



**Information Security Integration Within the
Enterprise Reference Architecture Model**
Part 2 - Implementation

Guy B. Sereff
22 August 2013

About The Presenter

Guy B. Sereff

- Author, Speaker and Technology Practitioner
- Vice President / Enterprise Architecture
- Technology Industry Experience
 - *Application Research & Development (12 years)*
 - *Large-Scale Technology Management (8 years)*
 - *Global Enterprise Architecture (7 years)*
- Enterprise Architecture Domain Experience
 - *Business Architecture*
 - *Information Architecture*
 - *Application Architecture*
 - *Solution Architecture*
 - *Architecture Governance*
- Pragmatic Blend of Strategy and Tactical Execution



<http://www.linkedin.com/in/guysereff>

Agenda

Recap of Fundamental Definitions and Relationships

- Enterprise Architecture
- Information Security Architecture

Integrating Information Security into the Enterprise Reference Architecture Model

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

Recommended Next Steps

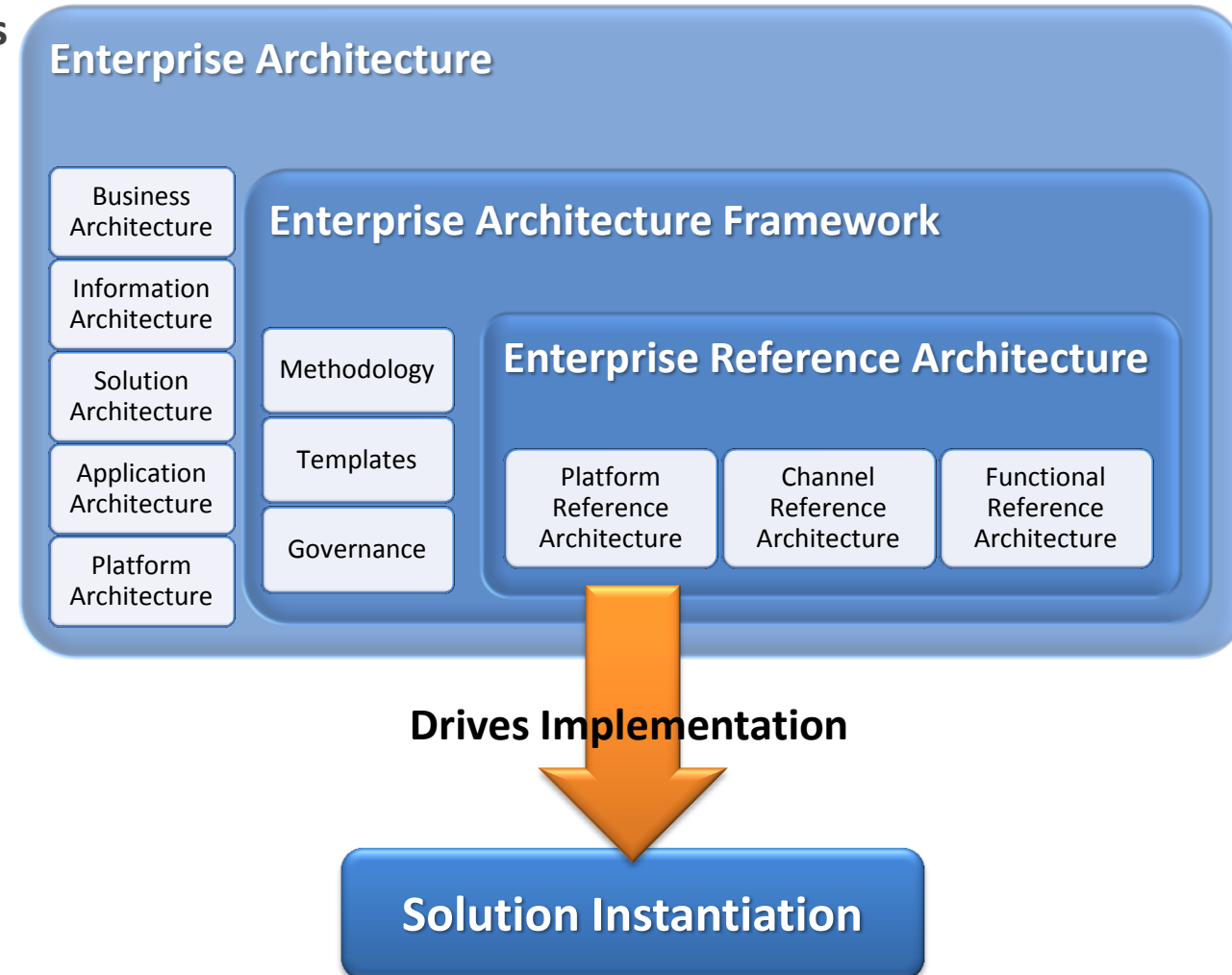
Questions and Comments



Recap: Enterprise Architecture

Strategy-Centric cross-cutting view of the organization's goals, objectives, existing capabilities, competitive advantages and external disruptive forces in order to formulate a strategy and align resources towards desired outcomes and objectives

