White Paper
Information Security Integration within the Enterprise Reference Architecture Model Part 2

WP0074 | May 2013

Guy B. Sereff

Guy Sereff is an author, speaker and technology practitioner. His Technology Industry experience includes Application Research and Development, Large-Scale Technology Management, and Global Enterprise Architecture.

As well as a pragmatic blend of Strategy and Tactical execution, Guy also has extensive Architectural Domain experience which covers Business Architecture, Information Architecture, Solution Architecture and Enterprise Architecture.

In Part 1: Foundation we reviewed the distinction of and the relationships between Enterprise Architecture, Enterprise Architecture Frameworks and Enterprise Reference Architecture Models. We also discussed several key Information Security Architecture considerations, such as available standards, relevant certifications and supplemental methodologies designed to offer organization resources to help them address the on-going challenge of providing secure and reliable technology solutions. Although not exhaustive or overly prescriptive, the intent of the first white paper was to provide a conceptual base from which to build on. With that base intact, we can now begin to discuss the more important aspect of putting theory into practice.

In this white paper, Part 2: Implementation, we will concisely focus on how to successfully bring these base concepts together into a strategic plan of action. That plan begins by carrying out a four-step approach that organizations must take if they want to better integrate Information Security into their broader Enterprise Reference Architecture Model. The goal is for these activities to become part of the organization's day-to-day standard operating procedures, rather than a one-time campaign or slogan-filled program du jour.

The four steps include:

1. Establish Information Security Architecture as its own Reference Architecture Domain
2. Add Information Security Attributes to the Reference Architecture Domain Template
3. Integrate Information Security Into the Delivery Process
4. Implement an on-going Information Security Audit Program

These steps don't have to be undertaken sequentially nor must they be addressed serially; it really depends on where the most critical process risks are today and how clearly the end-state vision is shared across the organization. Addressing two or more steps of the plan concurrently is quite possible, providing that there is open communication across the work teams, clear common objectives and a consensus of what successful Information Security Architecture looks like.

While there is never any guarantee of total risk mitigation from an Information Security perspective, adapting and applying these changes into an organization's Enterprise Reference Architecture Model practice will help strengthen the level of Information Security competency. Just keep in mind that being competent is not enough - protecting the assets, interests, and constituents of an organization requires constant and deliberate execution of risk management and threat neutralization techniques with minimal business and operational friction or disruption.

Establish Information Security Architecture as its own Reference Architecture Domain

It seems surprising to have to even identify this as a step at all, but many organizations have not formally established Information Security as a discrete reference architecture domain within their reference architecture portfolio. There may be best practices, security policies, secure design patterns and data governance rules already in place across the organization, yet a consolidated view of the Information Security domain may not explicitly exist. Not having an authoritative Information Security Reference Architecture to point to as the governing design standard introduces potential risk to all of the other domains, as each of them may or may not be addressing security in adequate detail or with sufficient consistency.

Another important consideration is the roadmap nature of reference architectures. If Information Security is not defined as its own reference architecture domain, stakeholders and domain participants will struggle to understand the end state vision and what the plan of record for achieving that visionary end state is. While perhaps not true at every organization, many institutions place tremendous pressure on project

TIP: Weave Information Security into the core fabric of all enterprise architecture disciplines by establishing a discrete Information Security Reference Architecture and aligning all other reference architecture domains to it. Move beyond technical implementation and get security awareness engrained into the engineering culture of the organization.

Guy Sereff, 2013

delivery teams to stay on track no matter what. If Information Security standards and constraints are not readily available at inception and design time, delivery teams must wait until the materials are located, wait until an Information Security Architect is assigned and provides input, or take action by making best efforts to incorporate their own interpretation of Information Security guidelines to keep the project moving.

The Information Security Reference Architecture will address all of the same topical areas as the other domains based on the reference architecture template the organization is using (i.e. domain metadata, strategy, capabilities, roadmap, etc.). As would be true for each domain, there will be certain domain-specific attributes that are unique to Information Security, such as security risk management, threat assessment, prevailing legal and compliance security controls, confidential data handling requirements, approved cryptography methods and so forth.

