TOGAF® Poster Series #23

Security Architecture and the ADM 2

by Roger Evernden

In this poster we show how to adapt the ADM to cover Security Architecture issues – the common theme is "what could go wrong?"

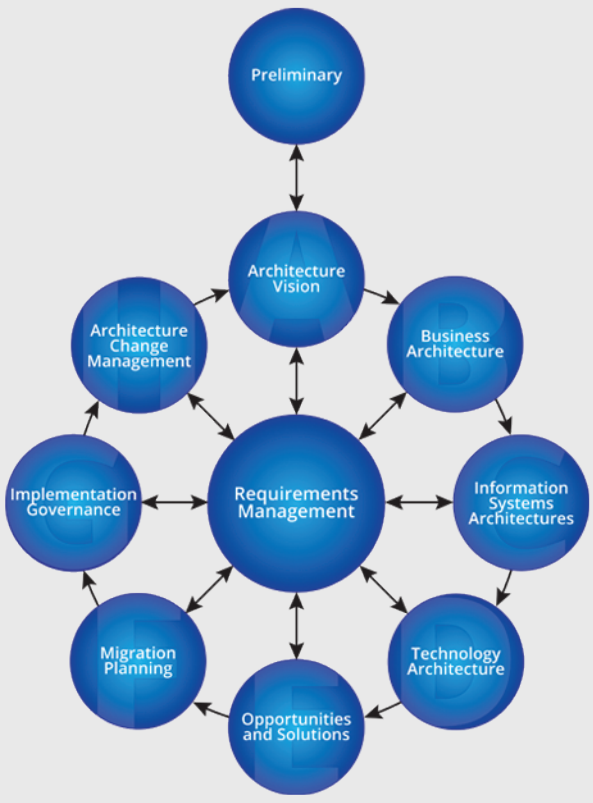
Recommended Security Steps to add to each Phase of the ADM:

Phase A: Architecture Vision
- Obtain management support for security measures
- Define necessary security-related management sign-off milestones of this architecture development cycle
- Determine and document applicable disaster recovery or business continuity plans/requirements
- Identify and document the anticipated physical/business/regulatory environment(s) in which the system(s) will be deployed
- Determine and document the criticality of the system: safety-critical/mission-critical/non-critical

Preliminary Phase
- Scope the enterprise organizations impacted by the security architecture
- Define and document applicable regulatory and security policy requirements
- Define the required security capability as part of Architecture Capability
- Implement security architecture tools

Phase B: Business Architecture
- Determine who are the legitimate actors who will interact with the product/service/process
- Assess and baseline current security-specific business processes (enhancement of existing objective)
- Determine whom/how much it is acceptable to inconvenience in utilizing security measures
- Identify and document interconnecting systems beyond project control
- Determine the assets at risk if something goes wrong - "What are we trying to protect?"
- Determine the cost (both qualitative and quantitative) of asset loss/impact in failure cases
- Identify and document the ownership of assets
- Determine and document appropriate security forensic processes
- Identify the criticality of the availability and correct operation of the overall service
- Determine and document how much security (cost) is justified by the threats and the value of the assets at risk
- Reassess and confirm Architecture Vision decisions
- Assess alignment or conflict of identified security policies with business goals
- Determine "what can go wrong?"

Phase H: Architecture Change Management
- Determine "what has gone wrong?"



Phase G: Implementation Governance
- Establish architecture artifact, design, and code reviews and define acceptance criteria for the successful implementation of the findings
- Implement methods and procedures to review evidence produced by the system that reflects operational stability and adherence to security policies
- Implement necessary training to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; ensure awareness training of all users and non-privileged operators of the system and/or its components
- Determine "what has gone wrong?

Phase C: Information Systems Architectures
- Assess and baseline current security-specific architecture elements (enhancement of existing objective)
- Identify safe default actions and failure states
- Identify and evaluate applicable recognized guidelines and standards
- Revisit assumptions regarding interconnecting systems beyond project control
- Determine and document the sensitivity or classification level of information stored/created/used
- Identify and document custody of assets
- Identify the criticality of the availability and correct operation of each function
- Determine the relationship of the system under design with existing business disaster/continuity plans
- Identify what aspects of the system must be configurable to reflect changes in policy/business environment/access control
- Identify lifespan of information used as defined by business needs and regulatory requirements
- Determine approaches to address identified risks:
- Identify actions/events that warrant logging for later review or triggering forensic processes
- Identify and document requirements for rigor in proving accuracy of logged events (non-repudiation)
- Identify potential/likely avenues of attack
- Determine "what can go wrong?"

Phase F: Migration Planning
- Assess the impact of new security measures upon other new components or existing leveraged systems Implement assurance methods by which the efficacy of security measures will be measured and communicated on an ongoing basis
- Identify correct secure installation parameters, initial conditions, and configurations
- Implement disaster recovery and business continuity plans or modifications
- Determine "what can go wrong?"

Phase D: Technology Architecture
- Assess and baseline current security-specific technologies (enhancement of existing objective)
- Revisit assumptions regarding interconnecting systems beyond project control
- Identify and evaluate applicable recognized guidelines and standards
- Identify methods to regulate consumption of resources
- Engineer a method by which the efficacy of security measures will be measured and communicated on an ongoing basis
- Identify the trust (clearance) level of:
- Identify minimal privileges required for any entity to achieve a technical or business objective
- Identify mitigating security measures, where justified by risk assessment
- Determine "what can go wrong?"

Phase E: Opportunities & Solutions
- Identify existing security services available for re-use
- Engineer mitigation measures addressing identified risks
- Evaluate tested and re-usable security software and security system resources
- Identify new code/resources/assets that are appropriate for re-use
- Determine "what can go wrong?"

The previous poster (Part 1) provides an overview of guidelines, explaining why Security is a separate chapter in TOGAF.