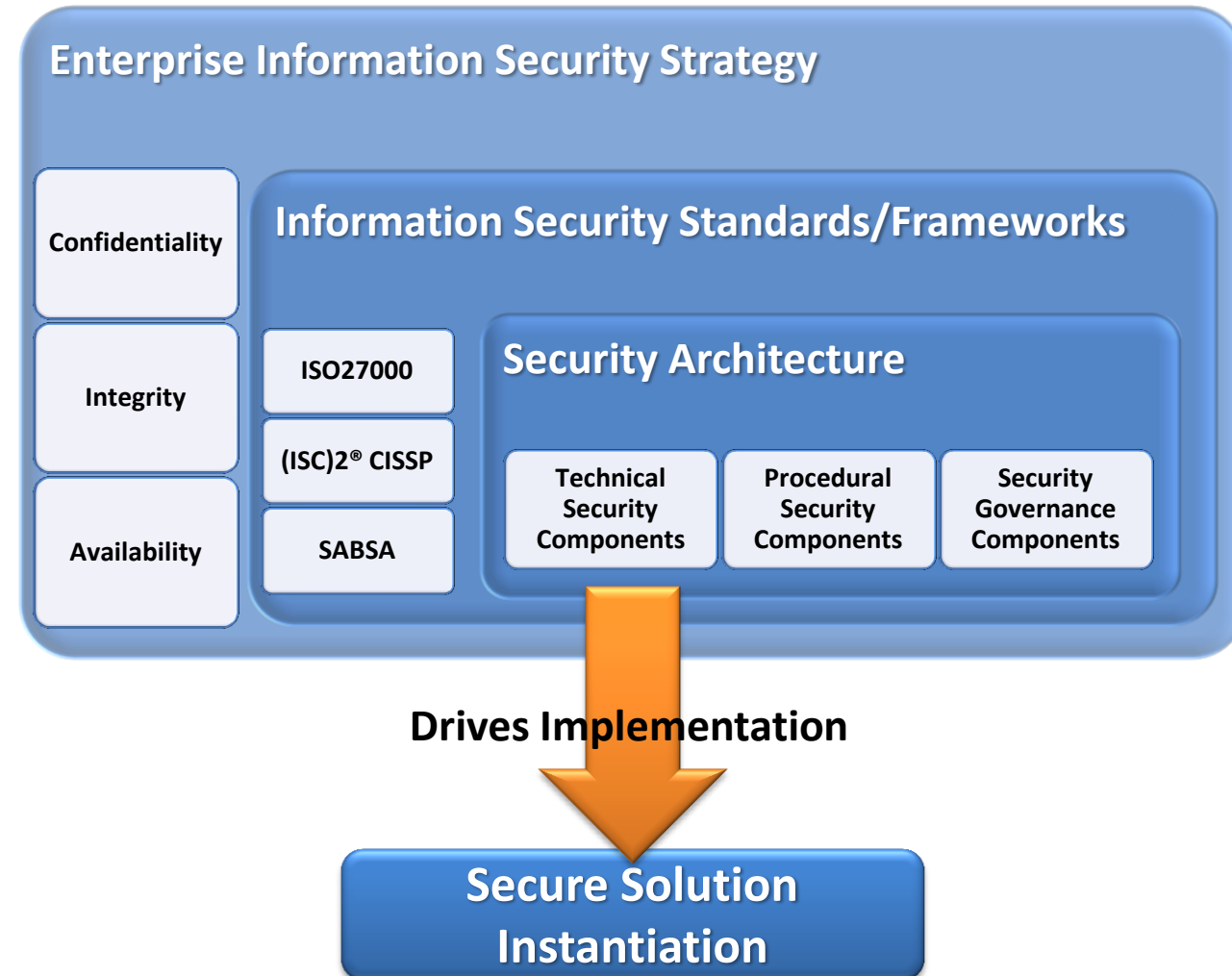
The purpose of **Enterprise Architecture** is to optimize across the enterprise the often fragmented legacy of processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the delivery of the business strategy.*



Recap: Enterprise Information Security Architecture

Risk-Centric view of Information Security across all aspects of the enterprise used to derive risk mitigation strategies, both from outside and within the organization's digital perimeter

Security is all about protecting business goals and assets. It means providing a set of business controls that are matched to business needs, which in turn are derived from an assessment and analysis of business risk. The objective in risk assessment is to prioritize risks so as to focus on those [risks] that most require mitigation.*



