

# The South African EA Forum

The EA Forum is a networking event sponsored by The Open Group in South Africa. It started in 2004 and is hosted every second month or so, with events in Durban, Johannesburg and Cape Town. At the EA Forum, industry leaders share their experiences and knowledge of architecture and related topics. Real-world case studies highlight how business problems are solved using the discipline and practice of architecture. The event is also an opportunity for the architecture community members to network and collaborate.

For more information or to submit your presentation topics please contact [Stuart Macgregor](#)



Subscribe to our  
EA FORUM  
DATABASE

Follow the EA Forum  
on Twitter...

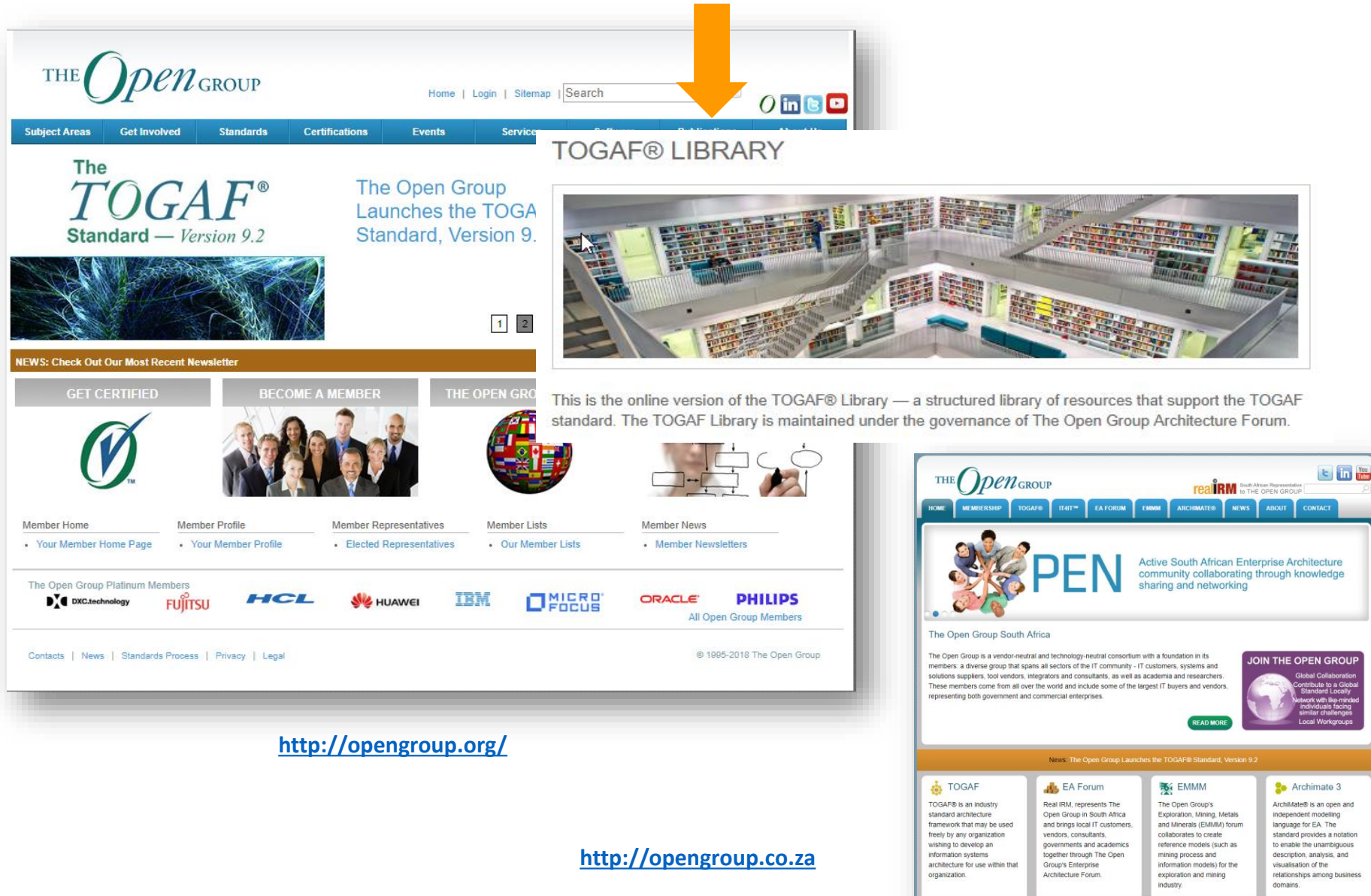
Our upcoming  
events

Twitter: @EAforumSA  
#ogza



<http://opengroup.co.za/ea-forum>

# Leading the development of open, vendor-neutral IT standards and certifications



The screenshot displays the main website of The Open Group, which is dedicated to IT standards and certifications. An orange arrow points to the 'TOGAF® LIBRARY' section. The page features a navigation bar with links to 'Subject Areas', 'Get Involved', 'Standards', 'Certifications', 'Events', and 'Services'. A prominent banner for 'The TOGAF® Standard — Version 9.2' is shown, along with a news item about the launch of the TOGAF Standard, Version 9. Below this, there are sections for 'GET CERTIFIED', 'BECOME A MEMBER', and 'THE OPEN GROUP'. The 'GET CERTIFIED' section includes a logo and links to 'Member Home', 'Member Profile', 'Member Representatives', 'Member Lists', and 'Member News'. The 'BECOME A MEMBER' section features a group photo of members. The 'THE OPEN GROUP' section includes a globe icon and a link to 'Our Member Lists'. A large image of a library interior is shown, with a caption stating: 'This is the online version of the TOGAF® Library — a structured library of resources that support the TOGAF standard. The TOGAF Library is maintained under the governance of The Open Group Architecture Forum.' Below the library image, there is a section for 'The Open Group Platinum Members' featuring logos for DXC technology, FUJITSU, HCL, HUAWEI, IBM, MICRO FOCUS, ORACLE, and PHILIPS. The footer includes links for 'Contacts', 'News', 'Standards Process', 'Privacy', and 'Legal', along with the copyright notice '© 1995-2018 The Open Group'.

<http://opengroup.org/>

<http://opengroup.co.za>

The screenshot also shows a secondary page for 'The Open Group South Africa' (PEN). This page features a navigation bar with links to 'HOME', 'MEMBERSHIP', 'TOGAF®', 'IT4IT™', 'EA FORUM', 'EMMM', 'ARCHIMATE®', 'NEWS', 'ABOUT', and 'CONTACT'. The main content area includes a large image of a group of people and the text 'PEN Active South African Enterprise Architecture community collaborating through knowledge sharing and networking'. Below this, there is a section for 'The Open Group South Africa' and a 'JOIN THE OPEN GROUP' button. The footer of this page includes a news item: 'News: The Open Group Launches the TOGAF® Standard, Version 9.2'. The footer also features a grid of links to 'TOGAF', 'EA Forum', 'EMMM', and 'Archimate 3', each with a brief description of the standard.