Note that the Information Security Reference Architecture does not replace or override any of the institution's existing security policies or standards. It simply takes those standards to the next level of detail by defining the architectural approach to be used across the organization when designing solutions that will ultimately instantiate capabilities governed by those policies and standards. Think of it as removing one layer of abstraction, in that it defines how those policies and standards will be manifested in delivered solutions. This may include everything from common security code libraries and shared services to third-party secure communication protocols. The key is to include those security architecture elements that can be generalized across the organization and support the security needs of the other reference architecture domains.

Governing the Information Security Reference Architectures should also follow the same approach as taken with the other domains. Solution delivery communities must be made aware that Information Security has now been promoted to its own domain, along with an education campaign of the domain's content, target end state and roadmap commitments. Design review mechanisms must validate adherence to Information Security aspects covered by the reference architecture before building permits are issued. Portfolio management techniques must be used to track information security objects and elements that are targeted for deprecation to ensure that they are being taken out of service and removed from the environment on a timely basis.

> *"Defining a 'single' and 'miracle' security architecture is hardly ever possible"*[i]

Finally, there simply are no magic bullets, potions, spells, incantations or software plug-ins that can make an organization instantly secure and remain that way in perpetuity. However, it is possible to effectively manage security risks in a more efficient manner under the control of a strong, well-constructed Information Security Reference Architecture.

Add Information Security Attributes to the Reference Architecture Domain Template

As we noted earlier when reviewing some of the commercially available Enterprise Architecture frameworks, Information Security has not always been included as a first priority, but rather treated to some degree as an ancillary topic or secondary concern. Commentary on the importance of Information Security appeared, but it was still not initially considered to be a critical component, which is disappointing. When reviewing various domain reference artifacts over the years from a variety of institutions, this trend seems to have made its way into the reference architecture content templates as well; thorough Information Security aspects also appear to be missing from many reference architecture templates in use today.

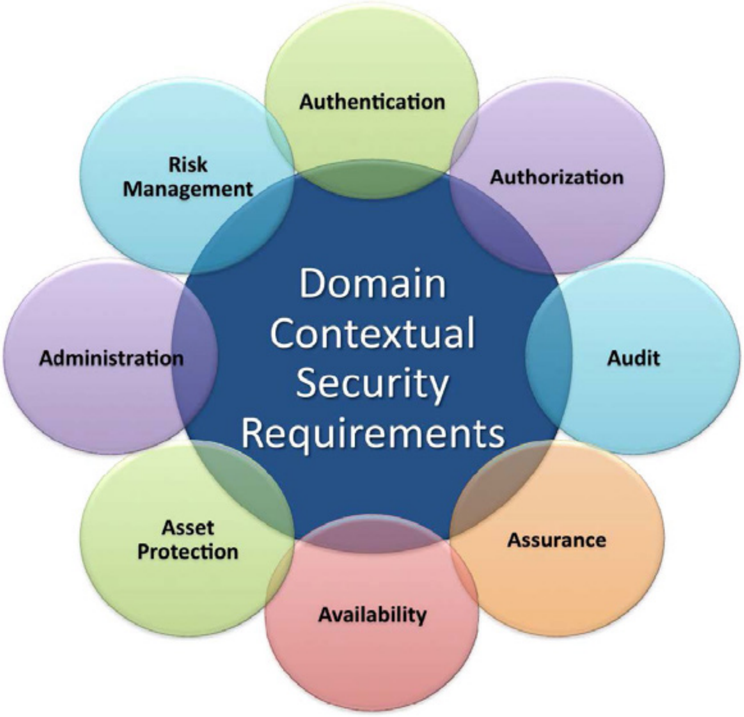


Figure 1 - TOGAF Security Areas as Domain Security Context

Establishing an Information Security Reference Architecture does not replace the need to assess and address Information Security considerations across all domains. The opposite is also true: including Information Security features in other domains does not negate the need for a separate Information Security Reference Architecture. Both approaches are required and are complimentary to one another. Common security characteristics can be moved up into the broader Information Security domain, while contextual attributes can be left on the reference architecture template to be captured as metadata describing the other domains. If the current reference architecture template accommodates Information Security considerations already, review them to make sure they are up to date and still relevant to the needs of the organization. For example, we can adapt the TOGAF security architecture areas discussed earlier to establish contextual domain security requirements as shown in *Figure 1*.

