unambiguously defined property, called the claim's property, and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions" (ISO/IEC/IEEE, 2019).

Effective claims have several key characteristics:

1. **Specificity**: Claims should be precise and unambiguous, clearly stating what property or behavior is being assured. Vague claims like "the system is secure" are not useful; specific claims like "all external communications are encrypted using AES-256" provide a clear target for assurance.

2. **Measurability**: Claims should be verifiable through objective evidence. This requires that the property being claimed can be observed, tested, or otherwise validated.

3. **Relevance**: Claims should address security properties that matter to stakeholders and align with security objectives. They should focus on properties that have significant security implications.

4. **Scope definition**: Claims should clearly define their applicability, including system boundaries, conditions, and timeframes. This helps ensure that the claim is evaluated in the appropriate context.

4.1.2 Arguments: Justifications for claims

Arguments provide a chain of reasoning that demonstrates how the evidence justifies confidence in the claim. They form the logical bridge between high-level claims and specific evidence, explaining why the available evidence is sufficient to support the claim.

Effective arguments should:

1. **Be structured logically**: Arguments should follow a clear, logical structure that connects evidence to claims in a coherent manner. This may involve breaking down high-level claims into sub-claims that can be more directly supported by evidence.

2. **Address all aspects of the claim**: Arguments should comprehensively address all aspects of the claim, ensuring that no critical elements are overlooked.

3. **Consider counterarguments**: Strong arguments anticipate and address potential counterarguments or weaknesses, demonstrating that the claim holds even in the face of challenges.

4. **Be explicit about assumptions**: Arguments should clearly state any assumptions upon which they rely, ensuring that these assumptions are reasonable and justified.

4.1.3 Evidence: Proof validating arguments

Evidence consists of the factual information that supports arguments. It provides the concrete basis for assurance, demonstrating that claims are not merely assertions but are grounded in reality.

Evidence can take many forms, including:

1. **Documentation**: System specifications, design documents, security policies, and procedures.
2. **Test results**: Results of security testing, penetration testing, and vulnerability assessments.
3. **Audit findings**: Reports from internal or external audits of security controls.
4. **Monitoring data**: Logs, alerts, and other operational data demonstrating control effectiveness.
5. **Configuration data**: Information about how systems and controls are configured.
6. **Certifications**: Third-party certifications of compliance with security standards.

The quality of evidence is crucial for the strength of an assurance case. Evidence should be relevant to the claim, sufficient to support the argument, reliable (from trustworthy sources), and current (reflecting the present state of the system).

4.2 Methodology for building assurance cases

Building effective assurance cases requires a systematic methodology that ensures comprehensive coverage, logical coherence, and sufficient evidence. The following methodology provides a structured approach to developing assurance cases:

4.2.1 Identifying security objectives

The first step in building an assurance case is to determine the security properties or requirements that need assurance. These objectives should be derived from:

- Organizational security policies and requirements
- Regulatory and compliance obligations
- Risk assessments and threat models
- Stakeholder concerns and expectations

Security objectives should be clearly defined and prioritized based on their importance to the organization's security posture.

4.2.2 Formulating top-level claims

Based on the identified security objectives, develop specific, measurable claims about how the system meets these objectives. Top-level claims should:

- Directly address security objectives
- Be stated in clear, unambiguous language
- Focus on outcomes rather than implementation details
- Be verifiable through evidence

For example, a top-level claim might be: “The organization’s firewall effectively protects the network by restricting unauthorized access while allowing legitimate traffic, in accordance with security policies and regulatory requirements.”

4.2.3 Developing sub-claims

Break down top-level claims into more specific sub-claims that collectively support the top-level claim. This decomposition makes the assurance case more manageable and helps identify specific areas where evidence is needed.

Sub-claims should:

- Address specific aspects of the top-level claim
- Be more detailed and focused than the top-level claim
- Collectively provide comprehensive coverage of the top-level claim
- Be directly supportable by evidence

For example, sub-claims for a firewall might address rule configuration, access control implementation, threat detection, resilience, and monitoring.

4.2.4 Constructing arguments

Develop logical reasoning that connects sub-claims to top-level claims and evidence to sub-claims. Arguments should:

- Clearly explain how evidence supports claims
- Address potential weaknesses or counterarguments
- Make explicit any assumptions or dependencies
- Provide a complete chain of reasoning from evidence to claims

Arguments may be structured in various ways, including deductive reasoning (from general principles to specific conclusions), inductive reasoning (from specific observations to general conclusions), or a combination of both.

4.2.5 Identifying and collecting evidence

Determine what evidence is needed to support arguments and collect this evidence through testing, auditing, and other methods. Evidence collection should:

- Focus on the most relevant and convincing evidence
- Consider multiple sources of evidence for critical claims
- Ensure evidence is current and accurate

- Document evidence in a way that facilitates review and validation

Evidence collection may involve various activities, including security testing, configuration reviews, log analysis, and documentation reviews.

4.2.6 Evaluating the case

Assess the completeness, coherence, and strength of the assurance case. This evaluation should:

- Verify that all claims are supported by arguments and evidence
- Check for logical consistency and completeness
- Identify any gaps or weaknesses in the case
- Assess the overall strength of the case in establishing justified confidence

Evaluation may involve peer reviews, expert assessments, or formal validation methods.

4.2.7 Addressing gaps and weaknesses

Identify and address any gaps in evidence or weaknesses in arguments. This may involve:

- Collecting additional evidence
- Strengthening arguments
- Refining claims to be more specific or realistic
- Documenting limitations or caveats

Addressing gaps and weaknesses is an iterative process that continues until the assurance case provides sufficient confidence in the security claims.

4.2.8 Documenting the case

Create comprehensive documentation of the assurance case for review and future reference. Documentation should:

- Clearly present claims, arguments, and evidence
- Explain the relationships between these elements
- Provide context for understanding the case
- Be accessible to relevant stakeholders

Documentation may take various forms, including structured reports, diagrams, or specialized assurance case notation.

4.2.9 Reviewing and updating

Periodically review and update the assurance case as systems, threats, and evidence evolve. This ensures that assurance remains current and relevant. Reviews should be conducted:

- When significant changes occur to the system

- When new threats or vulnerabilities emerge
- When new evidence becomes available
- At regular intervals as part of the security lifecycle

4.3 Limitations of assurance cases

While assurance cases provide a powerful framework for establishing justified confidence in security, they have several limitations that should be recognized:

1. **Not guarantees**: Assurance cases explain design decisions and provide justified confidence, but they do not certify absolute security. They support informed risk decisions rather than providing certainty.
2. **Evidence-bound**: Assurance cases rely on known information and may miss unknown or emerging threats. They are limited by the quality and completeness of available evidence.
3. **Resource-limited**: The depth and comprehensiveness of assurance cases depend on available time, people, and funding. Resource constraints may limit the scope or depth of assurance activities.
4. **Implementation-sensitive**: Poor execution can weaken even well-planned assurance cases. The effectiveness of assurance depends on how well the methodology is implemented.
5. **Bias-prone**: Those building assurance cases may unintentionally seek confirming evidence and overlook contradictory information. This confirmation bias can weaken the objectivity of assurance.
6. **Snapshot in time**: Assurance cases reflect a moment in a constantly changing threat landscape. They require regular updates to remain relevant.

These limitations highlight that assurance cases support informed risk decisions—not certainty—aligning with the reality that security manages, not eliminates, risk.

4.4 The role of doubt and skepticism in assurance

Doubt plays a crucial role in the development and evaluation of assurance cases. A healthy skepticism helps identify weaknesses, challenge assumptions, and strengthen the overall case. This skepticism can be directed at different elements of the assurance case:

1. **Doubt the claim**: Questioning whether the claim itself is valid or whether there is information that contradicts it. This helps ensure that claims are realistic and well-founded.
2. **Doubt the argument**: Questioning whether the reasoning connecting evidence to claims is sound and comprehensive. This helps identify logical fallacies, gaps in reasoning, or unstated assumptions.
3. **Doubt the evidence**: Questioning whether the evidence is sufficient, reliable, and relevant to support the arguments. This helps ensure that evidence is of high quality and directly supports the claims being made.

By incorporating doubt and skepticism into the assurance process, organizations can develop stronger, more resilient assurance cases that provide greater confidence in security controls. This approach acknowledges the inherent uncertainties in security and seeks to address them through rigorous questioning and validation.

In conclusion, developing assurance-specific workflows through structured assurance cases provides a systematic approach to establishing justified confidence in security controls. By understanding the anatomy of assurance cases, following a methodical approach to their development, recognizing their limitations, and embracing the role of doubt and skepticism, organizations can build more effective assurance practices that support sound security governance and trustworthy risk decisions.

5 Assurance in software and systems development

The integration of assurance practices into software and systems development lifecycles represents a critical evolution in how organizations approach security validation. This section explores how the ISO/IEC/IEEE 15288 systems lifecycle processes and ISO/IEC/IEEE 12207 software lifecycle processes can be aligned with ISO 15026 assurance workflows to create a comprehensive approach to development assurance.

5.1 ISO/IEC/IEEE 15288 systems lifecycle processes

ISO/IEC/IEEE 15288 establishes a common framework of process descriptions for describing the lifecycle of systems created by humans. This standard provides a comprehensive set of processes and associated terminology from an engineering viewpoint, applicable at any level in the hierarchy of a system's structure (ISO/IEC/IEEE, 2023).

5.1.1 Overview and key concepts

ISO/IEC/IEEE 15288:2023, the latest version of the standard, defines a system as a "combination of interacting elements organized to achieve one or more stated purposes." These elements may include hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities.

The standard recognizes that systems exist within a broader context that includes operational, social, regulatory, and environmental factors. This holistic view is essential for effective assurance, as it acknowledges that system security depends not only on technical controls but also on how the system interacts with its environment.

Key concepts in ISO/IEC/IEEE 15288 include:

1. **Lifecycle stages**: The evolution of a system through conception, development, production, utilization, support, and retirement.
2. **Processes**: A set of interrelated or interacting activities that transform inputs into outputs.
3. **Stakeholders**: Individuals or organizations having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations.
4. **System-of-interest**: The system whose lifecycle is under consideration.

5. **Enabling systems**: Systems that support a system-of-interest during its lifecycle stages but do not necessarily contribute directly to its function during operation.

5.1.2 Process groups and their relationship to assurance

ISO/IEC/IEEE 15288 organizes processes into four main groups, each with specific implications for assurance:

1. **Agreement processes**: These processes define the activities necessary to establish agreements between two organizations. From an assurance perspective, these processes ensure that security requirements and assurance expectations are clearly defined and agreed upon between acquirers and suppliers.
    - Acquisition process
    - Supply process
2. **Organizational project-enabling processes**: These processes manage the organization's capability to acquire and supply products or services through the initiation, support, and control of projects. For assurance, these processes establish the organizational foundation for security validation and provide resources for assurance activities.
    - Life cycle model management process
    - Infrastructure management process
    - Portfolio management process
    - Human resource management process
    - Quality management process
    - Knowledge management process
3. **Technical management processes**: These processes address the management of technical aspects of the project. In the context of assurance, these processes ensure that security considerations are integrated into project planning, assessment, control, and decision-making.
    - Project planning process
    - Project assessment and control process
    - Decision management process
    - Risk management process
    - Configuration management process
    - Information management process
    - Measurement process
    - Quality assurance process
4. **Technical processes**: These processes transform stakeholder needs into a product or service. From an assurance perspective, these processes ensure that security

requirements are properly defined, implemented, verified, and validated throughout the system lifecycle.

- Business or mission analysis process
- Stakeholder needs and requirements definition process
- System requirements definition process
- Architecture definition process
- Design definition process
- System analysis process
- Implementation process
- Integration process
- Verification process
- Transition process
- Validation process
- Operation process
- Maintenance process
- Disposal process

The verification and validation processes are particularly relevant to assurance, as they provide the mechanisms for confirming that the system meets its specified requirements (verification) and fulfills its intended use in its operational environment (validation).

5.2 ISO/IEC/IEEE 12207 software lifecycle processes

ISO/IEC/IEEE 12207 establishes a common framework for software lifecycle processes, with well-defined terminology that can be referenced by the software industry. This standard provides processes that can be employed for defining, controlling, and improving software lifecycle processes within an organization or a project (ISO/IEC/IEEE, 2017).

5.2.1 Overview and key concepts

ISO/IEC/IEEE 12207:2017, the current version of the standard, recognizes that software is rarely standalone and typically exists within a larger system context. The standard acknowledges a continuum of human-made systems from those that use little or no software to those in which software is the primary interest.

The processes in ISO/IEC/IEEE 12207 have the same process purpose and outcomes as their counterparts in ISO/IEC/IEEE 15288, but they differ in activities and tasks to focus specifically on software engineering rather than systems engineering.

Key concepts in ISO/IEC/IEEE 12207 include:

1. **Software element**: A system element that is software.
2. **Software item**: An identifiable part of a software product or software element.

3. **Software product**: A set of computer programs, procedures, and possibly associated documentation and data.
4. **Software system**: A system that consists predominantly of software elements.

5.2.2 Process groups and their relationship to assurance

ISO/IEC/IEEE 12207 organizes processes into the same four main groups as ISO/IEC/IEEE 15288, but with a specific focus on software:

1. **Agreement processes**: These processes define the activities necessary to establish agreements between two organizations for software acquisition or supply. From an assurance perspective, these processes ensure that software security requirements and assurance expectations are clearly defined and agreed upon.
2. **Organizational project-enabling processes**: These processes manage the organization's capability to acquire and supply software products or services. For software assurance, these processes establish the organizational foundation for security validation and provide resources for software assurance activities.
3. **Technical management processes**: These processes address the management of technical aspects of the software project. In the context of software assurance, these processes ensure that security considerations are integrated into project planning, assessment, control, and decision-making.
4. **Technical processes**: These processes transform stakeholder needs into a software product or service. From a software assurance perspective, these processes ensure that security requirements are properly defined, implemented, verified, and validated throughout the software lifecycle.