#### Upcoming Events

Digital in Practice and the Supply Chain, January 28th - 31st in Scottsdale 2019

#### Latest Announcements

Announcing a New Snapshot - The Digital Practitioner Body of Knowledge™

#### The Open Group Blog

Design Thinking for Enterprise Architects – A Conversation with Mayank Saxena

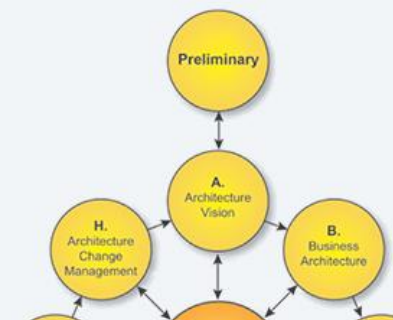
## The Open Group: Making Standards Work®

The Open Group works with customers and suppliers of technology products and services, and with consortia and other standards organizations to capture, clarify, and integrate current and emerging requirements, establish standards and policies, and share best practices. Our standards ensure openness, interoperability, and consensus.

[Learn More](#)

## The TOGAF® Standard, a standard of The Open Group

The TOGAF® Standard, a standard of The Open Group, is a proven Enterprise Architecture methodology and framework used by the world's leading organizations to improve business efficiency.



## Security-by-Design in Enterprise Architecture

Prof. Dr. Ernest Ketcha Ngassam / Ngoie Wandelewe / Frans Sauermann

The strategic importance of Information Security for organisations is gaining momentum. The current surge in cyber threats is compelling organisations to invest in information security to protect their assets. Rushing to protect assets often comes with the expense of excessive technology adoption without a valid strategic foundation. Enterprise Security Architecture is geared to address these issues, but is frequently misaligned with Enterprise Architecture.

At this month's EA Forum, we will explore avenues for the adoption and enforcement of Security-By-Design in the Enterprise Architecture value-chain so as position Risk, Security and IT as true business enablers.

**Prof. Dr. Ernest Ketcha Ngassam** is the General Manager: Information Security Architecture and Technical Excellence at MTN Group. He is also Professor Extraordinaire of Computer Science at the School of Computing, UNISA, and holds a PhD in Computer Science from the University of Pretoria.

**Ngoie Wandelewe** is the Solutions/Enterprise Architect - Strategy & Business Development where he designed the Technology and Strategy Road map. He is reviewing current system security measures and recommending and implementing enhancements to the Architectural design to be used across 22 countries

**Frans Sauermann** is the Senior Manager: Information Systems Security Architecture at MTN Group. He holds 25 certifications related to information security architecture from The Open Group, SABSA, ISACA, ISC^2, AXELOS, PMI, Cloud security alliance and others. He has over 14 years of experience in information security, 10 of which were spent with MTN.