Additional topics to potentially consider when refactoring the Reference Architecture Domain Template to address Information Security include:

Where does this domain align with the Information Security Reference Architecture Model?

- Current State
- End State
- Roadmap

Where does this domain not align with the Information Security Reference Architecture Model?

What unique Information Security capabilities or considerations does this domain require?

What inherent risks are associated with this domain relative to:

- Business
- Operations
- Technology

What are the Security Incident Metrics for this domain (i.e. Realized Risk Profile)?

- Lifetime Incidents (Count by Reporting Period, Net Economic Loss)
- Severity Stratification (% High, % Medium, % Low)
- Incident Velocity (Accelerating, Maintaining, Decelerating)

What other domains are potentially impacted from an Information Security perspective?

The intent is not to recreate the Information Security Reference Architecture numerous times within the reference architecture template, but rather to provide traceability and alignment across the domains. The goal is to ensure that Information Security is deliberately included in the Enterprise Reference Architecture Model, both vertically as its own domain, and horizontally across all other domains.

Integrate Information Security into the Delivery Process

Just as Six Sigma taught us not to inspect quality into something after the work has been done but to build quality into the process to begin with, the same holds true for Information Security. Waiting to review Quality Assurance (QA) or Vulnerability Assessment (VA) test results to see if Information Security considerations were well cared for during requirements, design and implementation is much too late. Problems found at that point in the process are expensive to fix and certify, leading to potential ‘scope negotiation’ where discovered risks are intentionally left unmitigated in an effort to protect the delivery date. Simply stated, Information Security considerations must be explicitly cared for by the organization’s entire Systems Development Life Cycle (SDLC). The National Institute of Standards and Technology (NIST) concurs, offering the following observation:[ii]

“To be most effective, information security must be integrated into the SDLC from system inception. Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:

Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;

Awareness of potential engineering challenges caused by mandatory security controls;

Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and

Facilitation of informed executive decision making through comprehensive risk management in a timely manner.”

The area of Information Security process integration alone is large enough to support many white papers and manuscripts well beyond our scope here. We’ll wrap this section up by highlighting a couple of interesting tools that others have found beneficial when trying to embed Information Security into their delivery process.

CORAS Model-Based Risk Assessment

Most requirement gathering efforts focus on ‘happy path’ use cases, hoping to cram as many business capabilities into the release window as possible. Some organizations do spend a limited amount of time on elicitation of alternative patch scenarios as well (at least the ones that can’t easily be ignored). Model Based Security analysis is an approach that seeks to identify and model mis-functionality and misuse cases early on in the definition phase.

Figure 2 shows a simple example of integrating Use Cases and Misuse Cases into a Combined Use Case Diagram.[iii] This approach is based off of the CORAS Model-Based Risk Assessment method, which is designed to provide model-driven analysis of critical security components.[iv] Risk Assessment following the CORAS model includes context identification, risk identification, risk analysis, risk evaluation and risk treatment.