The software verification process and software validation process are particularly relevant to software assurance, as they provide the mechanisms for confirming that the software meets its specified requirements and fulfills its intended use.

5.3 ISO 15026 workflow alignment and integration

The ISO/IEC/IEEE 15026 standard family provides a framework for assurance that can be integrated with the lifecycle processes defined in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207. This integration enables organizations to build assurance into their development processes rather than treating it as a separate activity.

5.3.1 Assurance in the lifecycle (ISO/IEC/IEEE 15026-4)

ISO/IEC/IEEE 15026-4:2021, titled "Systems and software engineering — Systems and software assurance — Part 4: Assurance in the life cycle," provides guidance and recommendations for assurance of selected claims about systems and software (ISO/IEC/IEEE, 2021). The standard offers:

1. A system assurance process view on top of ISO/IEC/IEEE 15288
2. A software assurance process view on top of ISO/IEC/IEEE 12207

These process views help organizations integrate assurance activities into their existing development processes, ensuring that assurance is considered throughout the lifecycle rather than as an afterthought.

The standard emphasizes achieving specific assurance outcomes:

- Identifying and justifying assurance claims
- Producing evidence to support these claims
- Ensuring that the required degree of confidence is achieved

5.3.2 Mapping assurance activities to development processes

To effectively integrate assurance into development processes, organizations need to map assurance activities to specific lifecycle processes. This mapping ensures that assurance considerations are addressed at the appropriate points in the development lifecycle.

The following table illustrates how assurance activities can be mapped to key lifecycle processes.

Lifecycle process	**Assurance activities**
Business or mission analysis	• Identify critical properties requiring assurance • Define assurance objectives based on business needs
Stakeholder needs and requirements definition	• Identify security and assurance requirements • Define assurance claims based on stakeholder needs
System/software requirements definition	• Specify verifiable security requirements • Develop preliminary assurance arguments
Architecture definition	• Evaluate security architecture against claims • Identify evidence needed to support arguments
Design definition	• Review security design against requirements • Update assurance arguments based on design decisions
Implementation	• Apply secure coding practices • Collect evidence of secure implementation
Integration	• Verify security of integrated components • Validate security properties at integration points

Lifecycle process	Assurance activities
Verification	• Test security controls against requirements • Validate assurance arguments with evidence
Validation	• Confirm system meets security objectives • Finalize assurance cases with complete evidence
Operation and maintenance	• Monitor ongoing control effectiveness • Update assurance cases as the system evolves
Disposal	• Verify secure decommissioning • Archive assurance information for future reference

Table 1: Mapping assurance activities to lifecycle processes

This mapping ensures that assurance activities are integrated throughout the development lifecycle, with each process contributing to the overall assurance of the system or software.

5.3.3 Integrating assurance into different development methodologies

The integration of assurance activities into development processes must be adapted to different development methodologies, such as waterfall, agile, or DevOps. ISO 15026 provides a flexible framework that can be tailored to various approaches.

Waterfall development In traditional waterfall development, assurance activities can be aligned with distinct phases:

1. **Requirements phase**: Define assurance claims based on security requirements
2. **Design phase**: Develop assurance arguments based on security architecture and design
3. **Implementation phase**: Collect evidence through secure coding practices and code reviews
4. **Testing phase**: Validate assurance arguments through security testing
5. **Deployment phase**: Finalize assurance cases before system release
6. **Maintenance phase**: Update assurance cases as the system evolves

This approach provides a structured, sequential process for building assurance, with clear deliverables at each phase.

Agile development In agile development, assurance activities must be adapted to fit within iterative sprints:

1. **Release planning**: Define high-level assurance claims for the release
2. **Sprint planning**: Identify assurance activities for the sprint
3. **Sprint execution**: Integrate assurance activities into daily development
4. **Sprint review**: Demonstrate security features and assurance evidence

5. **Sprint retrospective**: Improve assurance practices based on lessons learned
6. **Continuous integration**: Automate security testing and evidence collection

This approach distributes assurance activities across sprints, ensuring that security is considered throughout the development process rather than as a final checkpoint.

DevOps and DevSecOps In DevOps and DevSecOps environments, assurance must be highly automated and integrated into continuous integration/continuous deployment (CI/CD) pipelines (Kim et al., 2016; Myrbakken & Colomo-Palacios, 2019):

1. **Automated security testing**: Integrate security testing into CI/CD pipelines
2. **Continuous monitoring**: Collect evidence through automated monitoring
3. **Security as code**: Define security requirements and tests as code
4. **Automated compliance checking**: Verify compliance with security policies
5. **Continuous assurance**: Update assurance cases automatically based on evidence
6. **Feedback loops**: Provide immediate feedback on security issues

This approach enables assurance to keep pace with rapid development cycles, ensuring that security is not sacrificed for speed.

5.4 Challenges in implementing assurance in development

Integrating assurance into software and systems development presents several challenges that organizations must address:

1. **Balancing assurance with development velocity**: Assurance activities can potentially slow down development if not properly integrated. Organizations must find ways to incorporate assurance without impeding progress.
2. **Resource constraints**: Assurance requires expertise and resources that (Content truncated due to size limit. Use line ranges to read in chunks)

6 Building assurance through management systems

While dedicated assurance workflows provide a structured approach to validating security controls, organizations can also build assurance capabilities through their management systems. This section explores how information security management systems, particularly those based on ISO 27001, can serve as enablers for assurance, and how security policies can provide a foundation for assurance claims.

6.1 Assurance within ISO 27001

ISO 27001, the international standard for information security management systems (ISMS), neither explicitly defines nor requires assurance in the same way as specialized assurance standards like ISO 15026. Instead, assurance is built into the framework's core processes and activities, providing an implicit foundation for establishing confidence in security controls (ISO/IEC, 2022).

The standard's scope is limited to the specific information assets and processes covered by the ISMS, and it acknowledges that some risks may be accepted rather than mitigated. Within these boundaries, ISO 27001 provides a structured approach to security management that inherently supports assurance objectives.

6.1.1 ISO 27001 structure and assurance elements

The ISO 27001 framework includes several elements that contribute to assurance:

1. **Planning**: Establishing context, defining information security objectives, and implementing risk management processes and criteria.
2. **Operations**: Implementing operational planning and control, and conducting risk management activities.
3. **Evaluation**: Performing management reviews, internal audits, and continuous improvement activities.

The standard specifically addresses assurance in the context of internal audits, stating that "Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management." This recognition of assurance activities, even if not explicitly labeled as such, demonstrates the standard's awareness of the need for validation beyond mere implementation.

6.2 ISO 27001 PDCA, continual assurance enabler

The Plan-Do-Check-Act (PDCA) cycle that underpins ISO 27001 serves as a continual assurance enabler, providing a structured approach to establishing, implementing, maintaining, and improving an ISMS. Each phase of the PDCA cycle contributes to assurance in specific ways:

6.2.1 Plan phase

The Plan phase supports continual assurance by:

- Setting clear criteria and scope for what needs to be assured and how
- Defining security objectives, risks, and controls
- Establishing the planned intent and documented requirements that form the basis for assurance

Assurance starts with clear intentions and requirements, which the Plan phase provides through its focus on context, objectives, and risk assessment.

6.2.2 Do phase

The Do phase contributes to assurance by:

- Implementing controls and supporting procedures
- Embedding assurance-related activities into operations, such as monitoring and testing

The implementation of controls provides the foundation for what will later be assured, while the integration of assurance activities into operations ensures that validation is not treated as an afterthought.

6.2.3 Check phase

The Check phase is perhaps the most directly relevant to assurance, as it involves:

- Evaluating control effectiveness through audits, reviews, and performance metrics
- Generating assurance evidence and validating whether objectives are being met

This phase produces the evidence and validation that support assurance claims, demonstrating whether security controls are operating as intended and achieving their objectives.

6.2.4 Act phase

The Act phase completes the assurance cycle by:

- Adjusting and improving based on findings
- Updating controls, closing gaps, and strengthening assurance arguments
- Enabling dynamic response to new risks or weak points

This phase ensures that assurance is not a one-time activity but a continuous process of improvement based on feedback and changing circumstances.

The PDCA cycle operates within the limits of operational performance tolerance, creating control management loops that provide ongoing assurance while maintaining operational effectiveness. This balance between assurance and operations is essential for sustainable security management.

6.3 Integration of assurance principles in ISMS

While ISO 27001 does not explicitly require assurance cases, it incorporates several principles that align with assurance concepts:

- **Evidence-based approach**: ISO 27001 emphasizes the importance of evidence in demonstrating control effectiveness, similar to the evidence component of assurance cases.
- **Risk-based focus**: Like assurance cases, ISO 27001 prioritizes controls based on risk assessment, ensuring that resources are allocated to the most critical areas.
- **Systematic evaluation**: ISO 27001 requires systematic evaluation of control effectiveness through internal audits and management reviews, providing a structured approach to validation similar to assurance case methodology.
- **Continuous improvement**: Both ISO 27001 and assurance case methodology emphasize the importance of ongoing improvement based on evaluation results.

However, ISO 27001 certification provides assurance only within the limits of the defined scope and accepted risks. Organizations seeking more comprehensive assurance may need to supplement their ISMS with explicit assurance cases for critical controls or systems.

6.4 The best possible scenario: Trust-centric ISMS

While ISO 27001 helps organizations manage security effectively, a Trust-Centric ISMS, combining its governance framework with formal assurance cases (ISO 15026), is uniquely tailored for government agencies and high-security enterprises where public trust is both a strategic imperative and a legal and regulatory compliance requirement. This hybrid approach delivers the best of both worlds: comprehensive security management and rigorously validated confidence in control effectiveness, ensuring stakeholders (e.g., citizens, regulators, or customers) can rely not just on policies and mechanisms, but on evidence-backed guarantees of security resilience.

6.4.1 Complementary strengths

ISO 27001 (ISMS) and ISO 15026 (Assurance Cases) offer complementary strengths that, when combined, provide a more robust approach to security assurance:

ISMS (ISO/IEC 27001)	**Assurance cases (ISO/IEC/IEEE 15026)**
Provides the governance and control environment	Adds structured confidence that controls are effective
Builds baseline trust across the system	Supports deep trust where it matters most
Best for broad enterprise coverage	Best for targeted, high-assurance needs

Table 2: Complementary strengths of ISMS and assurance cases

ISO 27001 creates the conditions for assurance through its risk-based approach, security policies and controls, and processes for monitoring, review, and continual improvement. Assurance is implicit in processes like risk assessment and treatment, internal audits, management reviews, and performance evaluation. Control confidence is built over time through evidence generated by system operation.

In contrast, ISO 15026 is purpose-built for assurance, focusing on systematically demonstrating justified confidence that systems meet their security requirements through formal assurance cases. Its components—claims, arguments, and evidence—provide a specialized workflow for assurance, often applied to high-stakes systems such as those in defense, critical infrastructure, or aerospace.

6.4.2 Benefits and limitations

The combination of ISMS and assurance cases offers significant benefits but also has limitations:

Benefits of ISO 27001 (Embedded assurance via management systems):

- Scalable across the enterprise
- Integrated with business operations
- Focused on continuous improvement

Limitations of ISO 27001:

- Doesn’t explicitly test or justify security claims
- Lacks structured case-building methods
- May leave gaps in high-assurance environments

Benefits of ISO 15026 (Explicit assurance through assurance cases):

- High transparency and traceability
- Supports structured decision-making
- Builds trust among stakeholders (e.g., regulators, auditors, executives)

Limitations of ISO 15026:

- Resource intensive
- Requires assurance expertise
- May be hard to scale across entire organizations

By combining these approaches, organizations can leverage the comprehensive coverage and operational integration of ISO 27001 while using ISO 15026 assurance cases for critical systems or functions where higher levels of justified confidence are required.

6.5 Security policies as assurance enablers

Security policies, a core element of ISO 27001, can serve as powerful enablers for assurance claims under ISO 15026. The relationship between policies and assurance is multifaceted and mutually reinforcing.

6.5.1 Embedding claims into security policies

ISO 27001, in line with NIST SP 800-39, recognizes the importance of security policies in creating grounds for justified confidence. The standard requires that “Information security policy and topic-specific policies shall be defined, approved by management, published, and communicated to employees and relevant external parties” (ISO/IEC, 2022; Joint Task Force Transformation Initiative, 2011).

These policies operate at different levels:

1. **Enterprise policy**: At the highest level, approved by top management, the enterprise policy provides direction and support for information security.
2. **Topic-specific policies**: At a lower level, topic-specific security policies mandate the implementation of security controls for specific areas such as access control, physical security, network security, backup, and more.

6.5.2 Policies as the foundation for assurance claims

In ISO 15026, an assurance claim is a statement asserting that a system satisfies specific security properties. ISO 27001 requires that organizations establish policies that set expectations, define control objectives, and link to legal, regulatory, and business needs. These well-designed information security policies can serve as the foundation for sound assurance claims.

For example, a policy stating that “All sensitive data must be encrypted at rest and in transit using approved algorithms” provides a clear basis for an assurance claim about data protection. The policy establishes what must be achieved, while the assurance case demonstrates that it has been achieved.

6.5.3 Policies enable structured arguments

ISO 15026 requires that every claim be supported by a structured argument showing how evidence demonstrates the claim is valid. Policies provide the structure for these arguments by defining what must happen (e.g., multi-factor authentication for privileged accounts), which controls implement the policy, and what evidence (logs, configurations, reports) shows the control is in place.

A well-written policy acts as a logical bridge between claims and control evidence, forming the backbone of an assurance argument. It provides the context and requirements against which evidence can be evaluated, ensuring that arguments are grounded in organizational expectations and requirements.