# What we will be going through

---

Pick one:

- A. Do whole talk first then questions
- B. Questions while on discussion point
- C. Jump between discussion points until time runs out
- D. Corner me after the talk

By all means, differing opinions and backgrounds make us learn from each other

1

- **Introduction**

- Enterprise Architecture
- Enterprise Security Architecture
- Security by Design
- Stakeholder (CIO, CISO)

2

- **Problem Statement**

- EA Limitation
- ESA Limitation
- Stakeholder Conflict

3

- **Security By Design – ESA**

- EA, ESA, SRA & SSA
- EA Metamodel & Practice
- End goal of ESA & Practice

4

- **Conclusion**

The background of the slide is a yellow world map. Overlaid on the map is a complex network of dark grey lines and dots, representing a global communication or data network. The dots are of varying sizes, and some have concentric circles around them, suggesting nodes or hubs in the network. The network lines connect these nodes across all continents.

Enterprise Architecture (EA)  
Enterprise Security Architecture (ESA)  
Security by Design (SbD)

# Introducing EA,ESA, SbD - Definition

## Enterprise Architecture (EA)

- Formal and structured way of viewing and defining enterprise
- Aligns business vision with IT
- Builds transformative capabilities from people, processes, technology, and information

## Enterprise Security Architecture (ESA)

- Provides guidelines as services, models and standards to achieve the overall enterprise security strategy
- Translates business vision and strategy into effective enterprise security

# Introducing EA,ESA, SbD - Definition

## Security by Design (SbD)

- Formalize infrastructure design and automate security controls to enable building security into every part of IT
- Improving capability to develop secure products
- Enabling security capabilities - instead of auditing security into a system
- Includes build and operations phases



# Problem Statement

# CIO & CISO Conflicting Goals?

## CIO

- Information systems and digital management focus.
- Supports business with technology solutions.
- Helps businesses modernize legacy solutions/processes
- Positions IT as an enabler within the organization
- Typically ensures EA is practiced within the organization

## CISO

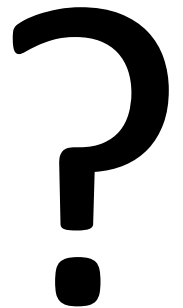
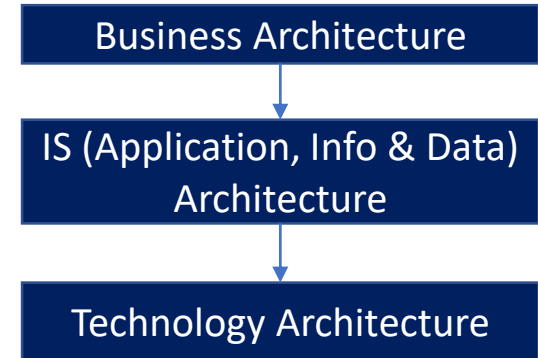
- Information security risk and compliance focus.
- Supports business with frameworks to properly govern, evaluate, and respond to risks.
- Partially takes ownership of security toolset
- Position Security capabilities as a business enabler

# Traditional EA

- Metamodel has no Risk and Security elements and relationships
- Solution architects consider risk and security as non-functional requirements
- Risk and security teams involved in projects post-solution design