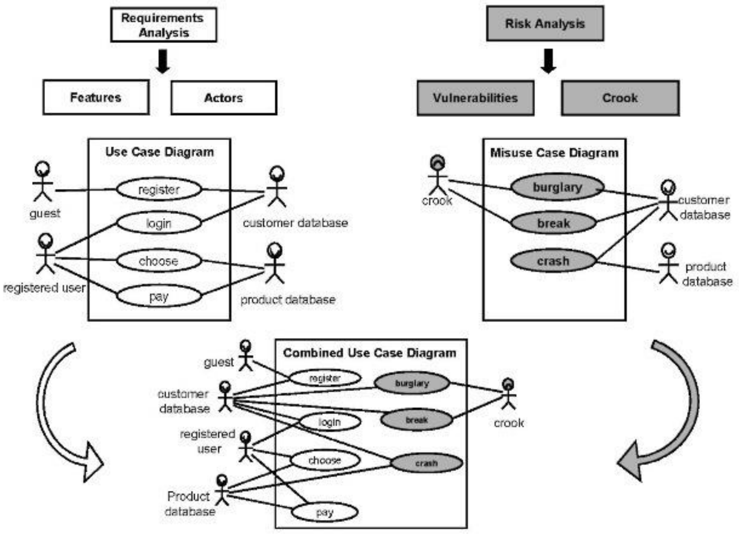


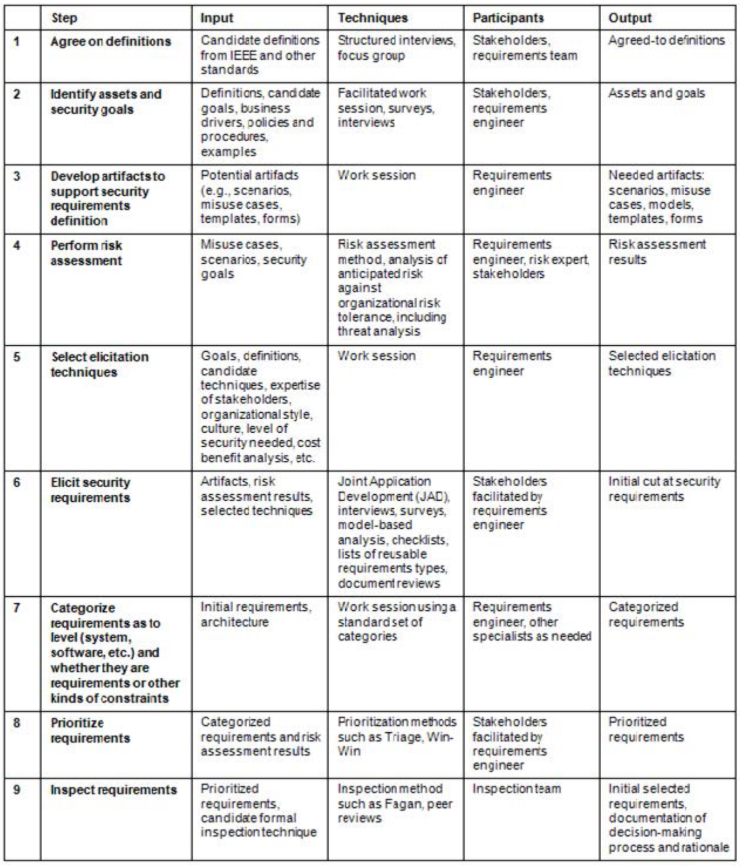
Figure 2 - Sample Model Base Security Combined Diagram

SQUARE - Security Quality Requirements Engineering

The Carnegie-Mellon Software Engineering Institute (SEI) established the Security Quality Requirements Engineering (SQUARE) approach in an effort to move security considerations further forward in the delivery live cycle. The SQUARE model is a nine-step program that provides inputs, techniques, participants and outputs across a set of activities as shown in *Figure 3*.

This model could be overlaid against most SDLC models to orchestrate security element integration with minimal disruption to the existing process. SEI also has tools available to help facilitate execution of the nine-step process while providing exports to various requirement management tools.