6.5.4 Policies are part of documented information

ISO 15026 emphasizes the need for accessible, reviewed, and controlled assurance documentation. ISO 27001 treats policies as documented information (clause 7.5), requiring that they be approved by management, communicated to relevant personnel, and reviewed and updated regularly.

This ensures that the policies cited in assurance cases are trustworthy and current, not vague or outdated. The documented nature of policies provides a stable reference point for assurance claims, ensuring that what is being assured aligns with organizational expectations.

6.5.5 Policies reflect risk-based thinking

Security assurance claims must reflect real risks and how they are addressed. Policies in ISO 27001 are shaped by risk assessments (clause 6.1), ensuring that they address the most significant threats to the organization.

For instance, if data loss is identified as a key risk, policies may mandate encryption at rest and in transit. The assurance case would then claim: “Data is protected against unauthorized access,” citing encryption controls tied to the policy. This demonstrates that claims are not arbitrary but are grounded in risk-informed, management-approved intentions.

6.5.6 Policies anchor roles and responsibilities

An assurance claim is only as credible as the processes and people behind it. ISO 27001 requires that policies assign roles and responsibilities (clause 5.3), establishing ownership of controls and enabling accountability in assurance arguments.

This helps substantiate that controls aren’t just defined—they’re operational and managed by specific individuals or teams with clear responsibilities. The assignment of roles and responsibilities provides assurance that controls are not merely theoretical but are actively maintained and monitored.

6.5.7 Policies support in shifting assurance left

The concept of “shifting left” involves identifying security weaknesses earlier in the development or operational lifecycle when they are less costly to address. Policies, particularly those related to software development lifecycle (SSDLC), can support this shift by establishing security requirements and validation points throughout the process (Howard & Lipner, 2006).

Examples of how policies can support shifting assurance left include:

- Validating security requirements before implementation
- Assessing design security before coding begins
- Testing security controls during development
- Verifying security properties in pre-production environments
- Providing continuous feedback throughout the development lifecycle

By embedding assurance requirements in policies that govern the entire lifecycle, organizations can ensure that security is considered from the earliest stages rather than being an afterthought or a final checkpoint.

In conclusion, building assurance through management systems provides a comprehensive approach to establishing justified confidence in security controls. By leveraging the strengths of ISO 27001 for broad security management, potentially complementing it with ISO 15026 assurance cases for critical systems, and using security policies as enablers for assurance claims, organizations can develop a robust assurance posture that supports their security objectives while maintaining operational effectiveness.

7 Assurance in the supply chain

Information security assurance in supply chains, particularly those leveraging cloud services, presents significant challenges that require structured approaches and clear methodologies. The shared responsibility model that underpins cloud security creates both opportunities and complexities for organizations seeking to establish justified confidence in their security posture.

International standards like the ISO/IEC 27000 family establish common terminology, define comprehensive control sets, and enable independent validation of security claims which are key components for managing security across supply chains and cloud environments. These standards, when combined with cloud-specific frameworks like the CSA STAR program and Cloud Controls Matrix, create a powerful foundation for effective security assurance throughout the whole supply chain.

In the same line, based on what have been analysed in ptrvious sections, ISO 15026 methodology, with its structured approach to claims, arguments, and evidence offers a particularly valuable framework for building comprehensive assurance cases in complex cloud environments. By clearly defining what needs to be assured, establishing logical arguments that account for shared responsibilities, and identifying appropriate evidence sources based on audit pass-through principles and practices, organizations can develop justified confidence in their cloud-based supply chains despite inherent visibility limitations and complex relationships.

Effective assurance in cloud supply chains requires a strategic approach that balances standardization with organizational requirements, leverages certifications while addressing their limitations, and continuously improves based on experience and emerging threats. By implementing risk-based, continuous, and evidence-based assurance approaches, organizations can establish justified confidence in their cloud-based supply chains despite the inherent challenges of limited visibility, shared responsibilities, and complex relationships.

The future of assurance will be increasingly automated, collaborative, and integrated into organizational processes, enabling more comprehensive and efficient validation of security controls across complex digital ecosystems. Organizations that embrace these emerging approaches will be better positioned to manage security risks in their increasingly cloud-based supply chains.

By focusing on assurance throughout the security lifecycle, organizations can move beyond simply implementing security controls to establishing justified confidence that these controls actually work as intended. This shift from security implementation to assurance validation represents a maturation in organizational security posture, enabling more robust risk management, more effective governance, and ultimately, greater resilience against evolving threats.

7.1 The strategic value of assurance for suppply chains

Supply chain assurance provides several strategic benefits to organizations and their ecosystems:

1. Trust building: Assurance activities demonstrate to stakeholders that security and reliability claims across the supply chain are valid and evidence-backed, fostering trust in both the organization and its partners. This is critical for maintaining customer confidence and business relationships in interconnected environments.
2. Risk management: By validating security controls and processes not just internally but also among suppliers and vendors, assurance helps organizations understand their true end-to-end risk exposure. This moves beyond assumed security postures to verified resilience across the entire supply chain.
3. Compliance demonstration: Supply chain assurance provides auditable evidence to meet regulatory requirements (e.g., cybersecurity directives, trade compliance) and contractual obligations with partners, ensuring alignment with industry standards and legal frameworks.
4. Decision support: Assurance insights enable executives and boards to make informed decisions about supplier relationships, risk acceptance thresholds, and investments in supply chain security, balancing operational efficiency with resilience.
5. Continuous improvement: By identifying gaps in both internal and external security controls, assurance drives iterative enhancements across the supply chain, elevating collective security postures through shared standards and collaborative remediation.

7.2 Supply chain security assurance challenges

Modern supply chains have evolved from linear relationships into complex, multi-dimensional networks and systems. Organizations no longer engage with just direct suppliers but must consider an extensive ecosystem of partners, service providers, and sub-contractors. This complexity is particularly evident in information and communication technology (ICT) supply chains, where hardware components, software elements, and cloud services convergeCybersecurity and Infrastructure Security Agency, 2020.

The digital transformation of supply chains has accelerated this complexity. As organizations integrate cloud services, Internet of Things (IoT) devices, and automated systems into their operations, the attack surface expands dramatically. Each connection point, API integration, and data exchange represents a potential vulnerability that adversaries can exploit. The challenge lies not merely in securing individual components but in ensuring the security of the entire interconnected ecosystem.

7.2.1 Third-party and fourth-party risk management

Organizations increasingly rely on third-party vendors for critical services and components. However, these vendors introduce significant security risks that must be managed effectively. The challenge extends beyond direct suppliers to include fourth-party risks, the suppliers of your suppliers, creating a cascading effect of potential vulnerabilities.

Cloud service providers represent a particularly significant category of third-party risk. When organizations migrate data and applications to cloud environments, they must trust that these providers implement appropriate and effective security controls. However, visibility into these controls is often limited, and organizations may struggle to verify that their security requirements are being met consistently.

The challenge is compounded by the fact that many cloud providers themselves rely on other service providers, creating complex chains of dependencies. For example, a Software as a Service (SaaS) provider might build their offering on a Platform as a Service (PaaS) infrastructure, which in turn runs on Infrastructure as a Service (IaaS) components from yet another provider. Each layer introduces additional risks that must be identified, assessed, and mitigated, as well as new highly challenging assurance issues.

7.2.2 Visibility and transparency challenges

One of the most significant challenges in supply chain security assurance is achieving adequate visibility into the security practices of suppliers, particularly cloud service providers. Traditional security assessments often rely on point-in-time evaluations that provide limited insight into ongoing security operations. Cloud environments, with their abstracted infrastructure and shared responsibility models, further complicate visibility efforts.

Organizations struggle to answer fundamental questions about their supply chains: How good are provider's risk management processes and practices? Where is our data really stored? Who has access to it? What security controls are in place? How are vulnerabilities managed? These challenges are particularly acute in cloud environments, where the physical infrastructure is entirely managed by the provider and customers have limited visibility into underlying systems.

Transparency is further complicated by proprietary technologies and competitive concerns. Cloud providers may be reluctant to share detailed information about their security architecture, considering it sensitive intellectual property. This creates an information asymmetry where customers must make security decisions with incomplete information.

7.2.3 Regulatory compliance across jurisdictions

Supply chains, particularly those leveraging cloud services, frequently span multiple jurisdictions with varying regulatory requirements. Organizations must navigate a complex landscape of data protection laws, sector-specific regulations, and national security requirements that may impose conflicting obligations.

Cloud services present particular challenges in this regard. Data may flow across national boundaries, be processed in multiple locations, or be subject to different legal regimes depending on where the provider is headquartered. This creates significant complexity in determining which regulations apply and how compliance should be demonstrated.

7.2.4 Challenges of continuous assurance in dynamic environments

Traditional, periodic assurance is increasingly insufficient in dynamic environments where threats evolve rapidly and systems change continuously. This is particularly true for cloud-based supply chains, where infrastructure changes, automatic updates, and continuous deployment practices create a constantly shifting security landscape.

Organizations face several challenges in implementing continuous assurance:

- The volume and velocity of changes in modern supply chains overwhelm traditional assessment approaches.
- Point-in-time certifications and audits quickly become outdated in rapidly evolving environments.
- Manual assurance processes cannot scale to address the complexity of modern supply chains.
- Traditional documentation-based approaches may not reflect actual operational security.
- The shared responsibility model in cloud environments creates ambiguity about assurance responsibilities.

Continuous assurance requires a fundamental shift from periodic assessments to ongoing monitoring, automated validation, and real-time risk assessment. This approach demands new tools, processes, and skills that many organizations have not yet developed.

7.3 International infromation security standards for supply chain assurance

Information security standards provide essential frameworks for establishing, implementing, and validating security controls across supply chains and cloud environments. The ISO/IEC 27000 family of standards offers comprehensive guidance for managing information security risks, with specific standards addressing the unique challenges of supply chains and cloud services.

7.3.1 ISO/IEC 27001 and its role in supply chain security

The ISO/IEC 27001 ISO/IEC, 2022 standard is particularly valuable, yet uniquely challenging, in supply chain contexts because it:

- Establishes a comprehensive framework for security governance that must be consistently applied across multiple organizations, each with varying security postures and maturity levels, creating alignment challenges in multi-tiered supply chains.
- Implements a risk-based approach that must account for not just internal risks, but also inherited risks from suppliers, third-party vendors, and service providers, requiring visibility into external security practices.
- Provides a certification mechanism that enables independent validation of security claims—though supplier certifications alone cannot guarantee end-to-end supply chain resilience due to gaps in scope or implementation.
- Creates a common language for security that helps bridge communication gaps between organizations, yet struggles with inconsistencies in how controls are interpreted or enforced across different suppliers and regions.
- Facilitates regulatory compliance across jurisdictions, but must contend with conflicting or overlapping requirements when operating in global supply chains with disparate legal frameworks.

Organizations that implement ISO/IEC 27001 for supply chain assurance must extend their structured risk management approach to include:

- Supplier risk assessments to evaluate external partners' security postures,
- Contractual security requirements that enforce control alignment with ISO 27001,
- Continuous monitoring of supplier compliance and control effectiveness, and
- Collaborative improvement initiatives to elevate security standards across the entire supply chain ecosystem.

In supply chain contexts, ISO/IEC 27001 certification serves as a baseline assurance mechanism that demonstrates a supplier's commitment to information security. By requiring ISO/IEC 27001 certification from suppliers, organizations can establish a minimum level of security assurance without conducting comprehensive assessments of each supplier's security practices.

7.3.2 ISO/IEC 27002 for supply chain security

ISO/IEC 27002 International Organization for Standardization, 2022 provides a comprehensive catalog of security controls, with Control 5.21 specifically addressing the management of information security in the ICT supply chain. This control focuses on establishing and maintaining security throughout the supply of products and services, covering both hardware and software components, including cloud-based solutions.

Control 5.21 is classified as preventative in nature, aiming to maintain risk at acceptable levels by establishing agreed security standards between organizations and their suppliers. It addresses all three primary information security properties: confidentiality, integrity, and availability.

Key requirements of Control 5.21 include:

1. Establishing clear information security standards that apply to the organization's specific needs, setting expectations for supplier conduct when delivering ICT products and services.
2. Ensuring that suppliers disseminate security requirements to any third-party vendors they use when acquiring components.
3. Obtaining information about the nature and function of software components used to deliver services.
4. Implementing procedures to ensure delivered products and services are secure and compliant with accepted industry standards.
5. Identifying and recording essential components that maintain core functionality, especially those originating from subcontractors.
6. Requiring suppliers to provide assurances that critical components benefit from thorough audit logs tracing their movement throughout the supply chain.
7. Seeking categorical assurance that products and services operate within scope and do not contain additional features that may present security risks.
8. Confirming that ICT products align with industry-standard and sector-specific security requirements through formal security certification.

These requirements establish a comprehensive framework for managing security throughout the ICT supply chain, addressing both technical and procedural aspects of security assurance. By implementing these requirements, organizations can establish justified confidence in the security of products and services provided by their suppliers.

7.4 Cloud services in the supply chain

Cloud services have become integral components of modern supply chains, introducing both opportunities and challenges for security assurance. The integration of cloud services into supply chains represents a significant evolution in how organizations manage their information technology resources and business processes.

7.4.1 Types of cloud services

Cloud services in supply chains typically fall into three primary categories, each with distinct security implications and assurance requirements:

Software as a service (SaaS)

SaaS applications provide specific supply chain functionality without requiring organizations to manage the underlying infrastructure or application platform. Common supply chain SaaS applications include:

- Supplier relationship management systems.
- Procurement platforms.
- Logistics and transportation management.

- Inventory and warehouse management.
- Supply chain analytics and visibility platforms.