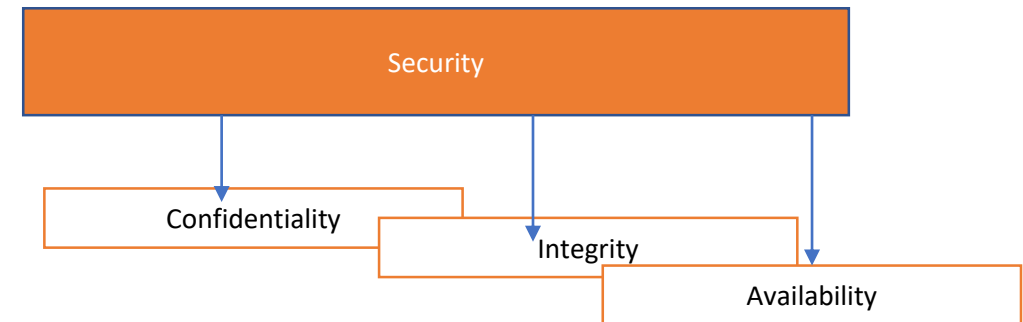
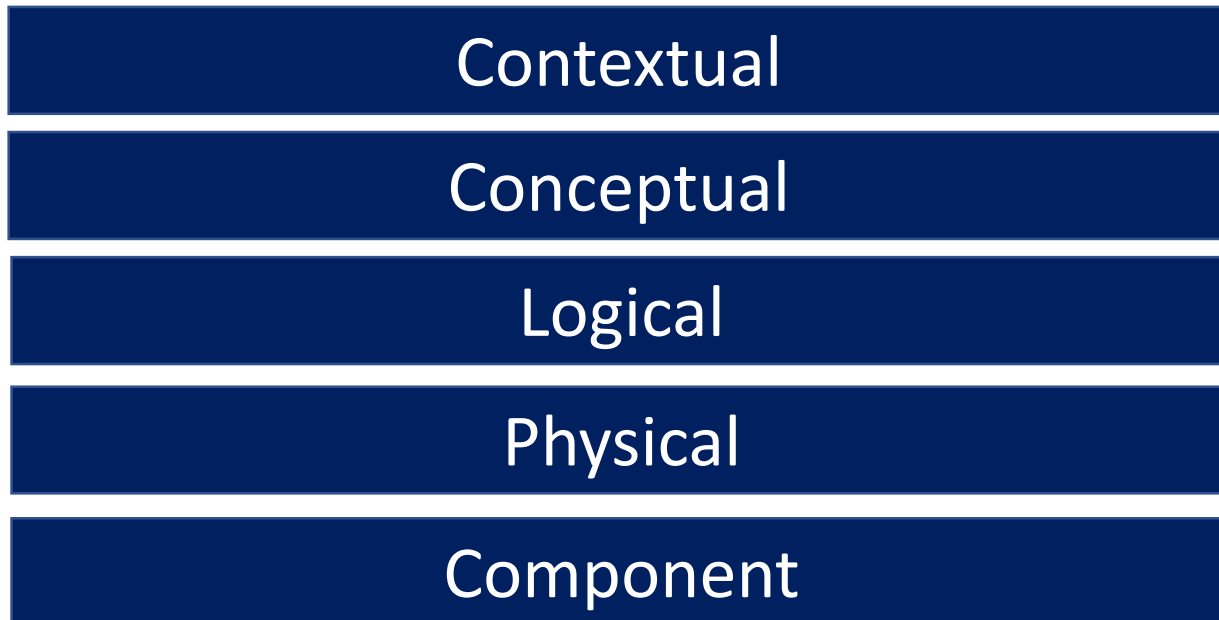
## Missing information security aspects

- Understanding risks and the assets exposed to risks
- Choosing correct risk assessment methods and management processes
- Integrating Security and Risk Management into the EA practice
- Generating appropriate views for demonstrating Compliance
- Vulnerabilities and threats landscape
- Design patterns, mechanisms and services used to mitigate risk and implement controls
- Defining a complete implementation and change roadmap at enterprise level



# Traditional Security Architecture

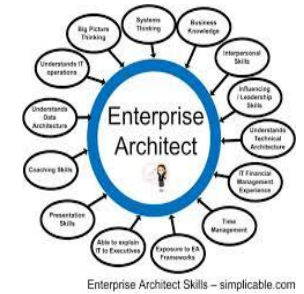
- Typically independent approach from EA
- Security architecture document typically the last document deliverable post data, application, and technology architectures
- Frequently, security aspects of a system are analyzed and designed separately



# Key role updates

## Enterprise Architect

- Ensure full integration of Security and Risk in the Architecture Value Chain
- Integrate new changes in the EA repository.
- Update changes in metamodel relationships and concepts
- Ensures security and risk support business strategy and objectives.



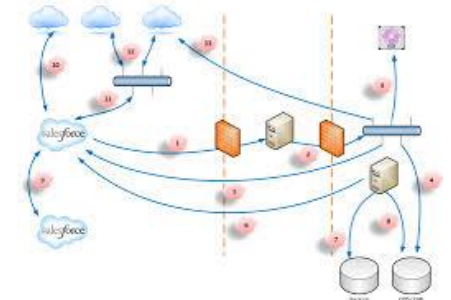
## Solution Architect

- Embeds Security Design Patterns into the solution in collaboration with the Security Solution Architect if necessary
- Sign off Solution Design and UAT