Enterprise Reference Architecture Model Security Integration

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



Reference Architecture

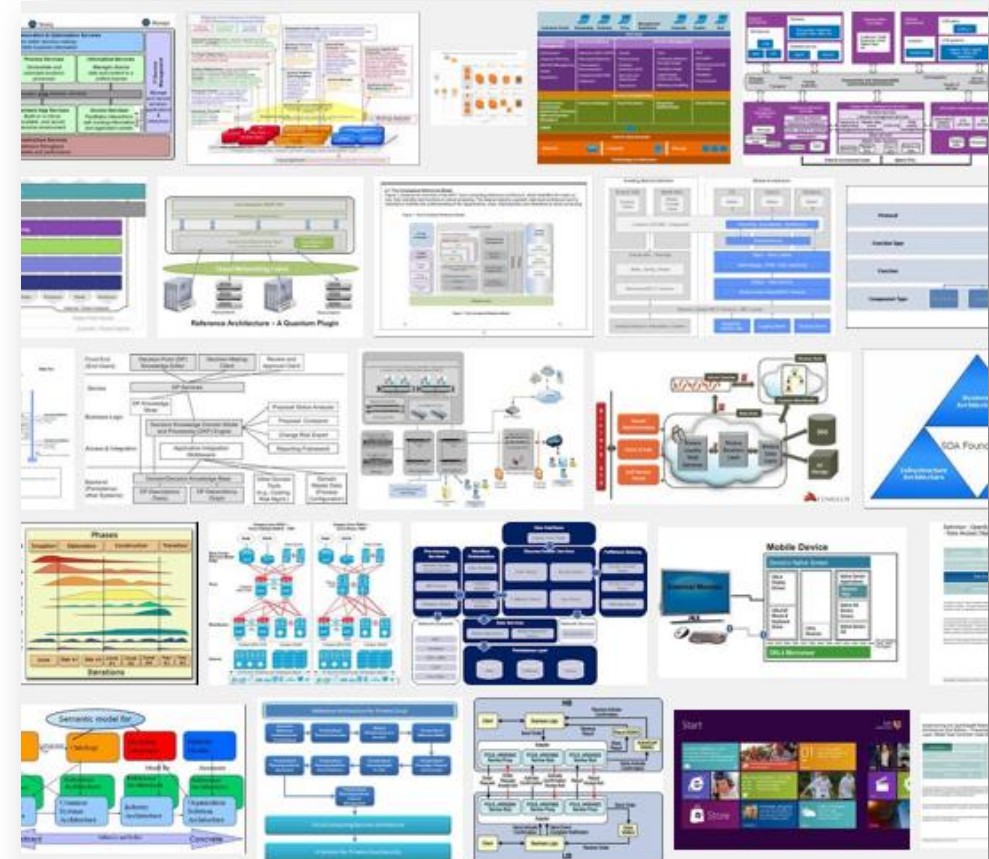
Pre-populated *Domain Reference Architecture Artifacts* published within the organization and available for anyone needing to deploy the capabilities captured within that domain

Wide variation in industry practices around what constitutes a Reference Architecture

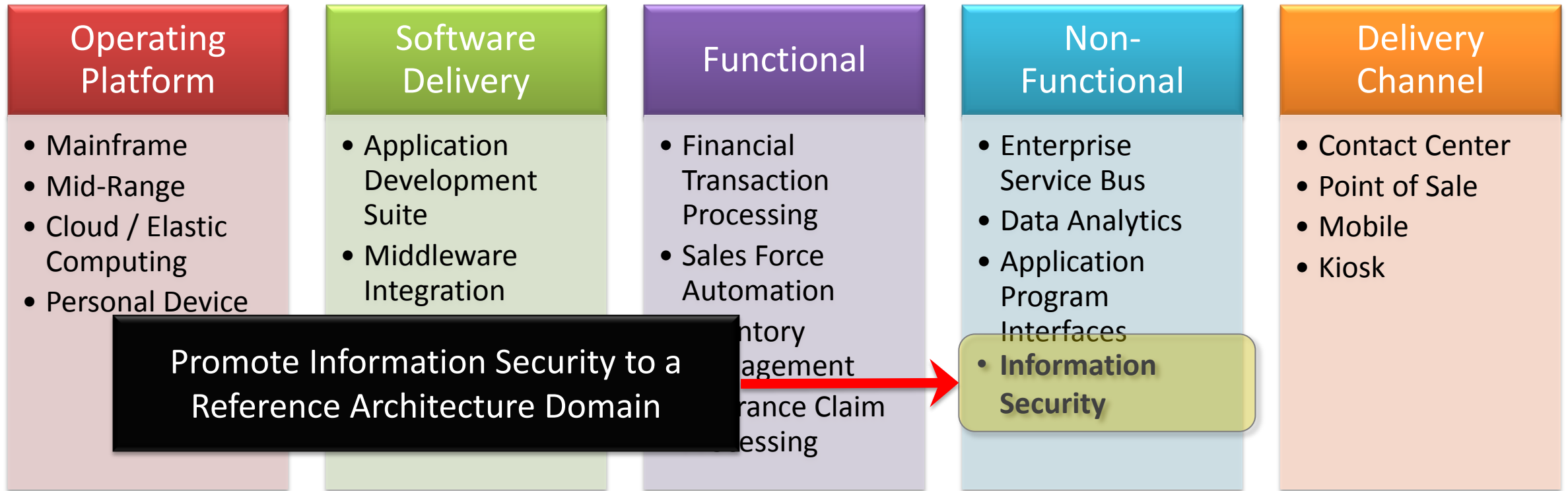
- Content and Meta Data
- Contextual Domains
- Level of Abstraction
- Level of Coverage
- Centralized Monarchy vs. Decentralized Federation
- Conformance Requirement