From a security perspective, SaaS applications shift most technical security responsibilities to the provider while leaving data governance, user access management, and configuration security with the customer. This model simplifies security management but reduces visibility and control, creating assurance challenges.

Platform as a service (PaaS)

PaaS environments provide development and runtime platforms for custom supply chain applications. Organizations use PaaS to develop specialized supply chain capabilities while avoiding the complexity of managing the underlying infrastructure.

Common PaaS use cases in supply chains include:

- Development of custom supplier portals.
- Creation of specialized integration platforms.
- Implementation of industry-specific supply chain processes.
- Development of analytics and reporting capabilities.
- Creation of mobile applications for supply chain participants.

PaaS environments create a shared security model where the provider secures the platform while the customer remains responsible for application security, data protection, and access controls. This division requires clear understanding of security boundaries and responsibilities.

Infrastructure as a service (IaaS)

IaaS provides virtualized computing resources that organizations use to build and operate supply chain systems. This model offers the greatest control but also places the most security responsibility on the customer.

Common IaaS use cases in supply chains include:

- Hosting legacy supply chain applications that cannot be migrated to SaaS.
- Implementing specialized supply chain systems with unique requirements.
- Creating development and testing environments for supply chain applications.
- Establishing disaster recovery capabilities for critical supply chain systems.
- Implementing data lakes and analytics platforms for supply chain intelligence.

IaaS environments require organizations to implement comprehensive security controls across the technology stack, from network security to application protection. This model provides the greatest control but also demands the most security expertise and resources.

7.4.2 Unique security considerations for cloud-based supply chains

Cloud-based supply chains present unique security considerations that differ from traditional on-premises environments. These considerations must be addressed through specialized approaches and controls.

Distributed data and processing

Cloud environments distribute data and processing across multiple locations, often spanning geographic and jurisdictional boundaries. This distribution creates several security and assurance challenges:

- Data sovereignty and compliance with location-specific regulations.
- Consistency of security controls across distributed environments.
- Secure data transfer between distributed components.
- Visibility into data location and processing activities.
- Coordination of security incident response across distributed systems.

Addressing these challenges requires clear understanding of data flows, jurisdictional requirements, and security controls implemented at each location where supply chain data is stored or processed.

Multi-tenancy and resource sharing

Cloud environments typically implement multi-tenant architectures where multiple customers share underlying infrastructure. This resource sharing introduces potential security and assurance concerns:

- Isolation between tenants to prevent unauthorized access.
- Resource contention that could impact availability.
- Side-channel attacks that exploit shared resources.
- Potential for configuration errors that expose data.
- Commingling of data in shared storage or processing systems.

Effective security in multi-tenant environments requires strong isolation mechanisms, careful configuration management, and monitoring for potential isolation failures or unauthorized access attempts.

Dynamic provisioning and scaling

Cloud environments enable dynamic provisioning and scaling of resources, allowing supply chain systems to adapt to changing requirements. This dynamism introduces security and assurance considerations:

- Maintaining security configurations as environments scale.
- Ensuring new resources are properly secured before use.
- Preventing unauthorized resource provisioning.
- Securing temporary resources that may be created and destroyed rapidly.
- Maintaining visibility into dynamically changing environments.

Addressing these considerations requires automated security controls that can adapt to changing environments, continuous monitoring for security issues, and processes that ensure security and assurance is maintained throughout resource lifecycle.

7.5 The shared responsibility model for cloud security

The shared responsibility model is a fundamental concept in cloud security that defines how security responsibilities are divided between cloud service providers and their customers Microsoft, 2023. This model is particularly relevant to supply chain security assurance, as it clarifies security boundaries and expectations across complex, multi-party relationships.

7.5.1 Fundamentals of the shared responsibility model

The shared responsibility model establishes a framework for dividing security responsibilities between cloud service providers and their customers. This division varies based on the service model (IaaS, PaaS, SaaS) and specific provider implementations, but generally follows consistent patterns.

At its core, the shared responsibility model recognizes that effective cloud security requires collaboration between providers and customers, with each party taking responsibility for different aspects of the security posture. This collaborative approach acknowledges that neither party can independently secure the entire environment.

Key principles of the shared responsibility model include:

1. Cloud providers are responsible for securing the underlying infrastructure and services they provide.
2. Customers are responsible for securing their data, applications, and configurations within the cloud environment.
3. Responsibilities shift based on the service model, with customers assuming more responsibility in IaaS environments and less in SaaS environments.
4. Some responsibilities are always retained by the customer, regardless of service model.
5. Some responsibilities are always retained by the provider, regardless of service model.
6. Many responsibilities are shared, requiring coordination between provider and customer.

Understanding these principles is essential for establishing effective security assurance in cloud-based supply chains, as they define the boundaries of responsibility and the areas where coordination is required.

7.5.2 Responsibility distribution across service models

The distribution of security responsibilities varies significantly across different cloud service models, with important implications for supply chain security assurance.

Infrastructure as a service (IaaS)

In IaaS environments, the provider typically assumes responsibility for:

- Physical security of data centers.
- Security of the underlying hardware infrastructure.
- Hypervisor security and isolation between virtual machines.

- Network infrastructure security.
- Storage infrastructure security.
- Availability of the infrastructure services.

Customers retain responsibility for:

- Operating system security, including patching and configuration.
- Network configuration and security.
- Identity and access management.
- Data classification and protection.
- Application security.
- Client and endpoint security.

This model places significant security responsibility on the customer, requiring comprehensive security programs that address all layers above the hypervisor. Organizations must implement controls for operating system security, network security, application security, and data protection. While more challenging from a security perspective, assurance in the context of SaaS is easier to achieve due to the existing visibility, transparency, and control over most of system's components.

Platform as a service (PaaS)

In PaaS environments, the provider assumes additional responsibilities:

- Operating system security and patching.
- Runtime environment security.
- Middleware security.
- Development tools security.
- Basic network security.

Customers retain responsibility for:

- Application security.
- Identity and access management.
- Data classification and protection.
- Client and endpoint security.
- Custom configurations of platform services.

This model reduces the customer's security burden compared to IaaS, but still requires significant attention to application security, data protection, and identity management. Organizations must focus on securing their applications and data while leveraging the security capabilities provided by the platform.

Software as a service (SaaS)

In SaaS environments, the provider assumes the most extensive responsibilities:

- Application security.
- Infrastructure security.
- Operating system security.
- Network security.
- Physical security.
- Availability and performance.

Customers retain responsibility for:

- Data classification and protection.
- User access management.
- Endpoint security.
- Secure use of the application.
- Configuration of available security controls.

This model significantly reduces the customer's security burden, focusing primarily on data governance, access management, and secure usage. However, it also reduces the customer's transparency, visibility, and control creating challenges for comprehensive security assurance.

7.5.3 Customer retained responsibilities

Regardless of the service model, certain security responsibilities are always retained by the customer. These responsibilities are particularly important in supply chain contexts, as they represent areas where organizations cannot transfer risk to their cloud providers.

Customers always retain responsibility for:

- Data classification and categorization.
- Defining data protection requirements based on sensitivity.
- Implementing appropriate data protection controls.
- Managing data lifecycle from creation to deletion.
- Ensuring compliance with data protection regulations.

These responsibilities require organizations to maintain comprehensive data governance programs that extend into cloud environments. This includes implementing appropriate encryption, access controls, and data lifecycle management processes.

On top of the presented data-centric responsibilities, customers also always retain responsibility for identity and access management:

- User identity management.
- Authentication and authorization policies.
- Privilege management and separation of duties.

- Access reviews and monitoring.
- Integration with enterprise identity systems.

These responsibilities require organizations to implement comprehensive identity and access management programs that extend into cloud environments. This includes establishing appropriate authentication mechanisms, implementing least privilege principles, and regularly reviewing access rights.

7.6 International standards for cloud security and privacy

7.6.1 ISO/IEC 27017 for cloud security

ISO/IEC 27017 International Organization for Standardization, 2015 extends the ISO/IEC 27002 control set with cloud-specific guidance and additional controls designed specifically for cloud environments. This standard is particularly important for cloud-based supply chains, as it addresses the unique security considerations of cloud services and strengthen assurance programs by bringing more control over well-known supply chain security challenges.

Key aspects of ISO 27017 relevant to supply chain assurance include:

Shared responsibilities guidance

ISO/IEC 27017 provides detailed guidance on establishing and documenting shared responsibilities between cloud service providers and customers, while ISO/IEC 27036-3 extends this to supply chain contexts. This guidance is particularly important in multi-party environments where coordinated security and assurance activities are critical.

The standard clarifies:

1. Responsibility allocation for security control implementation.
2. Evidence requirements for control validation and assurance.
3. Ongoing monitoring obligations for continuous assurance.

This structured approach helps organizations to understand their security management obligations, verify provider-controlled security measures through documented evidence, and maintain comprehensive security coverage with auditable assurance.

The clarity enables organizations to establish both security implementation and assurance verification without gaps or redundancies across the supply chain.

Asset management in cloud environments

ISO 27017 addresses the management of assets in cloud environments, including responsibilities for asset inventory, ownership, and acceptable use. These controls help organizations maintain visibility into their cloud-based supply chain assets and ensure appropriate protection.

The standard provides guidance on managing both customer-provided assets and provider-supplied assets, addressing the complex asset relationships that exist in cloud-based supply chains.

Access management

ISO/IEC 27017 provides cloud-specific guidance on access management, addressing the unique challenges of controlling and assuring access in distributed, multi-tenant environments. These controls and their verification mechanisms are particularly critical in supply chain contexts where multiple parties require demonstrable security across shared systems and data.

The standard addresses:

1. Privileged access management with requirements for activity logging and audit trails.
2. User provisioning/deprovisioning processes and their assurance through documented evidence.
3. Access review procedures with validation requirements for cloud services.
4. Implementation of authentication mechanisms with corresponding verification methods.

For assurance purposes, the standard also specifies evidence requirements for access control effectiveness, shared responsibility models for access verification, and monitoring obligations to maintain ongoing assurance.

This comprehensive approach ensures access management controls are not only implemented but also continuously validated across cloud supply chain environments.

Cryptography and data protection

ISO/IEC 27017 provides comprehensive guidance on implementing and verifying cryptographic controls in cloud environments, addressing:

1. Key management with audit requirements.
2. Encryption of data at rest and in transit with validation methods.
3. Cryptographic architecture with evidence requirements.

These controls and their assurance mechanisms are essential for both protecting and demonstrating the security of sensitive supply chain data in cloud environments.

The standard clearly defines:

- Implementation responsibilities for cryptographic controls.
- Verification obligations for cryptographic protection.
- Evidence requirements for key management processes.

This enables organizations to understand their cryptographic security obligations, validate provider-managed encryption through documented proofs, and maintain end-to-end cryptographic assurance across cloud supply chains. The guidance ensures cryptographic protections are not just implemented but also continuously verifiable, with unambiguous accountability for both security implementation and assurance validation.

Operations security

ISO/IEC 27017 provides comprehensive guidance on operational security in cloud environments, addressing change management, capacity management, malware protection, and backup processes, including their associated assurance requirements.

These controls and verification mechanisms help ensure both the ongoing security and demonstrable reliability of cloud-based supply chain systems.

The standard clarifies:

1. Operational responsibilities between providers and customers.
2. Evidence requirements for validating control effectiveness.
3. Monitoring obligations for continuous assurance.

This framework enables organizations to understand their operational security obligations, verify provider-managed controls through documented evidence, and maintain comprehensive operational assurance across the cloud supply chain. The guidance ensures operational security measures are not only implemented but also objectively verified, with clear accountability for both implementation and assurance activities.

7.6.2 ISO/IEC 27018 for cloud privacy

ISO/IEC 27018 International Organization for Standardization, 2019 provides specific guidance on protecting personally identifiable information (PII) in cloud environments. This standard is particularly relevant to supply chains that process personal data, such as customer information, employee data, or supplier contact details.

Key aspects of ISO 27018 relevant to supply chain assurance include:

Consent and choice

ISO/IEC 27018 provides comprehensive guidance on obtaining, managing, and verifying consent for processing personal data in cloud environments. These controls and their validation mechanisms help organizations both implement and demonstrate that personal data processing across their supply chains complies with privacy regulations and respects individual rights.

The standard specifically addresses:

1. Consent mechanisms with audit requirements.
2. Consent decision recording with evidence preservation.
3. Consent modification/withdrawal processes with verification methods.
4. Personal data handling procedures when direct consent isn't obtainable.

For privacy assurance, the standard also defines:

- Documentation requirements for consent management.
- Verification obligations for consent compliance.
- Monitoring processes for ongoing privacy assurance.

This framework enables organizations to meet their consent management obligations, validate cloud provider compliance through documented evidence, and maintain continuous privacy assurance throughout cloud supply chains.

The guidance ensures consent processes are not only properly implemented but also objectively verifiable, with clear accountability for both privacy protection and assurance demonstration.

Purpose legitimacy and specification

ISO/IEC 27018 addresses the requirement that personal data be collected for specified, explicit, and legitimate purposes, including mechanisms to verify compliance with these principles. These controls and their validation processes help organizations ensure and demonstrate that personal data processing throughout their supply chains adheres to appropriate purposes and privacy regulations.

The standard provides comprehensive guidance on:

1. Documenting processing purposes with audit requirements.
2. Aligning processing activities with documented purposes through verification methods.
3. Managing purpose changes with evidence preservation.
4. Addressing purpose specification challenges in multi-party supply chain environments.

For privacy assurance, the standard establishes:

1. Evidence requirements for purpose compliance.
2. Monitoring obligations for ongoing purpose validation.
3. Accountability frameworks for all processing parties.

This enables organizations to fulfill their purpose limitation obligations, validate supply chain partner compliance through documented proofs, and maintain continuous assurance of lawful processing purposes.