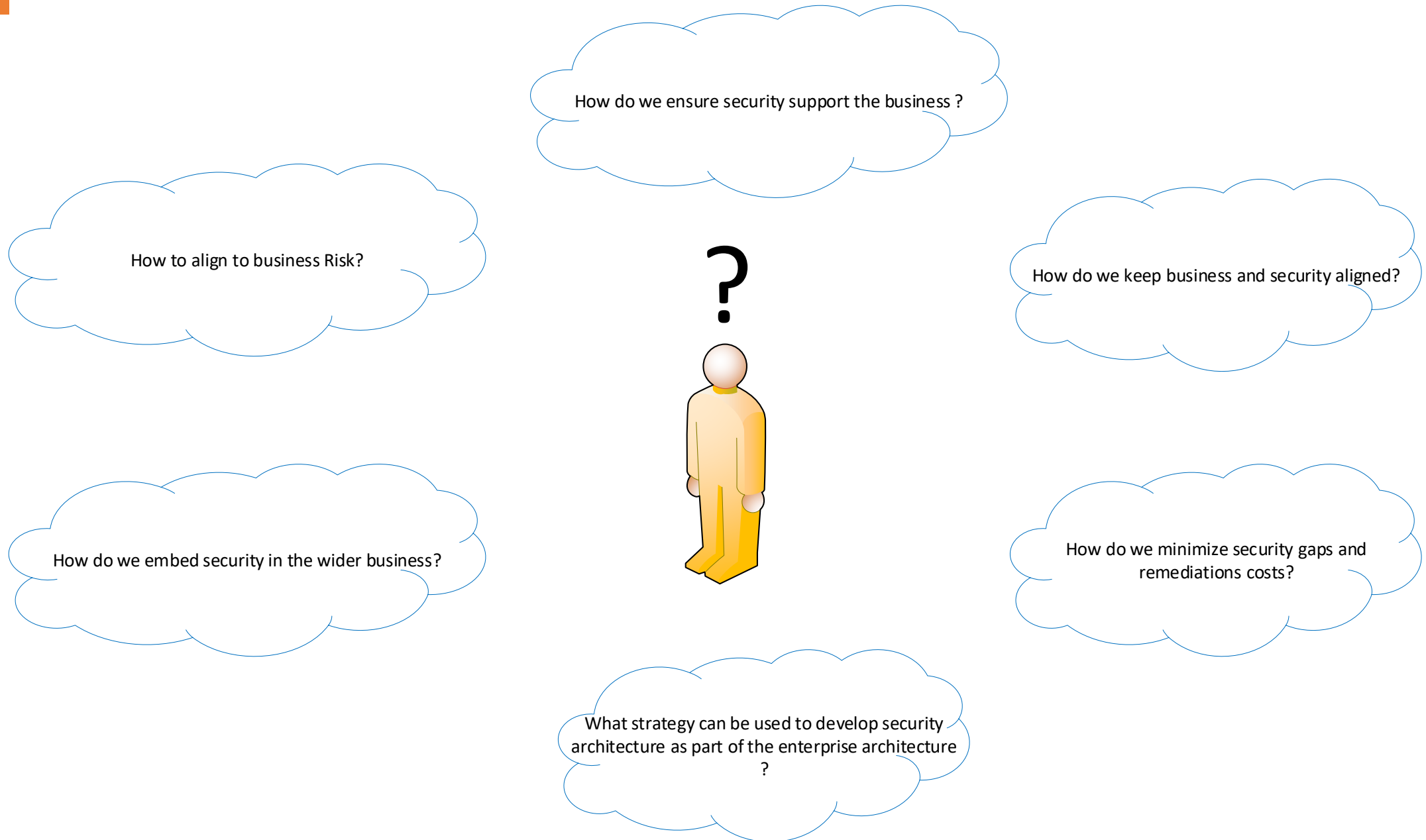


## Security Solution Architect

- Capture security requirements
- Update risk, threats, vulnerability catalogues and relationships in EA repository
- Define and populate Security Design Patterns in architecture repository
- Vet IT Solution Architectures from a Security perspective
- Use Solution Risk Assessment for new design patterns
- Co-signatory on Solution Design UAT