Templates can help structure / standardize content

Commercial Models and Templates available that can be adopted / adapted for use



Typical Reference Architecture Domains



IBM Security Blueprint Overview*

Business Security Reference Model

Governance, Risk,
Compliance

People & Identity

Date & Information

Application &
Process

IT Infrastructure:
Network, Server,
End Point

Physical
Infrastructure

Foundational Security Management

Software, System &
Service Assurance

Identity, Access &
Entitlement Mgmt

Date & Information
Protection Mgmt

Threat &
Vulnerability Mgmt

IT Service Mgmt

Command & Control
Mgmt

Security Policy
Mgmt

Risk & Compliance
Assessment

Physical Asset Mgmt

Security Services and Infrastructure

Security Info &
Event Infrastructure

Identity,
Access & Entitlement
Infrastructure

Security Policy
Infrastructure

Cryptography, Key &
Cert Infrastructure

Network Security

Storage Security

Host & Endpoint
Security

Application Security

Service Mgmt &
Process Automation

Physical Security

IT Security Services
& Mechanisms

Security Service
Level Objectives

Code, Images &
Designs

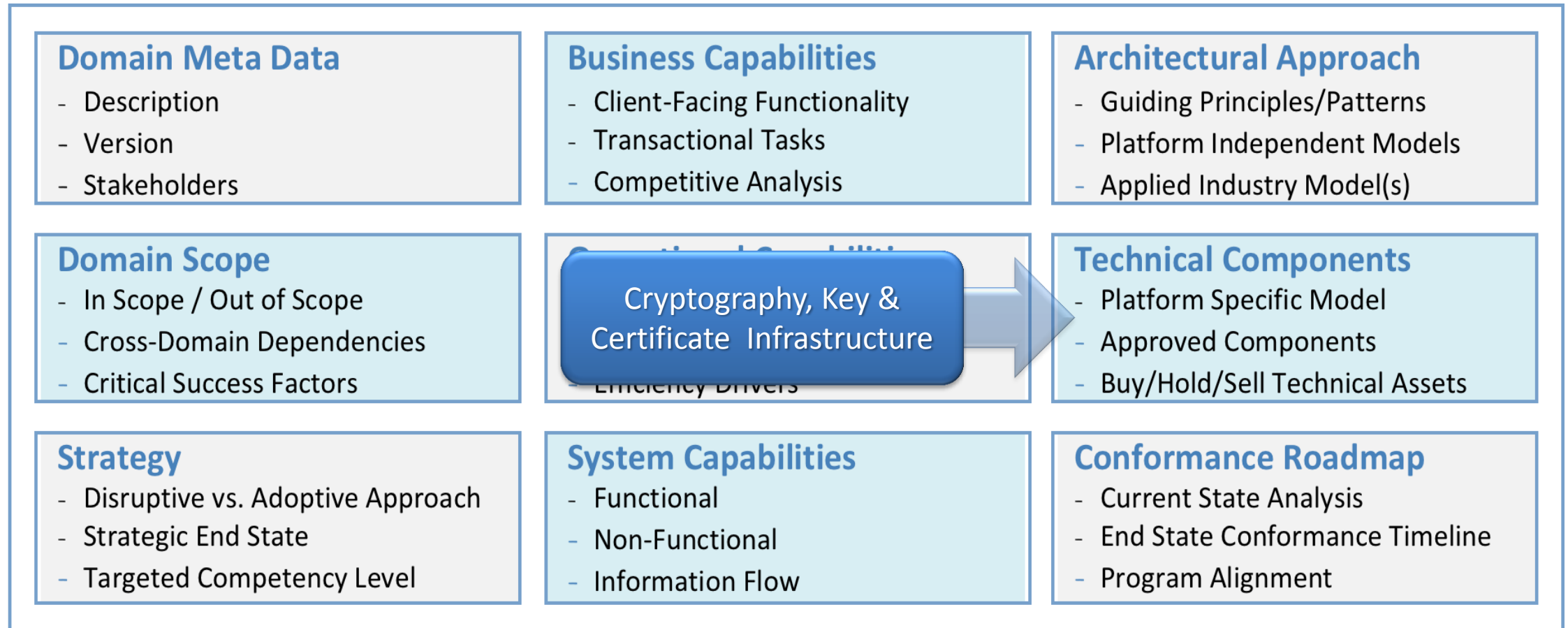
Policies, Config Info
and Registry

Identities &
Attributes /
Resources

Contents / Data

Security Events &
Logs

Common Reference Architecture Components



Enterprise Reference Architecture Model Security Integration

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



Add Information Security Considerations to all Domains

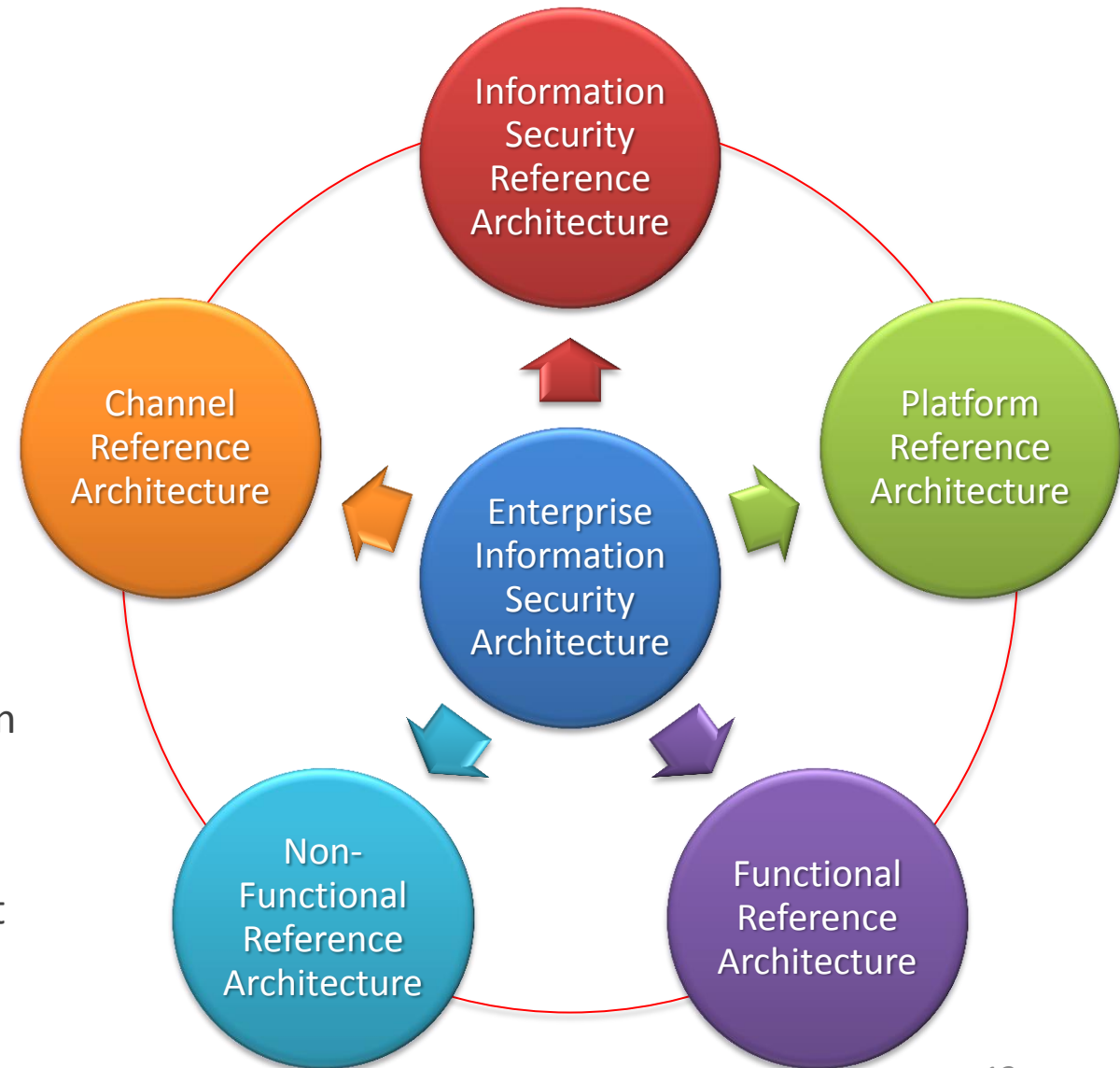
Having an Information Security Reference Architecture does not replace the need to address Information Security considerations across all other Reference Architecture domains