The guidance ensures purpose limitation principles are not only properly implemented but also objectively verifiable across complex cloud supply chains, with clear mechanisms to demonstrate compliance to regulators and data subjects.

Data minimization

ISO/IEC 27018 includes controls and verification mechanisms for data minimization, ensuring that personal data processing is properly limited to what is necessary for specified purposes and that this limitation can be objectively demonstrated. These controls help organizations both implement and validate appropriate data collection and processing practices throughout their supply chains.

The standard provides comprehensive guidance on:

1. Identifying minimum necessary data sets with audit requirements.
2. Implementing and verifying collection/processing limitations.
3. Regular data holding reviews with evidence preservation.

4. Documentation standards for minimization compliance.

For privacy assurance, the standard establishes:

- Evidence requirements demonstrating minimization practices.
- Validation processes for ongoing compliance.
- Accountability measures across supply chain partners.

This enables organizations to meet data minimization obligations, verify partner compliance through documented proofs, and maintain continuous assurance of minimization practices.

The guidance ensures data minimization principles are not only properly implemented but also objectively verifiable, reducing both privacy risks and compliance burdens while building trust across the supply chain ecosystem.

Transparency and individual rights

ISO/IEC 27018 addresses requirements for openness, transparency, and notice regarding personal data processing in cloud environments, including mechanisms to verify and demonstrate compliance. These controls help organizations both implement and validate appropriate information disclosure practices throughout their supply chain systems.

The standard provides specific guidance on:

1. Transparency mechanisms with audit requirements.
2. Notice requirements with verification methods.
3. Documentation standards for processing disclosures.
4. Evidence preservation for regulatory compliance.

For individual rights assurance, the standard includes:

- Access control implementation with validation processes.
- Rights fulfillment procedures with audit trails.
- Monitoring systems for continuous compliance.

This enables organizations to meet transparency obligations with verifiable proofs, validate individual rights fulfillment through documented evidence, and maintain ongoing assurance of privacy rights compliance.

The guidance ensures transparency and rights mechanisms are not only properly implemented but also objectively demonstrable, building trust with individuals and regulators across complex cloud supply chain environments.

7.7 The Cloud Security Alliance in security assurance

The Cloud Security Alliance (CSA) is a nonprofit organization dedicated to promoting best practices for providing security assurance within cloud computing environments. The CSA plays a crucial role in establishing standardized approaches to cloud security assessment and assurance, offering frameworks and certifications that help organizations validate the security of cloud services.

7.7.1 The CSA Security Trust Assurance and Risk program

The CSA Security Trust Assurance and Risk (STAR) program is a comprehensive security assurance framework specifically designed for cloud service providers. This program offers several levels of assurance through self-assessment, third-party audit, and continuous monitoring.

CSA STAR self-assessment

The self-assessment level of the STAR program allows cloud providers to document their security controls by completing the Consensus Assessments Initiative Questionnaire (CAIQ) or submitting a Cloud Controls Matrix (CCM) Cloud Security Alliance, 2020 report. These self-assessments are published in the CSA STAR Registry, providing transparency to potential customers.

Key benefits of the self-assessment include:

- Standardized documentation of security controls.
- Increased transparency about security practices.
- Baseline for comparing security capabilities across providers.
- Simplified initial assessment for potential customers.
- Foundation for more rigorous assurance activities.

While self-assessment provides valuable transparency, it offers limited assurance since the information is not validated by independent third parties.

CSA STAR certification and attestation

The STAR certification and attestation levels provide independent validation of cloud provider security controls. These assessments are conducted by third-party auditors and provide significantly stronger assurance than self-assessments.

The STAR attestation is based on SOC 2 criteria combined with the CSA Cloud Controls Matrix, providing a comprehensive assessment of security, availability, processing integrity, confidentiality, and privacy controls.

The STAR certification is based on ISO/IEC 27001 combined with the CSA Cloud Controls Matrix, providing a rigorous assessment of information security management systems with cloud-specific controls.

Key benefits of certification and attestation include:

- Independent validation of security claims.
- Comprehensive assessment against established criteria.
- Detailed reporting on control implementation and effectiveness.
- Regular reassessment to ensure ongoing compliance.
- Strong assurance suitable for high-risk environments.

These third-party validations provide the level of assurance needed for critical applications and sensitive data in cloud environments.

7.7.2 The Cloud Controls Matrix (CCM)

The Cloud Controls Matrix is a cybersecurity control framework specifically designed for cloud computing. The CCM provides a detailed set of controls that align with major standards and regulations, including ISO/IEC 27001, NIST SP 800-53, PCI DSS, and GDPR.

Key features of the CCM include:

1. Comprehensive control coverage: The CCM includes controls across 17 domains, ensuring that all relevant aspects of cloud security are addressed in assessments.
2. Mapping to major standards and regulations: The CCM provides detailed mappings between its controls and major standards and regulations. These mappings help organizations understand how CCM controls relate to their compliance requirements and how they can leverage CCM assessments to support multiple compliance objectives.
3. Cloud-specific control guidance: The CCM provides detailed implementation guidance specifically designed for cloud environments. This guidance addresses the unique security considerations of cloud services, including shared responsibilities, multi-tenancy, and dynamic provisioning.

7.7.3 Leveraging CSA for supply chain assurance

Organizations can leverage CSA frameworks and certifications to enhance supply chain assurance in several ways:

Requiring CSA STAR certification from cloud providers

Organizations can include CSA STAR certification requirements in their supplier security requirements. This approach:

- Establishes a baseline security expectation for cloud providers.
- Leverages independent validation of security controls.
- Provides standardized evidence for security assessment.
- Reduces the need for custom security assessments.
- Facilitates comparison across potential providers.

By requiring CSA STAR certification, organizations can establish justified confidence in their cloud providers' security capabilities without conducting comprehensive assessments of each provider.

Using the CCM for security requirements definition

Organizations can use the Cloud Controls Matrix to define security requirements for cloud providers. This approach:

- Ensures comprehensive coverage of security considerations.
- Leverages cloud-specific control definitions.

- Aligns with major standards and regulations.
- Provides clear, measurable security expectations.
- Facilitates consistent evaluation across providers.

By basing security requirements on the CCM, organizations can ensure that their cloud providers implement appropriate security controls that address cloud-specific risks.

7.8 Building effective assurance programs for cloud supply chains

This section explores key principles and approaches for building effective assurance programs that address these challenges.

7.8.1 Key principles for effective assurance

Effective assurance programs for cloud supply chains are built on several fundamental principles:

Risk-based approach

Assurance activities should be prioritized based on risk, focusing resources on the most critical systems, data, and relationships. This approach ensures that assurance efforts provide the greatest value in terms of risk reduction.

Key aspects of a risk-based approach include:

- Identifying and classifying critical assets and processes.
- Assessing the potential impact of security failures.
- Evaluating the likelihood of different threat scenarios.
- Prioritizing assurance activities based on risk levels.
- Adjusting assurance intensity based on risk factors.

By adopting a risk-based approach, organizations can allocate limited assurance resources more effectively, focusing on areas where assurance provides the greatest risk reduction.

Continuous validation

Traditional point-in-time assessments are increasingly insufficient in dynamic cloud environments. Effective assurance programs implement continuous validation approaches that provide ongoing visibility into security posture.

Key aspects of continuous validation include:

- Automated compliance monitoring.
- Continuous control validation.
- Real-time security monitoring.
- Regular reassessment of critical controls.
- Ongoing validation of security configurations.

These continuous approaches reduce the gap between security reality and assurance evidence, providing more timely and accurate insights into security posture.

Shared responsibility clarity

Effective assurance programs establish clear understanding of security responsibilities across all parties in the supply chain. This clarity is essential for comprehensive security coverage without gaps or unnecessary duplication.

Key aspects of shared responsibility clarity include:

- Documented responsibility matrices.
- Clear security requirements for each party.
- Defined coordination mechanisms.
- Regular validation of responsibility fulfillment.
- Processes for addressing responsibility gaps.

By establishing clear responsibility boundaries, organizations can implement more effective assurance activities that address the complete security landscape.

7.8.2 Leveraging certifications while addressing gaps

Certifications and audit reports provide valuable assurance evidence, but they often have limitations that must be addressed through supplemental activities.

Understanding certification scope and limitations

Organizations should develop a clear understanding of what certifications do and do not cover. Key considerations include:

- Control scope included in the certification.
- Specific systems and services covered.
- Testing methodologies used.
- Frequency and depth of assessments.
- Limitations explicitly noted in reports.

This understanding helps organizations identify where certifications provide sufficient assurance and where additional validation is needed.

Supplementing certifications with additional assurance

Organizations should implement supplemental assurance activities to address gaps in certification coverage. These activities might include:

- Targeted security assessments for critical areas.
- Continuous monitoring of key security indicators.
- Penetration testing focused on specific concerns.
- Configuration validation for critical systems.

- Custom security requirements for unique needs.

These supplemental activities provide additional assurance for areas not fully addressed by standard certifications.

8 Assurance and public trust

The achievement of public trust as a strategic objective relies on the public's firm belief in an organization's reliability, truth, and ability. This section explores how assurance serves as a strategic enabler for public trust, examining the relationship between assurance activities and trust-building, as well as the costs and considerations involved in establishing and maintaining public trust through assurance.

8.1 Strategic value of assurance

Trust doesn't happen by accident; it must be earned and sustained through clear evidence and consistent performance. That's where assurance comes in. Assurance is how organizations prove they are doing what they say, and that they will continue to do it. Assurance turns performance into credibility, and credibility into trust.

The strategic value of assurance lies in its ability to provide stakeholders—whether they are customers, citizens, regulators, or partners—with justified confidence in an organization's security measures. This confidence is essential for building and maintaining trust, particularly in environments where security breaches can have significant consequences for privacy, safety, financial stability, or national security.

Assurance provides strategic value in several key ways:

1. **Risk-informed decision making**: Assurance activities provide insights into the effectiveness of security controls, enabling more informed risk management decisions.
2. **Regulatory compliance**: Assurance demonstrates compliance with regulatory requirements, reducing legal and compliance risks.
3. **Competitive advantage**: Strong assurance can differentiate an organization in the marketplace, particularly in industries where security is a key concern.
4. **Operational resilience**: Assurance activities identify weaknesses before they can be exploited, enhancing the organization's ability to withstand security threats.
5. **Stakeholder confidence**: Assurance builds confidence among stakeholders, from customers and partners to investors and regulators.

By recognizing the strategic value of assurance, organizations can move beyond viewing it as a compliance exercise and instead see it as a strategic enabler that supports broader business objectives.

8.2 How assurance supports trust

Trust requires several key elements, each of which is supported by effective assurance practices (Nicholson et al., 2018):

8.2.1 Reliability

Trust depends on reliability—the consistent delivery of expected outcomes. Assurance supports reliability by:

- Providing evidence that systems and processes consistently meet expected outcomes
- Identifying and addressing inconsistencies or weaknesses before they affect performance
- Ensuring that controls operate as intended across different conditions and over time
- Validating that changes to systems or processes don't compromise reliability

Through systematic validation of control effectiveness, assurance demonstrates that an organization's security measures can be relied upon to protect information assets consistently.

8.2.2 Truthfulness

Trust requires truthfulness—honest and accurate communication about capabilities, limitations, and risks. Assurance supports truthfulness by:

- Enabling transparent, objective, and verifiable reporting on performance and risks
- Providing an evidence-based foundation for claims about security posture
- Identifying gaps between stated intentions and actual implementation
- Supporting honest assessment of security strengths and weaknesses

By providing an objective basis for security claims, assurance helps organizations communicate truthfully about their security posture, avoiding both overconfidence and unnecessary alarm.

8.2.3 Ability

Trust depends on ability—the capability to deliver on commitments and meet expectations. Assurance supports ability by:

- Confirming that capabilities and controls are in place to deliver on security commitments
- Identifying capability gaps that need to be addressed
- Validating that security measures are appropriate for the threats they address
- Ensuring that resources are allocated effectively to security priorities

Through systematic evaluation of security capabilities, assurance demonstrates that an organization has the ability to protect information assets effectively.

8.2.4 Confidence

Trust ultimately requires confidence—justified belief in reliability, truthfulness, and ability. Assurance supports confidence by:

- Providing credible data, audits, monitoring, and risk management information

- Establishing a systematic basis for belief in security effectiveness
- Addressing doubts and concerns through evidence and validation
- Building a track record of effective security over time

By providing justified confidence in security measures, assurance creates the foundation for trust among stakeholders.

8.3 Transparency and communication of assurance results

The strategic value of assurance depends not only on conducting validation activities but also on effectively communicating the results to stakeholders. Transparency about assurance findings—both strengths and weaknesses—builds credibility and trust.

Effective communication of assurance results involves:

- **Tailoring messages to different stakeholders**: Different stakeholders have different information needs and levels of technical understanding. Communication should be adapted accordingly, providing appropriate detail and context for each audience.
- **Balancing transparency with security**: While transparency builds trust, organizations must balance openness with the need to protect sensitive security information that could be exploited by adversaries.
- **Contextualizing findings**: Assurance results should be presented in context, explaining their significance, the risks they represent, and the actions being taken to address any identified weaknesses.
- **Regular reporting**: Consistent, regular reporting on assurance activities and results demonstrates ongoing commitment to security and provides stakeholders with current information about the organization's security posture.
- **Demonstrating improvement**: Communication should highlight not only current findings but also progress over time, showing how the organization has addressed previous weaknesses and strengthened its security controls.

By effectively communicating assurance results, organizations can maximize the strategic value of their assurance programs and strengthen stakeholder trust.

8.4 Regulatory and compliance considerations

Regulatory requirements increasingly emphasize the importance of assurance in information security. Many regulations and standards now require organizations to validate the effectiveness of their security controls through various assurance activities.

