IT4IT™ Forum & Security Forum
Security / Risk Reference Architecture Project Charter

Status: FINAL
Revision level: 1.0
Date: 4 Oct. 2021
Authors: Altaz Valani, Rob Akershoek

A. Project Description

General description of the project

Much of the delivery of digital products is focused on speed of our pipelines. While this is important, it misses key security and risk considerations that, unfortunately, end up slowing down the business because of remediation efforts (which incur both time and cost). The challenge lies with segregated processes, systems, and data which then need to be manually integrated. That leads to either slowing down our DevSecOps teams or deferring security activities until it is too late. Neither option is sustainable. We must ensure that our digital products and services are delivered securely and that compliance can be assured continuously (e.g., continuous control monitoring). In this way, security is part of the entire digital lifecycle as a key enabler rather than a disruptor.

This project will focus on integrating application security and risk management into the digital delivery process. This integration will involve identifying key components of the "security fabric" and how they will support reuse, automation, and traceability.

Challenges:

- Increasing complexity to manage security and risk (e.g., more services and components, more vendors, more data, more changes)
- Evolving security/risk tooling landscape (e.g., many different tools and vendors)
- Lack of an industry framework to manage security end-to-end

Market analysis:

- No security reference architecture currently exists in the market
- No standard security management capability model exists in the market

The need:

- Embed security and risk management activities into digital delivery fabric (e.g., DevSecOps, security controls in the CI/CD pipeline, intelligent pipelines)
- Automate security and risk management activities
- Integrate a security data model
- Define a consistent security management architecture that includes key capabilities, tools and data flows

B. Goals of this Project

- Primary Goals
    - Identify representative real-world security and risk use cases from delivery of a digital product

    - Define which security and risk management capabilities are needed to effectively deliver in those use cases
    - Understand the system and data integrations needed to enable the identified capabilities
    - Incorporate security and risk into the IT4IT Reference Architecture (v3.x)
- Secondary Goal
    - Incorporate requirements of governance by design in project deliverables to aid corporate counsels and litigators

C. Project Deliverables

This project will deliver:

- Phase 1
    - Step 1: Create a security/risk capability and data/information model, visualized similarly to IT4IT
        - Develop full list of use cases in delivering a digital product then select ones to fully build out, focusing on end-to-end value streams
            - Examples:
                - Security embedded in CI/CD pipeline
                - Security monitoring
                - Risk assessment, analysis
                - Cyber defense
        - Link use cases to challenges faced by organizations
        - Identify required tooling capabilities
        - Identify required capabilities from existing publications/groups/organizations:
            - Security Forum publications
                - O-ISM3
                - Open FAIR
            - IT4IT publications
            - OTTF publications (O-TTPS)
            - NIST, ISO, Open Cyber Security Alliance, etc.
    - Step 2: **Create Minimum Viable Product: Security/Risk Management Reference Model**
        - *Focused on the minimum required for any organization delivering a Digital product*
            - *Foundation risk management framework*
        - Support the use cases built out in the previous deliverable to be published as Guide(s)
        - Build security/risk capability and data/information model from Step 1
            - Utilize to determine key stakeholders for deliverable
            - Relate to security and risk management (e.g., risks, threats, vulnerabilities, pipeline)
        - Incorporate Agility for adapting to business requirements
            - Ensure Security becomes an enabler, not a blocker
        - Incorporate governance by design and considerations of corporate counselors and litigators

        - Establish common terminology, data, controls
            - Facilitate interoperability
    - Step 3: Create final deliverable: Security/Risk Management Reference Architecture
        - Refine end-to-end use cases
        - Provide guidance on additional requirements
            - Compliance, legal, risk management, etc.
        - Determine requirements for standardization
- Phase 2
    - Describe how Security/Risk Management Reference Architecture is embeddable in/complementary to the IT4IT™ Reference Architecture
        - Mapping to/embedding in already-existing IT4IT Reference Architecture standard
    - Potential expansion into other areas of IT, OT

D. Project Value Proposition

A. Much needed guidance for integrating security and risk into digital delivery pipelines without unnecessarily slowing down the business
    a. Framework to assess and improve security management capability
B. Create communications vehicle for discussion
C. Framework for supporting journey to automating more security activities
D. Improve the maturity of the security/risk management capabilities
E. Embed security and risk into the Digital delivery model, resulting in safer and more compliant delivery
F. Integrate security management capabilities, resulting in less wasted effort, built-in proactive security, traceability, defensible security assurance, and faster resolution of security issues
G. Incorporate requirements of corporate counsels and litigators and components of governance by design

Target audience:

- Executive level
    - Risk executive (Chief Risk Officer)
    - IT executive
    - Security executive
    - Business executive
    - Risk & Compliance Officer
    - Corporate counsels and litigators
- Management level
    - Security operations lead
    - Digital product manager
    - Enterprise Architect
- Practitioner level
    - Security architect
    - DevOps specialist (to understand how security is embedded into the digital delivery pipeline)

E. Project Personnel

A. Stakeholders

   a. The governing stakeholders of this project are:
      i. The Open Group

B. Team
   a. The project team will be drawn from members of The Open Group Security Forum and IT4IT™ Forum. The project leadership will be selected through the normal procedures of The Open Group.
   b. The Project Facilitator(s) will be Altaz Valani (representing the Security Forum) and Rob Akershoek (representing the IT4IT™ Forum).
   c. A liaison relationship will be created with the ABA Cyberspace Law Committee to facilitate regular feedback and input.

F. Project Methodology

This final section describes the project methodology, which includes:

A. Approach
   a. Creation of a charter.
B. Roadmap
   a. Identify relevant practices and standards as input (e.g., Open Fair, NIST, Zero Trust, ISO)
      i. Identify which practices are relevant
   b. Develop initial strawman model
   c. Create use cases or scenarios
   d. Analyze current security and risk management tooling landscape (and vendor landscape)
      i. Identify which tools are currently used
   e. Define a common ontology and taxonomy (e.g., threats, risks, audits)
      i. Determine data management
   f. Identify a number of end-to-end value streams (e.g., from vulnerability to remediation)
   g. Define initial draft security management capability model (with related data objects)
   h. Define security management tool reference model (defining the functions/application components) linked to the IT4IT reference architecture
C. Governance
   a. Governance of the initiative will be The Open Group standard policy and procedures
D. Approval
   a. Project deliverables will be approved by The Open Group. The project charter will be approved through the normal mechanism of The Open Group.