# Questions to be addressed



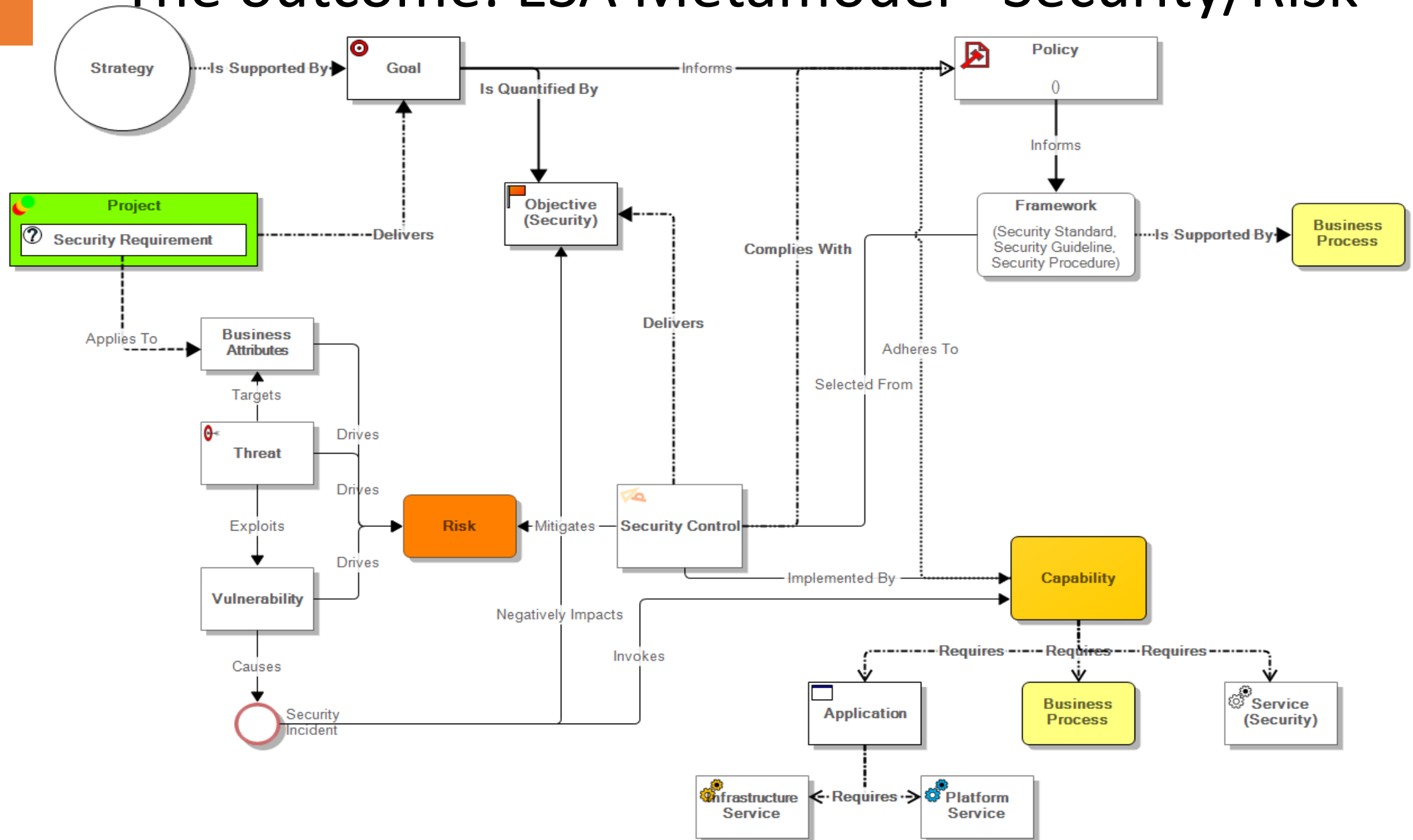
The background of the slide is a yellow world map. Overlaid on the map is a complex network of black dots (nodes) connected by thin black lines (edges). The nodes are distributed across all continents, with a higher density in North America and Europe. Some nodes are highlighted with concentric circles, suggesting a central or hub status. The network lines crisscross the globe, creating a web-like pattern that represents global connectivity.