Key regulatory and compliance considerations include:

- **Explicit assurance requirements**: Some regulations explicitly require specific assurance activities, such as penetration testing, vulnerability assessments, or independent audits.

- **Evidence preservation**: Regulations often require organizations to maintain evidence of control effectiveness, which aligns with the evidence collection aspect of assurance.
- **Independent validation**: Many regulatory frameworks emphasize the importance of independent validation of security controls, reinforcing the need for separation between security operations and assurance functions.
- **Risk-based approaches**: Regulatory frameworks increasingly adopt risk-based approaches that align with the risk-focused nature of effective assurance programs.
- **Continuous monitoring**: Some regulations now require continuous monitoring of security controls, driving the shift toward continuous assurance approaches.

Organizations should design their assurance programs to meet both their own strategic needs and applicable regulatory requirements. By aligning assurance activities with regulatory expectations, organizations can achieve compliance while also building the justified confidence that supports public trust.

The strategic implications of assurance highlight its importance beyond technical validation. By recognizing assurance as a strategic enabler that builds public trust, organizations can develop more effective approaches to security governance that balance technical, operational, and strategic considerations.

8.5 Cost considerations for public trust

Building and maintaining public trust through assurance involves significant costs that must be carefully considered and balanced against the benefits. These costs vary depending on the organization's security maturity and existing assurance capabilities.

8.5.1 Best case scenario: Strong risk management, limited assurance

Even in organizations with a relatively mature security posture, a strong enterprise risk management framework, capable staff, processes, and tools, there are still significant costs to establishing formal assurance capabilities.

Without a formal Information Security Management System (ISMS) or assurance function, organizations lack confidence in the selection, implementation, and ongoing effectiveness of their security processes and controls. Top managers may feel comfortable with the organization's security posture but recognize the need for something more—trust!

In this scenario, establishing and sustaining meaningful assurance typically requires a 25-50% increase in the existing security budget to properly design, implement, and manage assurance activities over time. This is the cost of catching up without rework—but from a strong baseline.

8.5.2 Worst case scenario: Weak risk management, limited assurance

In a low-maturity environment, organizations may not know exactly what controls are in place, who is managing risk, or whether policies are being followed. Security processes and controls may be missing, misaligned, or unverified, and decisions are made without evidence, which increases uncertainty and undermines confidence.

In this scenario, top managers often feel lost, and their lack of confidence undermines everything else. Achieving trustworthy assurance under these conditions typically requires a 50-75% increase in budget to close the risk management gaps as well as to build assurance capabilities. That's not just overhead—it's the cost of addressing uncertainty.

8.5.3 Balancing costs and benefits

When considering the costs of assurance, organizations should keep several factors in mind:

1. **Risk-based approach**: Focus assurance investments on the most critical systems and the most significant risks, ensuring that limited resources are directed where they will have the greatest impact.

2. **Incremental implementation**: Develop assurance capabilities incrementally, starting with the most critical areas and expanding over time as resources permit.

3. **Integration with existing processes**: Integrate assurance activities with existing processes where possible to reduce duplication and overhead.

4. **Automation**: Leverage automation to reduce the ongoing costs of assurance activities, particularly for evidence collection and analysis.

5. **Return on investment**: Consider the potential returns on assurance investments, including reduced risk of breaches, improved compliance, enhanced reputation, and increased stakeholder trust.

By taking a strategic approach to assurance investments, organizations can maximize the trust-building benefits while managing the associated costs effectively.

8.6 Reflecting on assurance and public trust

When reflecting on the relationship between assurance and public trust, several key considerations emerge:

1. **Assurance scope alignment with business value**: Defining assurance scope in line with business value is crucial. Not all systems and processes require the same level of assurance; focus should be on those that are most critical to the organization's mission and most important to stakeholders.

2. **Assurance as a key but often misunderstood part of security and trust**: Assurance is frequently misunderstood or overlooked in security programs, yet it is essential for establishing the justified confidence that underlies trust.

3. **Multiple approaches to assurance**: Assurance can be built into an ISMS from the ground up or developed as a complementary security domain. The approach should be tailored to the organization's structure, culture, and existing security program.

4. **The role of governance through sound policies**: Strong governance through sound policies supports assurance claims by establishing clear expectations and requirements that can be validated through assurance activities.

5. **The importance of skepticism**: Knowing the limitations of assurance cases and maintaining a healthy skepticism is key to effective assurance. Doubt plays a

crucial role in strengthening assurance by challenging assumptions and identifying weaknesses.

6. **Certification and Accreditation as part of the assurance landscape**: While Certification and Accreditation (C&A) processes like those in the NZISM are important, they are just one part of the assurance landscape. Comprehensive assurance goes beyond C&A to establish justified confidence that security processes and controls actually work as intended.

In conclusion, assurance plays a vital role in building and maintaining public trust by providing the justified confidence that security measures are effective. While establishing robust assurance capabilities involves significant costs, these investments are essential for organizations that depend on public trust for their success. By taking a strategic approach to assurance, organizations can build the credibility and confidence that underpin trusted relationships with stakeholders.

9 Challenges and limitations in assurance

While assurance provides valuable confidence in security controls, it is not without challenges and limitations. Understanding these challenges is essential for developing realistic and effective assurance programs that acknowledge the inherent constraints and complexities of security validation. This section explores common pitfalls in assurance activities, the challenge of balancing assurance with operational needs, and the fundamental limitations of assurance cases.

9.1 Common pitfalls in assurance activities

Organizations often encounter several common pitfalls when implementing assurance activities. Recognizing and addressing these pitfalls is crucial for maintaining the effectiveness and credibility of assurance programs.

9.1.1 Inadequate independence

When assurance functions lack sufficient independence, their objectivity and credibility are compromised. Common independence issues include:

- Assurance teams reporting to the same management as operational teams, creating potential conflicts of interest.
- Assurance personnel with prior involvement in control implementation, potentially biasing their evaluation.
- Budget dependencies that create pressure to report positive findings.
- Organizational pressure to report positive findings to avoid disrupting operations or projects.

To address these issues, organizations should establish clear separation between operational and assurance functions, ensure that assurance teams report to independent management, and provide dedicated resources for assurance activities.

9.1.2 Confirmation bias

Security professionals may unconsciously seek evidence that confirms their existing beliefs about control effectiveness rather than critically evaluating all available evidence. This confirmation bias can lead to overly optimistic assessments of security controls and missed opportunities for improvement.

To mitigate confirmation bias, organizations should:

- Encourage skepticism and critical thinking in assurance activities.
- Involve diverse perspectives in the evaluation of evidence.
- Establish clear criteria for evidence evaluation to reduce subjective judgment.
- Regularly rotate assurance personnel to bring fresh perspectives.

9.1.3 Siloed approaches

When assurance activities operate in silos, organizations miss opportunities for efficiency and comprehensive coverage. Siloed approaches can lead to:

- Duplicative testing efforts that waste resources and burden operational teams.
- Inconsistent methodologies and standards that produce conflicting results.
- Gaps in coverage where critical controls are not adequately evaluated.
- Contradictory findings that undermine confidence in assurance results.
- Excessive burden on operational teams responding to multiple, uncoordinated assurance activities.

To address these issues, organizations should establish integrated assurance programs that coordinate activities across different assurance functions, standardize methodologies and criteria, and ensure comprehensive coverage of security controls.

9.1.4 Evidence quality issues

Assurance activities are only as good as the evidence they examine. Common evidence quality issues include:

- Incomplete or fragmented evidence that provides only partial visibility into control effectiveness.
- Outdated information that doesn't reflect current configurations or practices.
- Lack of corroboration across multiple sources, reducing confidence in the evidence.
- Insufficient sample sizes for testing, limiting the statistical validity of results.
- Reliance on self-reported information without independent verification.

To address these issues, organizations should establish standards for evidence quality, including requirements for relevance, reliability, sufficiency, and currency. They should also implement processes for collecting, validating, and preserving evidence to ensure its integrity and usefulness for assurance activities.

9.2 Balancing assurance with operational needs

One of the most significant challenges in information security assurance is balancing the need for thorough validation with the operational realities of the organization. Too much assurance activity can disrupt operations and create resistance, while too little risks undetected weaknesses and false confidence.

To achieve an appropriate balance, organizations should consider several strategies:

- **Focus on risk**: Prioritize assurance activities based on risk assessment, focusing resources on high-risk areas and critical systems. This risk-based approach ensures that assurance efforts are proportionate to the potential impact of control failures.
- **Plan together**: Coordinate assurance efforts across different functions to reduce overlap and minimize operational impact. This coordination can include consolidating tests, coordinating evidence collection, and aligning schedules to reduce disruption.
- **Automate**: Use tools and technologies to increase coverage and enable continuous assessment without increasing operational burden. Automation can reduce the manual effort required for assurance activities and provide more consistent and timely results.

By adopting these strategies, organizations can develop assurance programs that provide adequate confidence in security controls without imposing excessive burden on operational teams or disrupting business activities.

9.3 Limitations of assurance cases

While assurance cases provide a structured approach to building justified confidence in security controls, they have inherent limitations that must be acknowledged. Understanding these limitations helps organizations develop realistic expectations about what assurance can and cannot achieve.

9.3.1 Not absolute guarantees

Assurance cases help build justified confidence in security, but they do not provide absolute guarantees. They explain design decisions and validate control effectiveness, but they cannot certify that a system is completely secure or immune to all possible attacks. Security is inherently probabilistic, and assurance cases reflect this reality by providing reasoned arguments rather than absolute certainty.

9.3.2 Evidence constraints

Assurance cases rely on known information and available evidence. They cannot account for unknown or emerging threats that have not yet been identified or for which evidence is not available. This limitation is particularly significant in the rapidly evolving landscape of information security, where new threats and vulnerabilities emerge regularly.

9.3.3 Resource limitations

The depth and comprehensiveness of assurance cases depend on available time, people, and funding. Resource constraints may limit the scope of assurance activities, the thoroughness of evidence collection, or the rigor of argument evaluation. Organizations must make pragmatic decisions about how to allocate limited resources to assurance activities, potentially leaving some areas with less thorough validation.

9.3.4 Implementation sensitivity

Even well-planned assurance cases can be weakened by poor execution. If evidence collection is flawed, arguments are not rigorously evaluated, or findings are not properly documented, the assurance case may not provide the intended level of confidence. The effectiveness of assurance cases depends not only on their design but also on the quality of their implementation.

9.3.5 Temporal limitations

Assurance cases represent a snapshot in time in a constantly changing threat landscape. They reflect the state of the system and the available evidence at a specific point, but they may not remain valid as systems evolve, threats change, or new vulnerabilities are discovered. This temporal limitation underscores the need for regular review and update of assurance cases to maintain their relevance and validity.

Despite these limitations, assurance cases remain a valuable tool for building justified confidence in security controls. They support informed risk decisions—not certainty—aligning with the reality that security manages, not eliminates, risk. By acknowledging these limitations, organizations can develop more realistic and effective approaches to assurance that recognize the inherent uncertainties and constraints of security validation.

10 Emerging trends in information security assurance

The field of information security assurance is evolving rapidly in response to changing technology landscapes, development methodologies, and threat environments. This section explores emerging trends in assurance, including the shift toward continuous assurance, the integration of assurance with modern development methodologies, and future directions for assurance research and practice.

10.1 Continuous assurance

Traditional, periodic assurance is increasingly insufficient in dynamic environments where threats evolve rapidly and systems change continuously. In response, organizations are moving toward continuous assurance approaches that provide near-real-time validation of control effectiveness.

10.1.1 Shift from periodic to ongoing validation

Continuous assurance represents a fundamental shift from scheduled, point-in-time reviews to ongoing, embedded validation activities. Rather than conducting assurance activities at predefined intervals (e.g., quarterly or annually), continuous assurance integrates validation into daily operations, providing constant feedback on control effectiveness.

This shift enables organizations to:

- Detect and address control weaknesses more quickly, reducing the window of vulnerability.
- Adapt to changing threats and system configurations in near-real time.
- Maintain more current and accurate understanding of their security posture.
- Provide stakeholders with more timely and relevant assurance information.

10.1.2 Automation and AI in evidence collection

Continuous assurance relies heavily on automation and artificial intelligence to collect, analyze, and validate evidence at scale and speed. These technologies enable organizations to:

- Continuously monitor system configurations, user activities, and security events.
- Automatically compare actual configurations against security baselines and policies.
- Use machine learning to identify anomalies and potential security issues.
- Generate real-time alerts when controls deviate from expected behavior.
- Maintain comprehensive audit trails with minimal manual effort.

Emerging technologies such as blockchain can also enhance evidence integrity by providing tamper-evident storage for security logs and configuration data. Security Orchestration, Automation, and Response (SOAR) technologies can integrate assurance activities with incident response, creating a more cohesive approach to security operations and validation.

10.1.3 Challenges in implementation

Despite its potential benefits, continuous assurance presents several significant challenges:

- **High resource demands**: Implementing and maintaining continuous assurance capabilities requires significant investment in technology, infrastructure, and skilled personnel.
- **Technical complexity**: The technical complexity of automated monitoring and validation systems can create implementation and maintenance challenges.
- **Alert fatigue**: Continuous monitoring can generate a high volume of alerts, potentially leading to alert fatigue and overlooked issues.
- **Prioritization difficulties**: With continuous data collection, organizations may struggle to distinguish significant deviations from minor ones.
- **Integration barriers**: Legacy infrastructure and systems may not support the instrumentation and monitoring required for continuous assurance.

To address these challenges, organizations can benefit from a maturity model that guides the incremental development of continuous assurance capabilities. By starting with critical systems and high-risk areas, organizations can gradually expand their continuous assurance coverage as they build expertise and infrastructure.