Having 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

- Move common security characteristics up into the broader Information Security domain
- Capture contextual security metadata within the domain reference architecture definition

TIP: Re-evaluate current Reference Architecture template Information Security considerations and refactor per current needs of the organization



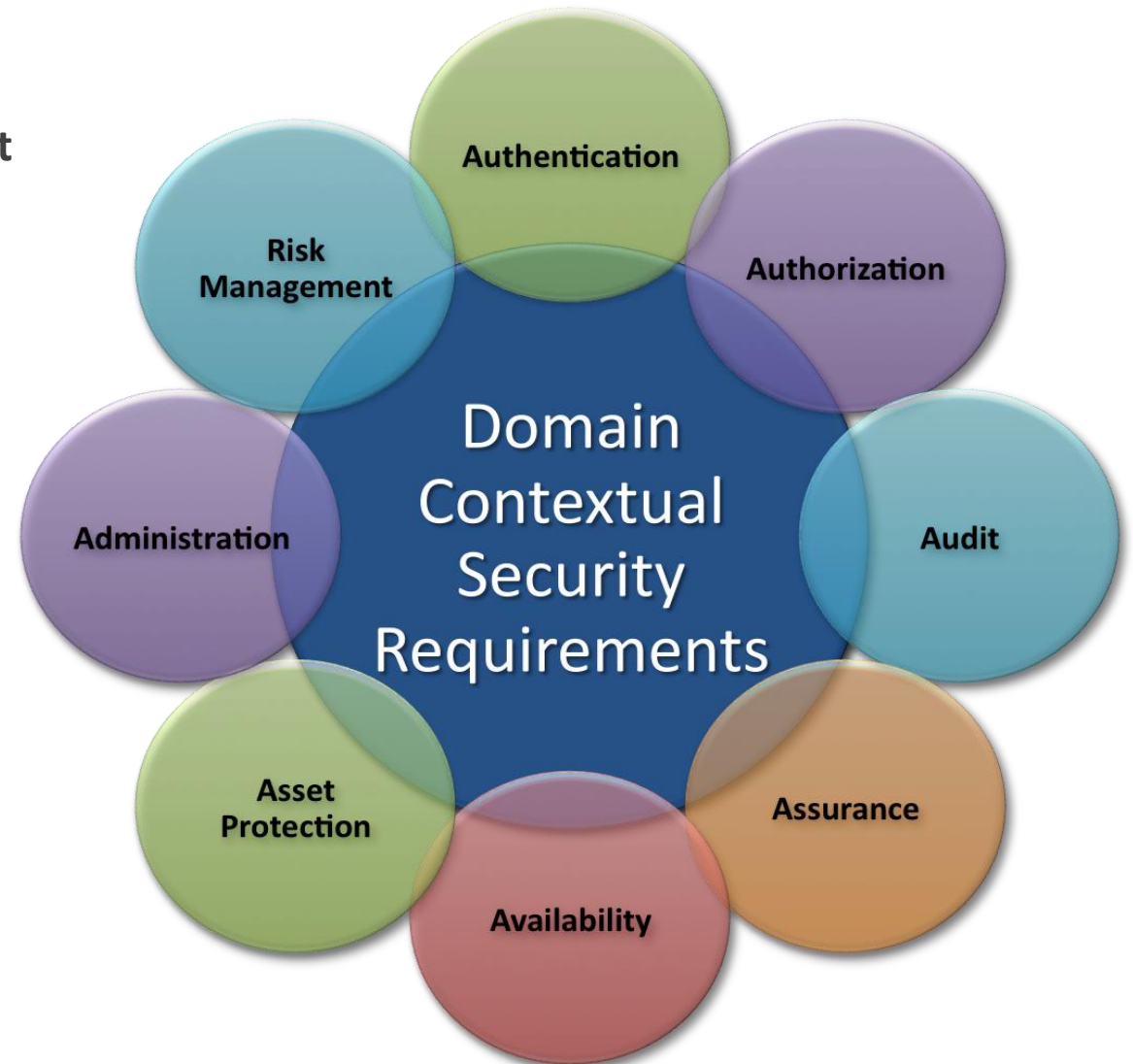
Adapt TOGAF®* Information Security Areas