The important takeaway here is that Information Security becomes very difficult to replace or significantly enhance once its host application makes its way into the production.[v]



	Step	Input	Techniques	Participants	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Stakeholders, requirements team	Agreed-to definitions
2	**Identify assets and security goals**	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Stakeholders, requirements engineer	Assets and goals
3	**Develop artifacts to support security requirements definition**	Potential artifacts (e.g., scenarios, misuse cases, templates, forms)	Work session	Requirements engineer	Needed artifacts: scenarios, misuse cases, models, templates, forms
4	**Perform risk assessment**	Misuse cases, scenarios, security goals	Risk assessment method, analysis of anticipated risk against organizational risk tolerance, including threat analysis	Requirements engineer, risk expert, stakeholders	Risk assessment results
5	**Select elicitation techniques**	Goals, definitions, candidate techniques, expertise of stakeholders, organizational style, culture, level of security needed, cost benefit analysis, etc.	Work session	Requirements engineer	Selected elicitation techniques
6	**Elicit security requirements**	Artifacts, risk assessment results, selected techniques	Joint Application Development (JAD), interviews, surveys, model-based analysis, checklists, lists of reusable requirements types, document reviews	Stakeholders facilitated by requirements engineer	Initial cut at security requirements
7	**Categorize requirements as to level (system, software, etc.) and whether they are requirements or other kinds of constraints**	Initial requirements, architecture	Work session using a standard set of categories	Requirements engineer, other specialists as needed	Categorized requirements
8	**Prioritize requirements**	Categorized requirements and risk assessment results	Prioritization methods such as Triage, Win-Win	Stakeholders facilitated by requirements engineer	Prioritized requirements
9	**Inspect requirements**	Prioritized requirements, candidate formal inspection technique	Inspection method such as Fagan, peer reviews	Inspection team	Initial selected requirements, documentation of decision-making process and rationale

Figure 3 - The SQUARE Nine-Step Program

TOGAF 9 Architecture Contract

The last point we will talk about is the adaptation of the Architecture Contract from TOGAF 9 as a design governance tool for Information Security.[vi] Architecture Contracts are agreements between the architecture community and the various constituents tasked with solution delivery for architecturally significant efforts. As these agreements typically contain conformance to key design principles and associated reference architectures, the contract can be adapted to specifically address Information Security requirements and solution constraints.

Post Mortem project evaluation will reveal the level of adherence to the security aspects of the contract and can be used to track progress towards the strategic Information Security end state on an initiative-by-initiative basis. Note that evaluating the project against the architectural contract after it has gone into production is typically too late to influence the final release candidate build - evaluation against the contract should occur once programming is complete and the release is certified for quality testing.

The critical points to highlight from this step are (1) move Information Security Architecture and design treatments up as early in the delivery life cycle as possible, (2) ensure that Information Security is cared for throughout the delivery process, and (3) create a governance model that holds participants accountable for delivering secure solutions aligned to the Information Security Reference Architecture model.

Implement an on-going Information Security Audit Program

Most organizations will already have some form of an Information Security Audit and Control process in place, testing various aspects of policy adherence and enforcement around the institution. Going a step beyond that, we propose auditing each significant project or initiative against the prevailing Information Security Reference Architecture model to ensure that new risks are not being introduced and that non-strategic mitigation solutions are not getting implemented. In addition to the traditional post-design evaluation against the reference architecture model, additional testing specifically designed to validate Information Security adherence should also be conducted.

Vulnerability assessments, or ‘ethical hacks’ are not uncommon for solutions delivered through browser-based channels such as the web or mobile devices. But what about other platforms that expose corporate data and communication networks through other channels or ‘thick’ client applications? These systems are also prone to security breaches and should be exhaustively tested during the certification process to assess their level of soundness from an Information Security perspective.

An effective Information Security governance and audit practice, according to the ISACA (Information Systems Audit and Control Association), will result in the following benefits:[vii]