10.2 Integration with modern development methodologies

Modern development methodologies such as DevSecOps and Agile present both challenges and opportunities for information security assurance. These methodologies emphasize speed, flexibility, and continuous delivery, requiring assurance approaches that can keep pace with rapid development cycles.

10.2.1 Assurance in DevSecOps

DevSecOps integrates security into the DevOps pipeline, emphasizing security as a shared responsibility throughout the development lifecycle. This integration has significant implications for assurance:

- **Pipeline integration**: Assurance activities must be integrated into CI/CD pipelines to provide validation without disrupting development workflows.
- **Automated testing**: Security tests and validations must be automated to match the speed of development and deployment.
- **Fast feedback**: Assurance results must be delivered quickly to developers, enabling immediate remediation of security issues.
- **Guardrails vs. gates**: Assurance in DevSecOps often shifts from gate-based approaches (blocking progress until validation is complete) to guardrail-based approaches (guiding secure development without impeding progress).
- **Continuous metrics**: Security and assurance metrics must be continuously tracked to provide visibility into the security posture of applications and infrastructure.

By adapting assurance approaches to the DevSecOps model, organizations can maintain security validation while supporting the speed and agility required by modern development practices.

10.2.2 Assurance in Agile environments

Agile methodologies, with their emphasis on iterative development and frequent releases, also require adapted assurance approaches:

- **Iterative validation**: Assurance activities must be performed iteratively, validating security in each sprint or release rather than as a final gate.
- **Just-in-time checks**: Security control checks must be performed just in time, focusing on the specific features or components being developed in each iteration.
- **Cross-functional collaboration**: Assurance activities must involve cross-functional teams, including developers, security professionals, and quality assurance specialists.
- **Adaptive planning**: Assurance plans must adapt to changing priorities and emerging risks, aligning with the adaptive planning approach of Agile.
- **Regular reassessment**: Assurance priorities must be regularly reassessed to ensure they remain aligned with the evolving product and threat landscape.

By aligning assurance activities with Agile principles and practices, organizations can maintain security validation while supporting the flexibility and responsiveness required by Agile development.

10.3 Future directions for assurance research and practice

As information security assurance continues to evolve, several areas emerge as promising directions for future research and practice:

- **Assurance for AI and machine learning**: As AI and machine learning become more prevalent in security controls, new approaches are needed to provide assurance for these complex, often opaque systems.
- **Quantitative assurance metrics**: Developing more rigorous, quantitative metrics for assurance can enhance the objectivity and comparability of assurance results.
- **Assurance for cloud and distributed systems**: The shift to cloud and distributed architectures requires adapted assurance approaches that can address the unique challenges of these environments.
- **Standardization of continuous assurance**: As continuous assurance matures, standardization of approaches, tools, and metrics will become increasingly important.
- **Integration of assurance with risk quantification**: Connecting assurance results to quantitative risk assessments can provide more meaningful context for decision-making.
- **Assurance for supply chain security**: As supply chain attacks become more prevalent, assurance approaches must extend beyond organizational boundaries to address third-party and supply chain risks.

By exploring these and other emerging areas, the field of information security assurance will continue to evolve, providing more effective approaches to building justified confidence in security controls in increasingly complex and dynamic environments.

11 Conclusion

Throughout this technical essay, we have explored the multifaceted domain of information security and assurance, examining how organizations can build justified confidence in their security measures through standardized approaches, structured methodologies, and systematic validation. As we conclude, several key insights emerge that highlight the importance of assurance in establishing effective security programs and building public trust.

11.1 Key takeaways

First and foremost, we have seen that there is a fundamental distinction between implementing security controls and proving they work effectively. Security operations focus on designing, implementing, and running controls to protect information, while assurance focuses on validating those controls, testing their effectiveness, and providing confidence that they work as intended. This distinction is essential for sound security governance and trustworthy risk decisions.

We have also explored how various authoritative bodies have defined assurance, from ISO/IEC/IEEE 15026's "grounds for justified confidence that a claim has been or will be achieved" (ISO/IEC/IEEE, 2019) to NIST's "measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the security policy" (Joint Task Force Transformation Initiative, 2011). These definitions share a common emphasis on justified confidence based on evidence, highlighting that assurance is not about absolute certainty but about establishing reasonable confidence through systematic validation.

The anatomy of assurance cases—comprising claims, arguments, and evidence—provides a structured framework for validating security controls. By systematically linking specific claims about security requirements to logical arguments and tangible evidence, assurance cases enable organizations to demonstrate the effectiveness of their security measures in a clear and convincing manner. However, we have also acknowledged the limitations of assurance cases, recognizing that they support informed risk decisions rather than providing absolute certainty.

Our exploration of assurance in software and systems development, based on ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 lifecycles with a focus on ISO 15026 workflow alignment, has demonstrated how assurance can be integrated throughout the development process. By mapping assurance activities to specific lifecycle processes and adapting them to different development methodologies, organizations can build security validation into their development practices, ensuring that security is considered from the earliest stages rather than as an afterthought.

The assurance case examples—including the network firewall example and the software development assurance case with five claims—have illustrated how assurance principles can be applied in practice. These examples demonstrate that effective assurance requires not only well-structured claims and arguments but also high-quality evidence that is relevant, sufficient, reliable, and current.

We have also seen how assurance can be built through management systems, particularly through the integration of ISO 27001 Information Security Management Systems with ISO 15026 assurance cases. This combination provides a comprehensive approach to security management and validation, leveraging the strengths of both frameworks to establish justified confidence in security controls.

Finally, we have explored the strategic value of assurance in building and maintaining public trust. By providing evidence of reliability, truthfulness, and ability, assurance creates the foundation for trust among stakeholders, from customers and partners to regulators and the public. While establishing robust assurance capabilities involves significant costs, these investments are essential for organizations that depend on public trust for their success.

11.2 Recommendations for implementing effective assurance programs

Based on the analysis presented in this paper, several recommendations emerge for organizations seeking to implement effective assurance programs:

- **Establish clear separation between security operations and assurance**

functions to ensure independence and objectivity in the evaluation of control effectiveness.

- **Develop structured assurance cases for critical systems and controls**, systematically linking claims, arguments, and evidence to build justified confidence.
- **Integrate assurance principles into management systems** like ISO 27001, leveraging the PDCA cycle as a continual assurance enabler.
- **Design security policies to serve as assurance enablers** by formulating clear, verifiable requirements that can form the basis for assurance claims.
- **Address common pitfalls in assurance activities**, such as inadequate independence, confirmation bias, siloed approaches, and evidence quality issues.
- **Balance assurance with operational needs** by focusing on risk, coordinating efforts, and leveraging automation to increase efficiency.
- **Acknowledge the limitations of assurance** and set realistic expectations about what assurance can and cannot achieve.
- **Explore continuous assurance approaches** that provide more timely and relevant validation in dynamic environments.
- **Adapt assurance to modern development methodologies** like DevSecOps and Agile to maintain validation without impeding agility.
- **Recognize the strategic value of assurance** in building public trust and enabling business initiatives.
- **Communicate assurance results effectively** to different stakeholders, balancing transparency with security considerations.
- **Align assurance programs with regulatory requirements** while also meeting the organization's strategic needs.

By following these recommendations, organizations can develop more effective assurance programs that provide genuine confidence in their security controls while addressing the practical challenges of security validation in complex environments.

11.3 Future directions for assurance

As technology continues to evolve and security challenges become more complex, assurance practices must also evolve to remain effective. Several trends are likely to shape the future of assurance:

1. **Continuous assurance**: The shift from periodic, point-in-time assessments to continuous, real-time validation will accelerate, enabled by advances in automation, artificial intelligence, and monitoring technologies (Bird & Kim, 2016).
2. **Integration with DevSecOps**: Assurance will become more tightly integrated with DevSecOps practices, with automated security testing, validation, and evidence collection embedded in CI/CD pipelines (Myrbakken & Colomo-Palacios, 2019).

3. **Risk-based approaches**: Assurance activities will increasingly be prioritized based on risk, focusing resources where they will have the greatest impact on security posture and stakeholder trust.
4. **Standardization and interoperability**: Greater standardization of assurance practices and interoperability of assurance tools will enable more efficient and effective assurance across complex, interconnected systems.
5. **Transparency and communication**: Assurance results will be communicated more transparently to stakeholders, supporting informed decision-making and building trust through openness.

11.4 Final reflections

In conclusion, assurance plays a vital role in information security by providing the justified confidence that security measures are effective. It bridges the gap between security implementation and stakeholder trust, enabling organizations to demonstrate not only that they have implemented security controls but that these controls actually work as intended.

By adopting structured approaches to assurance, based on standards such as ISO/IEC/IEEE 15026, ISO/IEC/IEEE 15288, and ISO/IEC/IEEE 12207, organizations can establish a systematic foundation for validating their security measures. By integrating assurance into development processes, management systems, and strategic planning, they can build security validation into their operations rather than treating it as a separate activity.

Ultimately, effective assurance is not just about compliance or technical validation—it is about building and maintaining the trust that is essential for organizational success in an increasingly digital and interconnected world. By investing in robust assurance capabilities, organizations can establish the justified confidence that underpins trusted relationships with stakeholders and supports the achievement of strategic objectives such as public trust.

As we navigate the evolving landscape of information security, assurance will remain a critical enabler of trust, providing the bridge between security implementation and stakeholder confidence. By understanding and applying the principles, methodologies, and practices of assurance explored in this essay, organizations can build more effective security programs that not only protect information assets but also establish the justified confidence that is essential for success in today's digital environment.

A Appendix - Assurance case examples

To illustrate the practical application of assurance principles, this section presents two detailed assurance case examples: a network firewall example based on the presentation and a software development assurance case with five claims. These examples demonstrate how assurance cases can be structured to provide justified confidence in security controls across different domains.

A.1 Network firewall assurance case

Firewalls represent one of the most fundamental security controls in modern networks, making them an ideal subject for examining how assurance principles translate into practice. This example illustrates how an organization can build an assurance case for a network firewall.

A.1.1 Policy foundation

The assurance case begins with a clear policy statement that establishes the requirements and expectations for the firewall:

Purpose: To ensure the organization's network is protected from unauthorized access and malicious activity while supporting the secure flow of legitimate traffic, in alignment with applicable security policies and regulatory requirements.

Scope: This policy applies to all organizational networks, networked systems, and devices protected by firewalls, including perimeter, internal segmentation, and cloud-based virtual firewalls.

Policy statement: The organization's firewall systems shall be configured and maintained to:

- Restrict unauthorized access to internal and external networks
- Allow legitimate traffic in accordance with defined business and operational requirements
- Enforce access control rules that are aligned with security policies and regulatory obligations
- Be regularly reviewed, updated, and tested to ensure effectiveness

This policy provides the foundation for the assurance case, establishing what must be achieved and providing a basis for claims about firewall effectiveness.

A.1.2 Top-level claim

The assurance case is built around a top-level claim that captures the essential security property being assured:

Claim: "The organization's firewall effectively protects the network by restricting unauthorized access while allowing legitimate traffic, in accordance with security policies and regulatory requirements."

This claim has several important characteristics:

- **Specificity**: It focuses on a particular control (the firewall) and its specific function (restricting unauthorized access while allowing legitimate traffic)
- **Effectiveness**: It addresses not just the existence of the firewall but its effectiveness in protecting the network
- **Compliance**: It references alignment with security policies and regulatory requirements, adding a governance dimension

A.1.3 Supporting arguments

The top-level claim is supported by five key arguments, each addressing a specific aspect of firewall effectiveness:

Argument 1: Firewall rule configuration and compliance The firewall enforces predefined security rules based on industry best practices (e.g., NIST, CIS benchmarks). Traffic filtering follows a least privilege model, ensuring only required traffic is permitted. Configuration changes follow a change management process to prevent unauthorized modifications.

Evidence:

- Firewall access control policies and configuration reports
- Rule review logs showing periodic validation and updates
- Change management logs with approvals for firewall rule modifications

Argument 2: Access control implementation Firewall access control lists (ACLs) and policies only allow authorized users, services, and IP addresses. Role-based access control (RBAC) is applied to firewall administration.

Evidence:

- Access control policies and role-based permissions documentation
- Authentication logs showing approved access to firewall settings
- Network segmentation diagrams showing separation of sensitive zones

Argument 3: Threat detection and prevention The firewall includes Intrusion Detection and Prevention System (IDPS) capabilities. Regular updates to threat intelligence feeds ensure protection against emerging threats. Anomaly detection mechanisms alert security teams of suspicious traffic patterns.

Evidence:

- Intrusion detection logs and event history
- SIEM reports analyzing firewall alerts
- Security incident records demonstrating firewall effectiveness in blocking attacks

Argument 4: Resilience and availability Firewalls are configured in high-availability (HA) mode to prevent downtime. Redundant connections ensure business continuity in case of hardware failure. Regular failover testing confirms that secondary firewalls activate seamlessly when needed.

Evidence:

- High-availability setup documentation
- Results of failover tests validating redundancy mechanisms
- Network uptime reports showing availability metrics

Argument 5: Logging and monitoring All firewall activities are logged and centrally monitored via a Security Information and Event Management (SIEM) system. Security teams analyze logs regularly to detect and respond to anomalies. Automated alerts notify security teams of unauthorized access attempts or policy violations.

Evidence:

- Firewall log retention policies and log samples
- SIEM integration reports demonstrating real-time monitoring
- Security team investigation records of past firewall-related alerts

A.1.4 Enterprise requirements considerations

It's important to note that while the original claim and arguments may be sufficient from a topic-specific policy perspective, they may not address all enterprise-level requirements. For example, enterprise security architecture might require that all network security components implement:

- Clock synchronization (for incident management support)
- Use of cryptography (cryptographic key management for multi-factor authentication)

If these enterprise requirements are not addressed in the arguments, the network firewall would fail the assurance case from an enterprise security perspective, even if it meets its topic-specific requirements.