One example would be to assess each Reference Architecture Domain against the TOGAF recommended list of Information Security Areas on a 2-Dimensional scale:

Applicability (*Applicable, Not Applicable*)

Compliance (*Compliant, Non-Compliant*)

- Authentication - *Identity Substantiation*
- Authorization – *Capability Enforcement*
- Audit – *Forensic Data Support*
- Assurance – *Policy Validation*
- Availability – *Functional Continuity*
- Asset Protection – *Prevention from Unauthorized use*
- Administration – *Policy Implementation*
- Risk Management – *Vulnerability Assessment*



Additional Reference Architecture Considerations

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

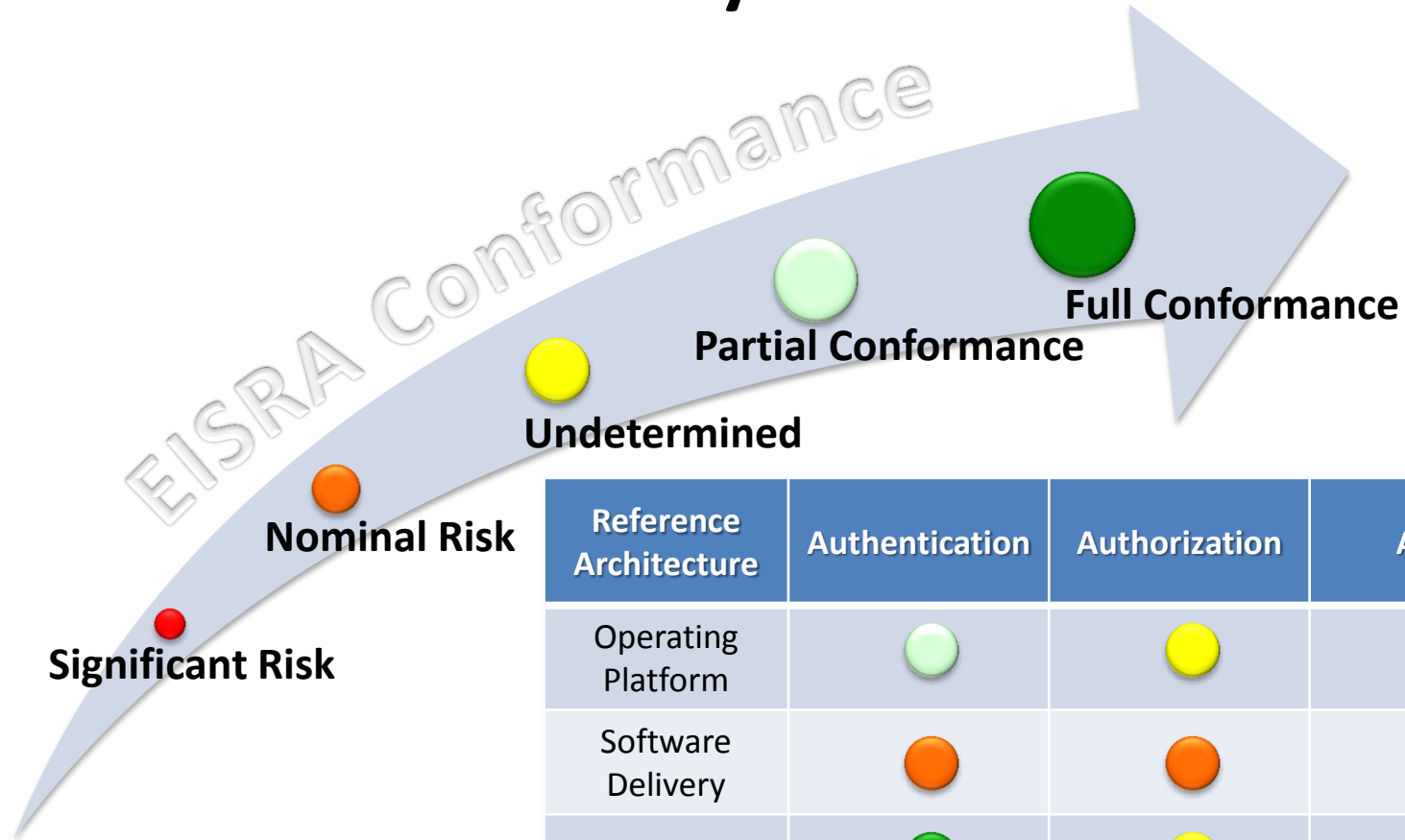
What are the Security Incident Metrics for this domain (i.e. Realized Risk Profile)?































- 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?