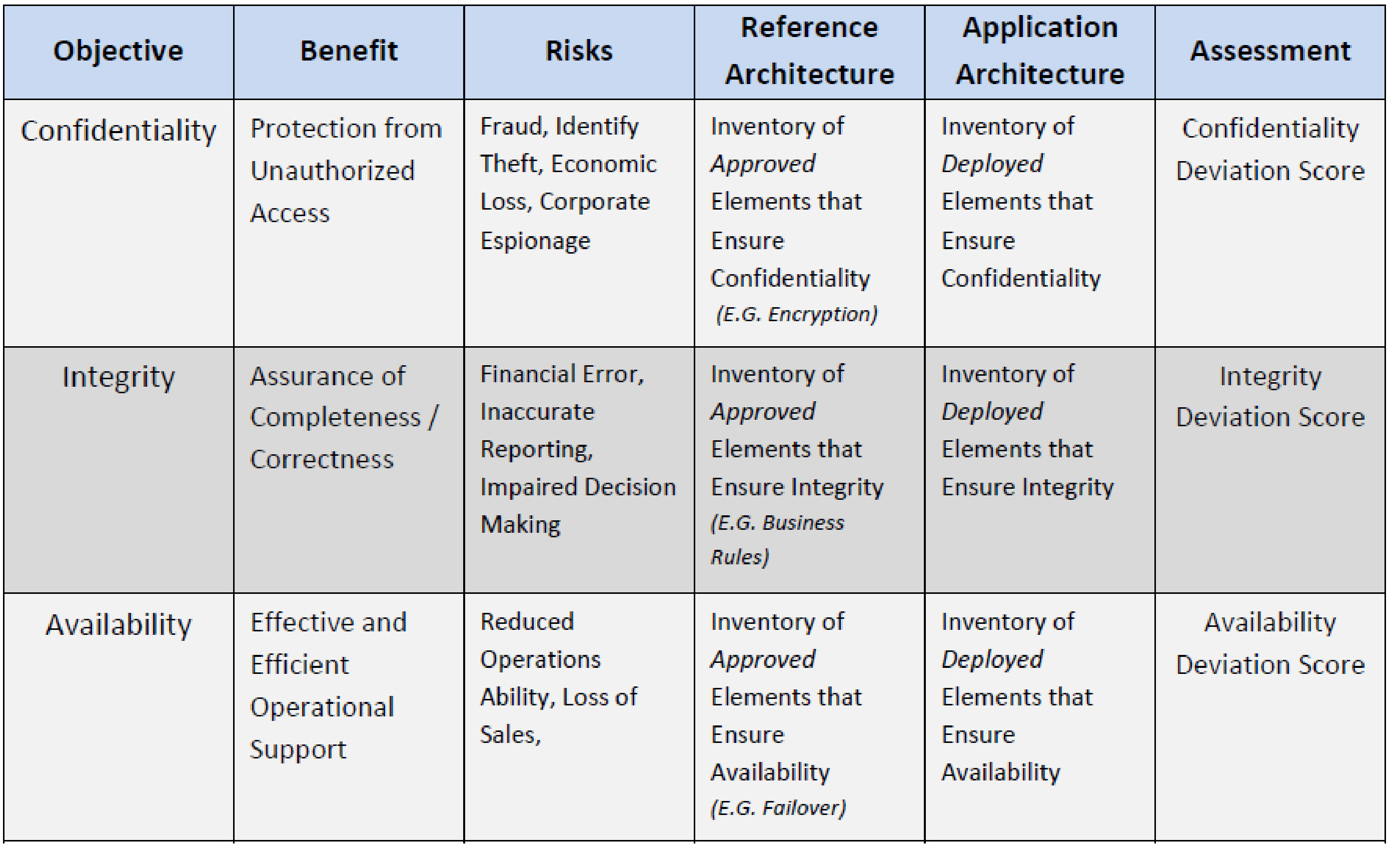
- Strategic Alignment
- Risk Management
- Business Process Assurance / Convergence
- Value Delivery
- Resource Management
- Performance Measurement

We can leverage these concepts to not only evaluate the benefits of Information Security Governance, but to also highlight the benefits of aligning solutions to the Information Security Reference Architecture:

- Consistent Application of Information Security Policies
- Reduced Solution Complexity, Redundancy and Variation
- Measurable Progression Towards Strategic End-State

According to Senft and Gallegos, “the three fundamental objectives for information [security] are Confidentiality, Integrity, and Availability.”[viii] Adapting their observations into an assessment of an application’s alignment to the Enterprise Information Security Reference Architecture