# Security by Design

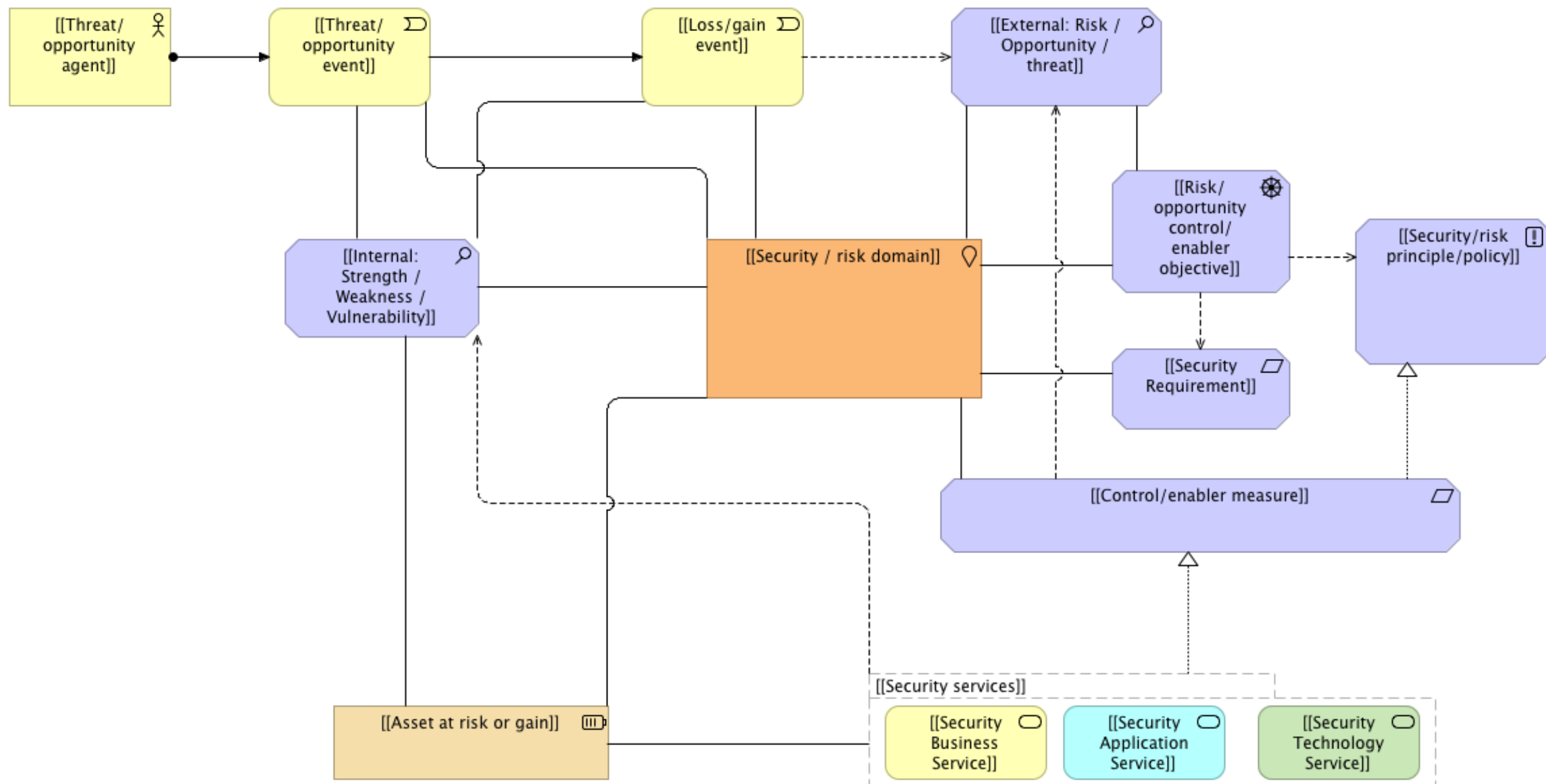




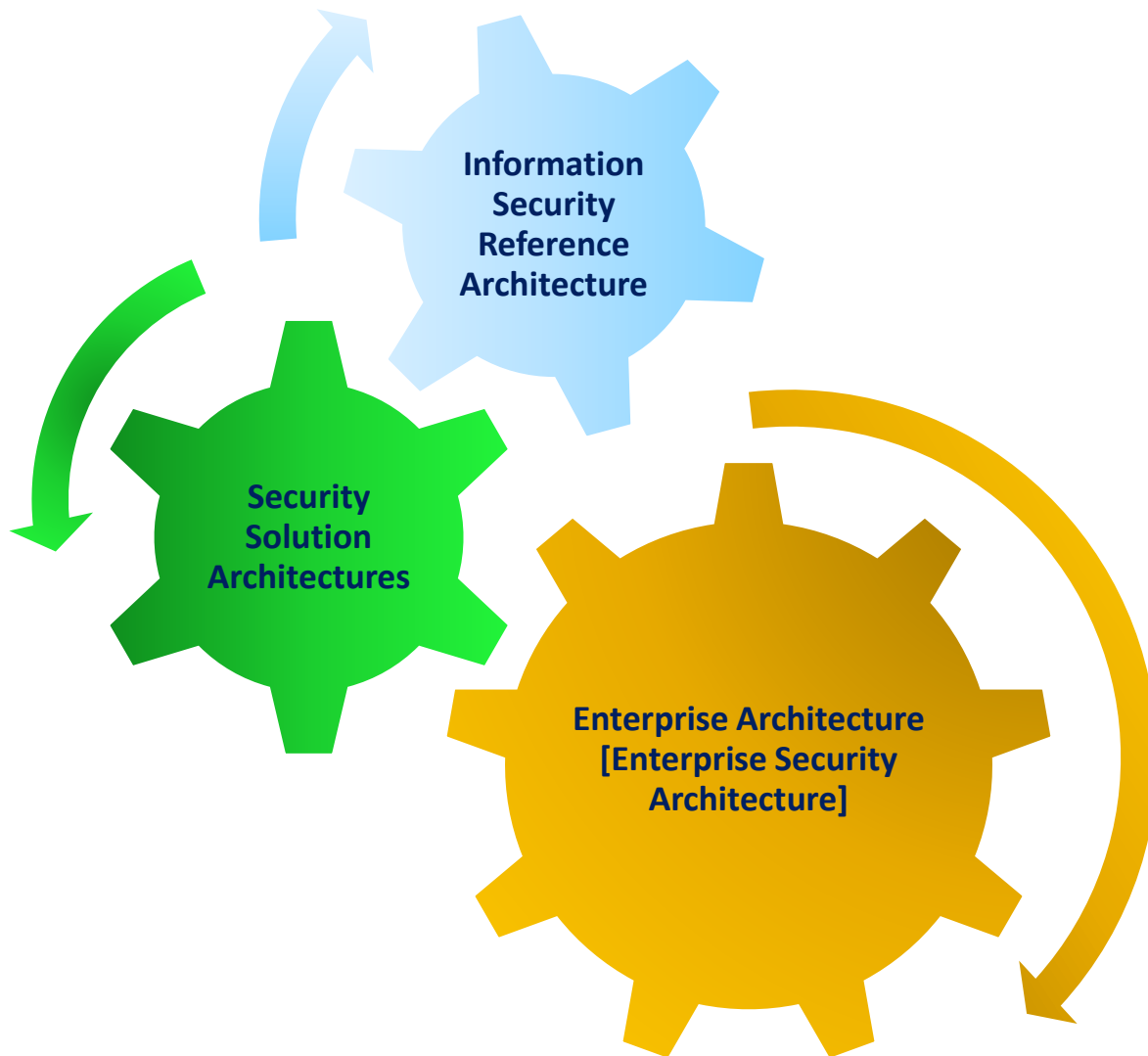
# The outcome: ESA Metamodel - Security/Risk