Information Security Assessment Heat Map



Reference Architecture	Authentication	Authorization	Audit	Assurance	Availability	...
Operating Platform						
Software Delivery						
Functional						
Non-Functional						
Delivery Channel						

Enterprise Reference Architecture Model Security Integration

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



Integrate Information Security Into the Delivery Process

Six Sigma taught us not to inspect quality in something after the work has been done but to build quality into the process to begin with - the same holds true for Information Security

Don't wait to review Quality Assurance (QA) results or Vulnerability Assessment (VA) findings to see if Information Security considerations were cared for

Problems found late in the delivery 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

Information Security considerations must be explicitly cared for and validated at each milestone throughout the entire Systems Development Life Cycle (SDLC)

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;
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.*

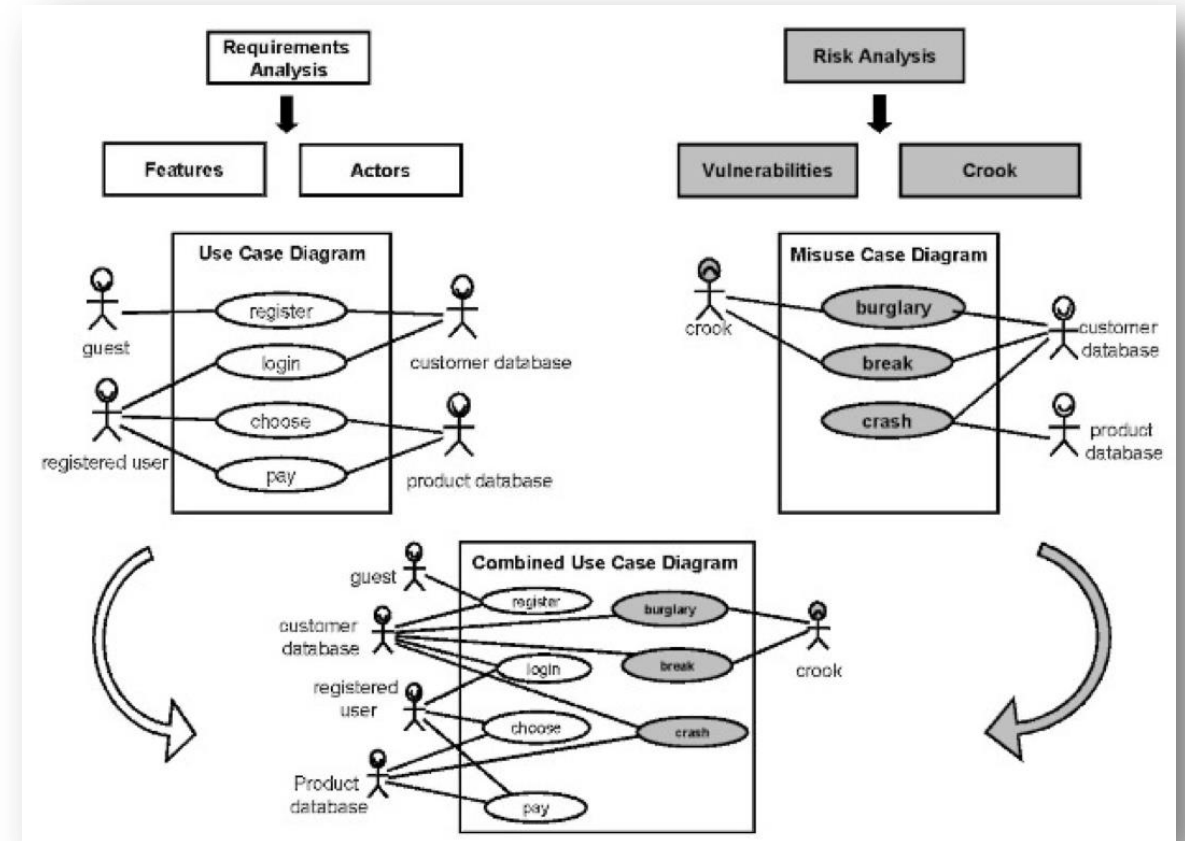
CORAS Model-Based Risk Assessment*

Most requirement gathering efforts focus on 'happy path' use cases, hoping to cram as many business capabilities into the release window as possible

Model Based Security Analysis is an approach that seeks to identify and model mis-functionality and misuse cases early on in the definition phase

CORAS Model-Based Risk Assessment method is designed to provide model-driven analysis of critical security components

- Context Identification
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment



Secure Quality Requirements Engineering

Information Security becomes very difficult to replace or significantly enhance once its host application makes its way into the production

Software Engineering Institute (SEI) established the *Security Quality Requirements Engineering (SQUARE)* approach in an effort to move security considerations further forward in the delivery life cycle*

Nine-Step Approach that identifies Inputs, Technologies, Participants and Outputs

SQUARE could be overlaid against most SDLC models to orchestrate security element integration with minimal disruption to existing processes

	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	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

TOGAF® Architecture Contract*

Architecture Contracts are agreements between the architecture community and the various constituents tasked with solution delivery for architecturally significant efforts

Adapt the Architecture Contract process to specifically address Information Security design elements and their alignment to the Enterprise Information Security Reference Architecture

Create and ratify the Information Security aspects of the Architecture Contract before solution design begins

Validate solution conformance to the Information Security Architecture Contract aspects before production load authorization is granted



Best Practices:

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
3. Create a governance model that holds participants accountable for delivering secure solutions aligned to the Information Security Reference Architecture model



Enterprise Reference Architecture Model Security Integration

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



Audit Information Security Architecture Alignment

Most organizations have some form of an Information Security Audit and Control process in place, testing various aspects of policy adherence and enforcement around the institution

Go a step beyond to audit significant projects, programs and initiatives against the prevailing Information Security Reference Architecture model