Model would provide for a two-way validation; one for the reference architecture itself, and one for the application being compared to the reference architecture:



Objective	Benefit	Risks	Reference Architecture	Application Architecture	Assessment
Confidentiality	Protection from Unauthorized Access	Fraud, Identify Theft, Economic Loss, Corporate Espionage	Inventory of *Approved* Elements that Ensure Confidentiality *(E.G. Encryption)*	Inventory of *Deployed* Elements that Ensure Confidentiality	Confidentiality Deviation Score
Integrity	Assurance of Completeness / Correctness	Financial Error, Inaccurate Reporting, Impaired Decision Making	Inventory of *Approved* Elements that Ensure Integrity *(E.G. Business Rules)*	Inventory of *Deployed* Elements that Ensure Integrity	Integrity Deviation Score
Availability	Effective and Efficient Operational Support	Reduced Operations Ability, Loss of Sales,	Inventory of *Approved* Elements that Ensure Availability *(E.G. Failover)*	Inventory of *Deployed* Elements that Ensure Availability	Availability Deviation Score

This assumes that elements within the Information Security Reference Architecture model have been classified to the fundamental objectives. Deviation scores simply reflect the number of deployed elements that differ from their corresponding approved elements. Information Security elements can be any number of assets, whether they are usage of specific software components, such as a SOA-based common service, or a prescribed protocol, such as 2-way SSL (Secure Socket Layer) with Mutual Authentication. An additional metric can be captured for those deployed assets or elements that do not have a counterpart within the reference architecture. This secondary metric can help determine additional areas of coverage and the reference architecture may need to address to keep it relevant to the needs of the organization.

You may recall from our discussion in Part 1: Foundation that we covered a few standards and frameworks related to Information Security. ISO/IEC 27002 provides a comprehensive set of best practices and techniques related to Information Security management. Several independent providers have developed audit and self-assessment tools to validate ISO/IEC 27002 based on those practices that could be augmented to address conformance to the Information Security Reference Architecture as well.

The last item we'll consider related to security auditing is the ITIL Security Management Evaluation process. Those familiar with ITIL will recognize the multi-faceted evaluation approach related to implementation (Self Assessment, Internal Audit, External Audit) and operation (Security Event Logging).[ix]

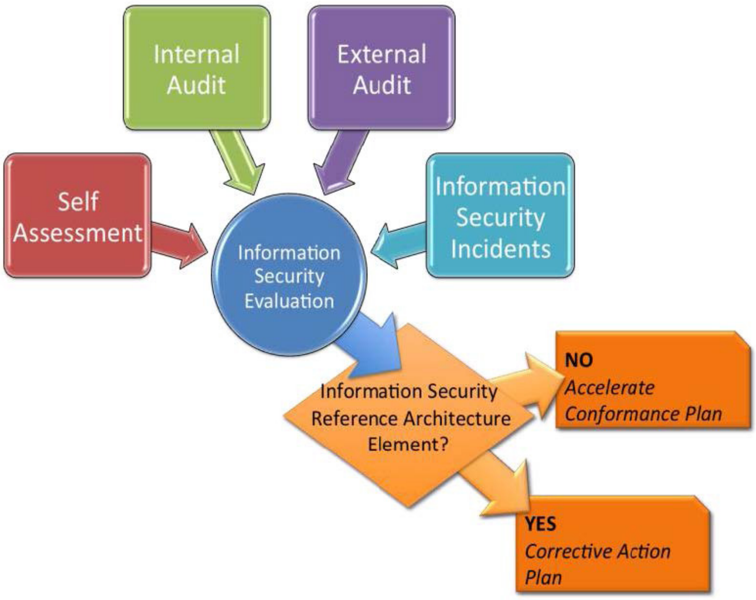

Internal Audit
External Audit
Self Assessment
Information Security Incidents
Information Security Evaluation
Information Security Reference Architecture Element?
NO
Accelerate Conformance Plan
YES
Corrective Action Plan