A.2 Software development assurance case

Building on the network firewall example, we now present a software development assurance case that demonstrates how assurance principles can be applied to the software development lifecycle. This example includes five claims that collectively provide assurance that the software development process produces secure software.

A.2.1 Top-level claim

Claim: "The organization's software development lifecycle produces secure software that protects sensitive data, resists common attacks, and complies with security requirements and industry standards."

This top-level claim addresses the overall security of the software development process and its outputs, focusing on the protection of sensitive data, resistance to attacks, and compliance with requirements and standards.

A.2.2 Five supporting claims

The top-level claim is supported by five specific claims, each addressing a different aspect of secure software development:

Claim 1: Security requirements integration **Claim**: "Security requirements are systematically identified, documented, and integrated into the software development process from the earliest stages."

Arguments:

1. Security requirements are derived from business needs, threat models, and compliance obligations
2. Security requirements are documented in a verifiable and testable manner
3. Security requirements are prioritized based on risk and integrated into the development backlog
4. Security requirements are reviewed and approved by security experts before implementation
5. Security requirements are traceable throughout the development lifecycle

Evidence:

- Security requirements documentation with clear traceability to sources
- Threat modeling documentation showing systematic identification of security concerns
- Development backlog showing security requirements with appropriate prioritization
- Security review records demonstrating expert approval of requirements
- Traceability matrices linking requirements to design, implementation, and testing artifacts

Claim 2: Secure design and architecture **Claim**: "The software is designed and architected using secure-by-design principles that mitigate security risks and protect against common vulnerabilities."

Arguments:

1. Security architecture follows defense-in-depth and least privilege principles
2. Design incorporates secure patterns and avoids known anti-patterns
3. Architecture undergoes security review before implementation
4. Design decisions consider security implications and are documented
5. Security architecture is validated against industry standards and best practices

Evidence:

- Security architecture documentation showing defense-in-depth strategies
- Design review records with security considerations
- Security architecture review reports with findings and resolutions
- Documentation of security design decisions and their rationale
- Mapping of architecture to relevant security standards (e.g., OWASP ASVS) (OWASP Foundation, 2021)

Claim 3: Secure implementation and testing **Claim**: "The software is implemented using secure coding practices and undergoes comprehensive security testing to identify and remediate vulnerabilities."

Arguments:

1. Developers follow secure coding standards and guidelines
2. Code undergoes security-focused peer reviews
3. Automated security testing is integrated into the development pipeline
4. Vulnerabilities identified during testing are tracked and remediated
5. Security testing coverage is measured and continuously improved

Evidence:

- Secure coding standards documentation
- Code review records with security-specific comments
- Static application security testing (SAST) reports and trends
- Dynamic application security testing (DAST) reports and trends
- Vulnerability tracking records showing remediation timelines
- Security testing coverage metrics and improvement plans

Claim 4: Third-party component security **Claim**: "Third-party components and dependencies are evaluated, monitored, and managed to prevent the introduction of security vulnerabilities."

Arguments:

1. Third-party components are evaluated for security before approval
2. Approved components are inventoried and tracked
3. Components are continuously monitored for new vulnerabilities
4. Vulnerable components are promptly updated or replaced
5. Component usage follows licensing and compliance requirements

Evidence:

- Third-party component evaluation criteria and process documentation

- Software Bill of Materials (SBOM) showing all components and versions
- Vulnerability scanning reports for third-party components
- Records of component updates in response to vulnerabilities
- Compliance documentation for component licensing

Claim 5: Security verification and validation **Claim**: "The software undergoes independent security verification and validation to confirm that security controls are implemented correctly and effectively."

Arguments:

1. Independent security testing is performed by qualified personnel
2. Penetration testing is conducted before major releases
3. Security verification activities are aligned with risk levels
4. Security validation confirms that controls meet their objectives
5. Security findings are addressed before release

Evidence:

- Independent security testing reports
- Penetration testing reports with findings and remediation
- Risk-based verification planning documentation
- Security validation reports confirming control effectiveness
- Release approval documentation with security signoff

A.2.3 Required arguments

For each claim in the software development assurance case, arguments must:

1. **Be logically structured**: Arguments should follow a clear, logical structure that connects evidence to claims in a coherent manner.
2. **Address all aspects of the claim**: Arguments should comprehensively address all aspects of the claim, ensuring that no critical elements are overlooked.
3. **Consider counterarguments**: Arguments should anticipate and address potential counterarguments or weaknesses, demonstrating that the claim holds even in the face of challenges.
4. **Be explicit about assumptions**: Arguments should clearly state any assumptions upon which they rely, ensuring that these assumptions are reasonable and justified.
5. **Link to specific evidence**: Arguments should explicitly reference the evidence that supports them, establishing a clear connection between claims and their factual basis.

A.2.4 Evidence requirements

Evidence in the software development assurance case must meet several key requirements:

1. **Relevance**: Evidence must be directly relevant to the claims and arguments it supports.
2. **Sufficiency**: Evidence must be comprehensive enough to support the arguments convincingly.
3. **Reliability**: Evidence must come from trustworthy sources and be generated through reliable processes.
4. **Currency**: Evidence must be up-to-date and reflect the current state of the software and development process.
5. **Accessibility**: Evidence must be accessible for review and verification by relevant stakeholders.
6. **Traceability**: Evidence must be traceable to its source and to the claims and arguments it supports.

A.2.5 Integration with development lifecycle

The software development assurance case is integrated with the development lifecycle through:

1. **Requirements phase**: Claims and arguments related to security requirements integration
2. **Design phase**: Claims and arguments related to secure design and architecture
3. **Implementation phase**: Claims and arguments related to secure implementation and testing
4. **Testing phase**: Claims and arguments related to security verification and validation
5. **Release phase**: Final validation of all claims before software release
6. **Maintenance phase**: Ongoing monitoring and updating of claims, arguments, and evidence as the software evolves

This integration ensures that assurance is built into the development process rather than being an afterthought, aligning with the principles of ISO/IEC/IEEE 15288, ISO/IEC/IEEE 12207, and ISO 15026 (ISO/IEC/IEEE, 2017, 2021, 2023).

In conclusion, these assurance case examples demonstrate how organizations can systematically build justified confidence in their security controls, whether for network infrastructure like firewalls or for software development processes. By structuring claims, arguments, and evidence in a logical and comprehensive manner, assura (Content truncated due to size limit. Use line ranges to read in chunks)

A.3 Cloud SaaS assurance use case

Consider a healthcare organization that uses a cloud-based Electronic Health Record (EHR) SaaS application to store and process patient health information. The organization needs to establish justified confidence that the SaaS service adequately protects patient data and complies with relevant regulations.

The SaaS provider operates their application on a major cloud infrastructure provider and also integrates with third-party services for specific functions like analytics and billing. This creates a complex supply chain with multiple parties involved in delivering the service.

A.3.1 Top-level claims

The assurance case begins with top-level claims about the properties that need to be assured:

1. **Security Claim**: The EHR SaaS service protects the confidentiality, integrity, and availability of patient health information in accordance with healthcare industry standards and regulations.
2. **Privacy Claim**: The EHR SaaS service processes patient health information in compliance with applicable privacy regulations and organizational policies.
3. **Compliance Claim**: The EHR SaaS service meets all regulatory requirements applicable to healthcare information systems in the relevant jurisdictions.

These top-level claims are then decomposed into more specific sub-claims that can be directly supported by arguments and evidence. The focus of the use case is on the security claim now.

A.3.2 Security claim decomposition

While the security claim decomposition is normally a comprehensive and challenging exercise, the use case will be built around four essential Cloud security sub-claims to show how the assurance process works:

1.1 Access Control: The SaaS service implements appropriate access controls to prevent unauthorized access to patient health information.

1.2 Data Protection: The SaaS service protects patient health information through appropriate encryption and data protection mechanisms.

1.3 Secure Operations: The SaaS service is operated according to security best practices that maintain the security of patient health information.

1.4 Incident Management: The SaaS service includes appropriate incident detection, response, and recovery capabilities to address security incidents affecting patient health information.

The rest of the Cloud assurance use case will be focused over the Access Control sub-.

A.3.3 Access Control sub-claim

For the access control sub-claim defined above (1.1), the following arguments and evidence can be developed:

Argument 1.1.1: *"The SaaS provider implements appropriate identity and access management controls."*

Evidence:

- SaaS provider's SOC 2 Type 2 report covering access control.
- ISO/IEC 27001 certification with statement of applicability including access control.
- Access control policy documentation.
- Results of penetration testing focused on access controls.
- Access review documentation and results.

Argument 1.1.2: *"The healthcare organization configures and manages user access appropriately."*

Evidence:

- Organization's access management procedures.
- User access review documentation.
- Role definition documentation.
- Privileged access management procedures.
- Authentication configuration documentation.

Argument 1.1.3: *"The integration between the organization's identity systems and the SaaS service is secure."*

Evidence:

- Identity federation configuration documentation.
- Single sign-on implementation details.
- Authentication protocol security assessment.
- Integration security testing results.

A.3.4 Shared responsibility considerations

The access control example demonstrates how the shared responsibility model affects assurance. The SaaS provider is responsible for implementing the access control infrastructure, while the healthcare organization is responsible for configuring and managing user access within that infrastructure.

This division of responsibilities requires evidence from both parties to support the access control claim. The assurance case must account for this shared responsibility by:

1. Clearly defining responsibility boundaries.
2. Identifying evidence required from each party.
3. Establishing arguments that address the integration between responsibilities.
4. Validating that there are no gaps in responsibility coverage.

A.3.5 Pass-through assurance considerations

The SaaS provider relies on an infrastructure cloud provider for certain security controls. This creates a pass-through assurance relationship where the SaaS provider must obtain and validate evidence from their cloud provider to support their own security claims.

For example, to support claims about Access Control, the SaaS provider might rely on:

- The infrastructure provider's access control capabilities.
- Provider's ability to support role-based access controls (RBAC).
- Provider's infrastructure ability to enforce multi-tenant isolation.

The SaaS provider must obtain appropriate evidence from the infrastructure provider, validate that it supports their security requirements, and incorporate it into their own assurance case. This evidence is then passed through to the healthcare organization as part of the overall assurance package.

Pass-through assurance requires:

1. Clear documentation of dependencies on third-party providers.
2. Validation that third-party evidence is sufficient and appropriate.
3. Integration of third-party evidence into the overall assurance case.
4. Ongoing monitoring of changes to third-party controls and evidence.

References

Bird, J., & Kim, F. (2016). Continuous assurance and the continuous assurance case. *AIAA SPACE Forum.*

Cambridge University Press. (2023). *Cambridge dictionary.*

Cloud Security Alliance. (2020). *Cloud controls matrix v4.0* (tech. rep.). CSA. https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Cybersecurity and Infrastructure Security Agency. (2020). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations. *Alert AA20-352A.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

Force, J. T. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (tech. rep. No. NIST Special Publication 800-37, Revision 2). National Institute of Standards and Technology. Gaithersburg, MD.

Government Communications Security Bureau. (2023). *New zealand information security manual.* Government Communications Security Bureau. Wellington, New Zealand.

Howard, M., & Lipner, S. (2006). *The security development lifecycle.* Microsoft Press.

International Organization for Standardization. (2015). *Iso/iec 27017:2015 information technology — security techniques — code of practice for information security controls based on iso/iec 27002 for cloud services* (tech. rep.). ISO.

International Organization for Standardization. (2019). *Iso/iec 27018:2019 information technology — security techniques — code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors* (tech. rep.). ISO.

International Organization for Standardization. (2022). *Iso/iec 27002:2022 information security, cybersecurity and privacy protection — information security controls* (tech. rep.). ISO.

ISO/IEC. (2022). *Information technology — security techniques — information security management systems — requirements* [ISO/IEC 27001:2022]. International Organization for Standardization.

ISO/IEC/IEEE. (2017). *Systems and software engineering — software life cycle processes* [ISO/IEC/IEEE 12207:2017]. International Organization for Standardization.

ISO/IEC/IEEE. (2019). *Systems and software engineering — systems and software assurance — part 1: Concepts and vocabulary* [ISO/IEC/IEEE 15026-1:2019]. International Organization for Standardization.

ISO/IEC/IEEE. (2021). *Systems and software engineering — systems and software assurance — part 4: Assurance in the life cycle* [ISO/IEC/IEEE 15026-4:2021]. International Organization for Standardization.

ISO/IEC/IEEE. (2023). *Systems and software engineering — system life cycle processes* [ISO/IEC/IEEE 15288:2023]. International Organization for Standardization.

Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view* (tech. rep. No. NIST Special Publication 800-39). National Institute of Standards and Technology. Gaithersburg, MD.

Kim, G., Humble, J., Debois, P., & Willis, J. (2016). *The DevOps handbook: How to create world-class agility, reliability, and security in technology organizations.* IT Revolution Press.

Microsoft. (2023). Shared responsibility in the cloud. *Microsoft Azure Documentation.* https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Myrbakken, H., & Colomo-Palacios, R. (2019). Shifting left: DevSecOps as an approach to building secure applications. *International Conference on Information Systems Development.*

Nicholson, J., Coventry, L., & Briggs, P. (2018). Trust in information security: A survey of trust in computing and the implications for security requirements and controls. *International Journal of Human-Computer Studies*, *118*, 54–71.

OWASP Foundation. (2021). Owasp application security verification standard. *Open Web Application Security Project*, *4.0.3*.

Ross, R., McEvilley, M., & Oren, J. C. (2016). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems* (tech. rep. No. NIST Special Publication 800-160, Volume 1). National Institute of Standards and Technology. Gaithersburg, MD.

The Institute of Internal Auditors. (2020). The IIA's three lines model: An update of the three lines of defense. *The Institute of Internal Auditors.*