Use findings to educate and address recurring patterns of non-conformance as well as assess the level of difficulty in implementing the Information Security Reference Architecture

Integrate additional post-design Reference Architecture conformance testing specifically calculated to validate Information Security Reference Architecture adherence

Benefits from an effective Information Security Governance and Audit Practice*:

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

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

C-I-A Triad: Confidentiality, Integrity, Availability*

The C-I-A Triad consists of:

- Confidentiality
Protection from Unauthorized Access
- Integrity
Assurance of Completeness / Correctness
- Availability
Effective and Efficient Operational Support

C-I-A Triad can be adapted into an assessment of an application's alignment to the Enterprise Information Security Reference Architecture Model

- Validate the reference architecture itself
- Validate the solution being compared to the reference architecture

Deviation scores reflect the number of deployed elements that differ from their corresponding approved elements

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

ITIL Security Management Evaluation Process*

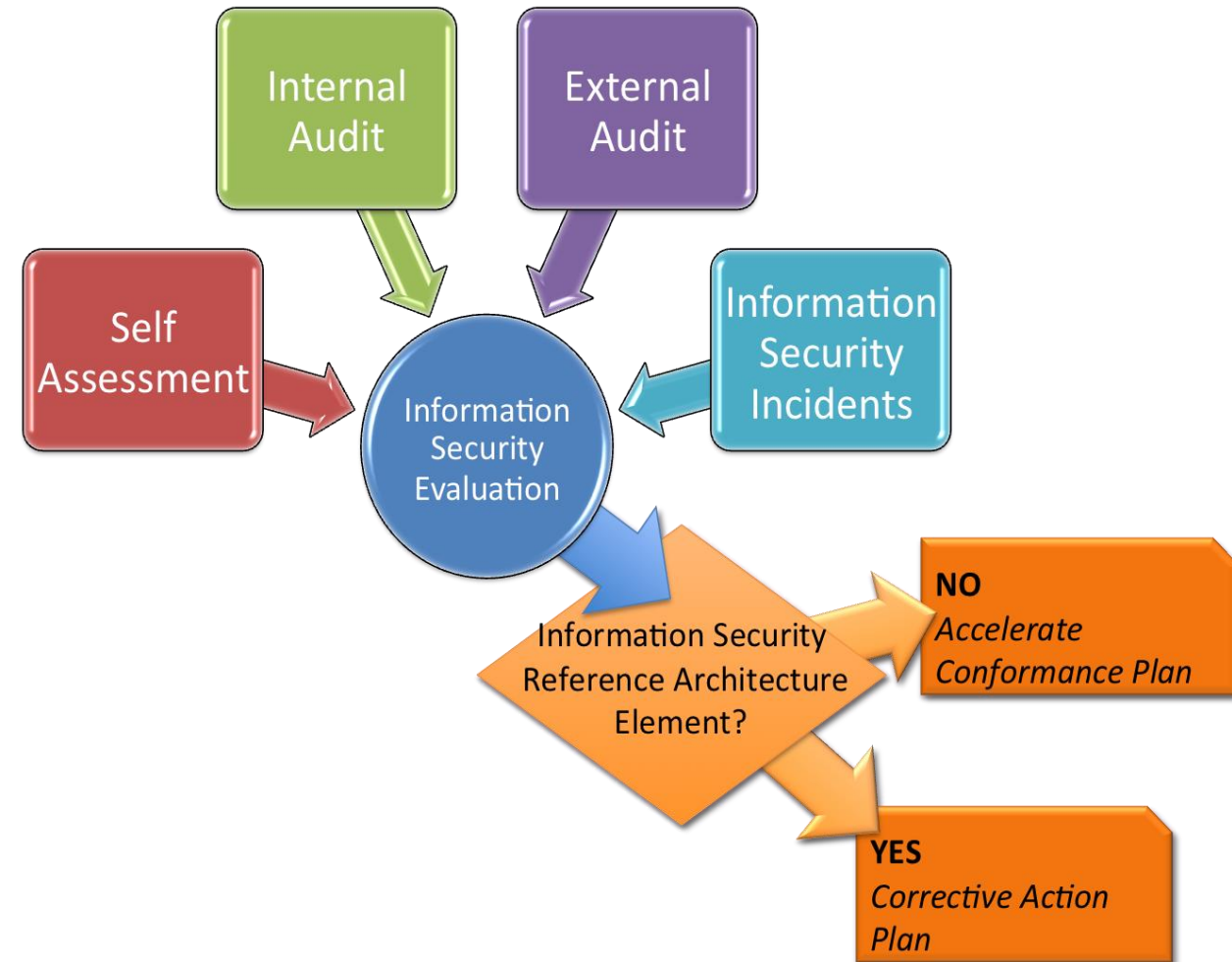
Multi-faceted evaluation approach related to Implementation (Self Assessment, Internal Audit, External Audit) and Operation (Security Event Logging)

Extend ITIL process to analyze findings to determine if incident involved an Information Security Reference Architecture element

- Yes: Corrective Action Plan to address the Reference Architecture
- No: Accelerate Information Security Reference Architecture conformance velocity

Two-fold benefit:

- Accelerates Information Security Reference Architecture adoption
- Establishes a pattern of continuous improvement by hardening the shell and providing insight into how well the Information Security components are performing



Recommended Next Steps

- 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



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.

Any Questions?



in Orbus Software Group

 **@OrbusSoftware**



Download this presentation and accompanying white paper from:
www.orbussoftware.com/downloads

Thank You!