Figure 4 - ITIL Security Management Evaluation Extension

The proposal here is to take the audit findings and documented security events and tie them back to their source in order to determine if the incident occurred due to a non-reference architecture component or not. If so, there is a strong case for driving an accelerated conformance plan and eliminating variation to mitigate further risk. However if the finding was related to a reference architecture component, there is an opportunity to further strengthen the reference architecture component itself through a Corrective Action Plan, thereby hardening the security shell of all implementations of the referenced element. The two-fold benefit comes from targeted conformance to the reference architecture model, as well as establishing a pattern of continuous improvement. Go beyond the mechanics of auditing for the sake of testing for policy conformance or penetration resistance of web sites and deeply assess how the components defined in the Information Security Reference Architecture model are being adopted across the enterprise and how well they are actually performing.

Conclusion

Few organizations will argue that they want to be less secure than they are today. Yet when you look for evidence of Information Security Architecture's importance in terms of process rigor and investment levels, a mixed message emerges. The pragmatic steps we discussed in this white paper are not really provocative or overly complicated. However, they do require an intentional and disciplined approach, the speed and effectiveness of which will be impacted by (1) the organization's access to domain expertise, (2) the organization's level of readiness/willingness for change, and (3) the organization's ability to change.

Organization's can strengthen their Information Security integration within their Enterprise Reference Architecture model by taking decisive action:

- Make Information Security Architecture a vital part of the Enterprise Architecture Model
- Establish an Information Security Reference Architecture Domain
- Address Information Security Architecture both vertically (intra-domain) and horizontally (inter-domain)
- Engrain Information Security into every aspect of the solution delivery process

- Assume the work is never done; continually assess the threat landscape and adapt
- Follow a structured Information Security Audit program to assess reference architecture effectiveness and adoption

References

[i] Khadraoui, Djamel and Francine Hermann (ed). (2007) Advances in Enterprise Information Technology Security (Premier Reference). Chapter 1 - Security Architecture (Gastellier-Prevos, Sophie and Maryline Laurent-Maknavicius). Hershey, Pennsylvania, USA: Information Science Reference (IGI Global).

[ii] Kissel, Richard et al. (2008) Security Considerations in the System Development Life Cycle. P. 1. Washington, DC; National Institute of Standards and Technology, U.S. Department of Commerce

[iii] Integrating Security in the Development Process with UML. what-when-how. http://what-when-how.com/information-science-and-technology/integrating-security-in-the-development-process-with-uml/. Accessed 4/2/2013

[iv] Aagedal, Jan Øyvind et al. (2002) Model-based Risk Assessment to Improve Enterprise Security. IEEE.

[v] SEI. (2012). SQUARE - Requirements Engineering for Improved System Security and Privacy. Carnegie Mellon Software Engineering Institute. http://www.cert.org/sse/square/. Accessed 4/8/2013.

[vi] TOGAF 9. (Section8.1.1)

[vii] Brotby, Krag. (2009) Information Security Governance: A Practical Development and Implementation Approach. P. 6. Hoboken, New Jersey, USA: John Wiley & Sons, Inc.

[viii] Senft, Sandar and Frederick Gallegos. (2013) Information Technology Control and Audit, Fourth Edition. P. 468. Boca Raton, Florida, USA: CRC Press

[ix] ITIL Security Management. http://en.wikipedia.org/wiki/ITIL_Security_Management. Accessed 5/8/2013.

Recommended Reading

OWASP Application Security Verification Standard
Paulo Coimbra (2009)

Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
TJ O'Conner (2012)

2012 Data Breach Investigations Report
Verizon (2012)

Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis
Talabis and Martin (2012)

IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data
Lance Hayden (2010)

Information Security Management with ITIL V3
Jacques Cazemier (2010)

Orbus Software
3rd Floor
111 Buckingham Palace Road
London
SW1W 0SR
United Kingdom

+44 (0) 870 991 1851
enquiries@orbussoftware.com
www.orbussoftware.com