# Future dreams: Archimate alignment



# Security by Design – ESA, SRA, SSA

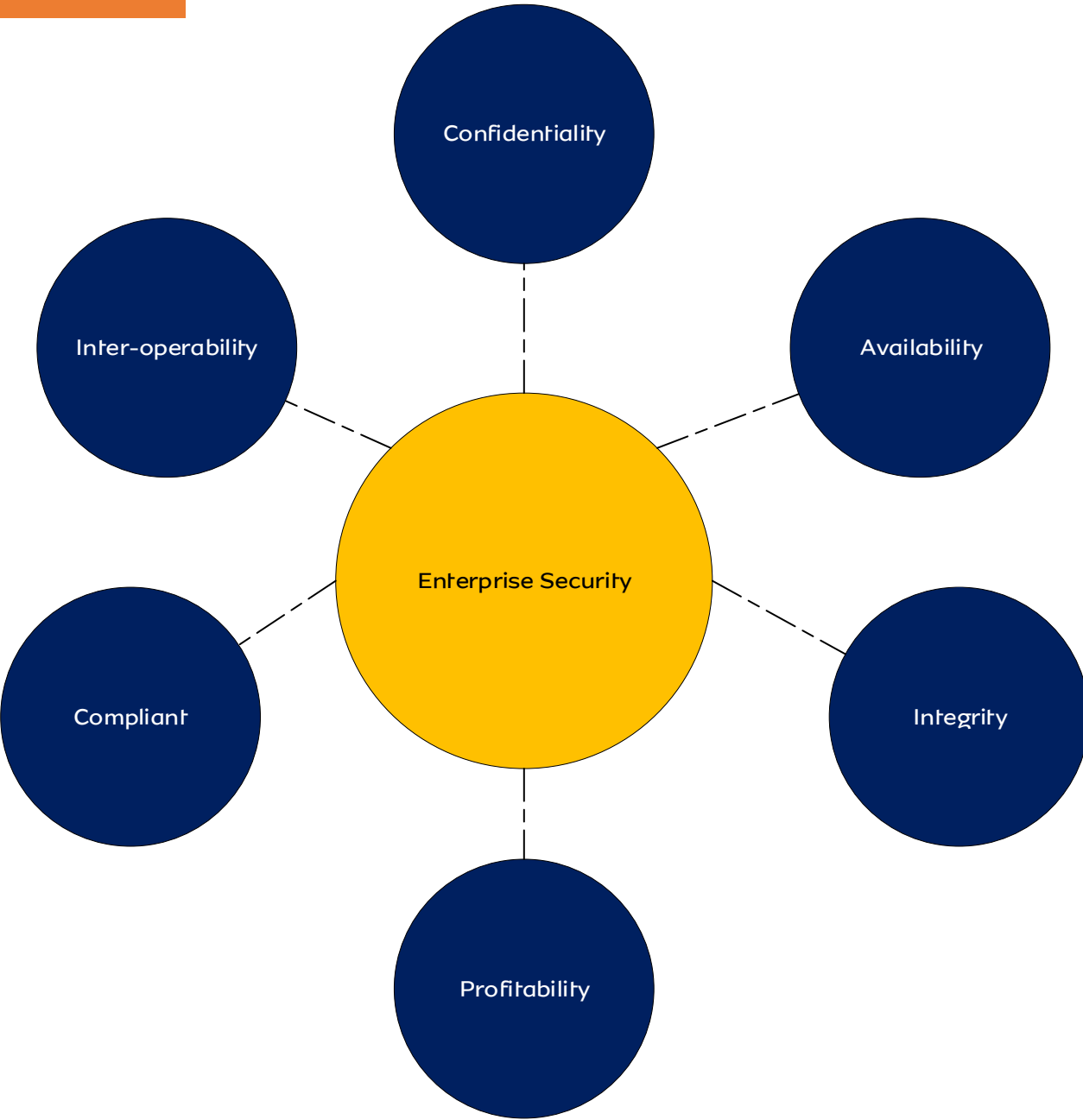


- Business and Risk-Driven approach
- Traceability for completeness & Justification
- Reusability of patterns, solutions and technologies
- Business value & cost to support/enable a strategy

- Blueprint of reference for Solution Architects
- Includes policies, controls, procedure and guidelines
- Enforce the use of Design Patterns
- Vetted and approved as part of the established governance framework

- Understand business requirements and risks
- Articulate security requirements: Core and Generic
- Make use of patterns from Reference Architecture
- Vet design, implementation & acceptance testing

# End Goal in EA & ESA: Capabilities enablement



Value-assured

Prioritized & proportional responses

Scalable scope

Agility - ease of implementation & management

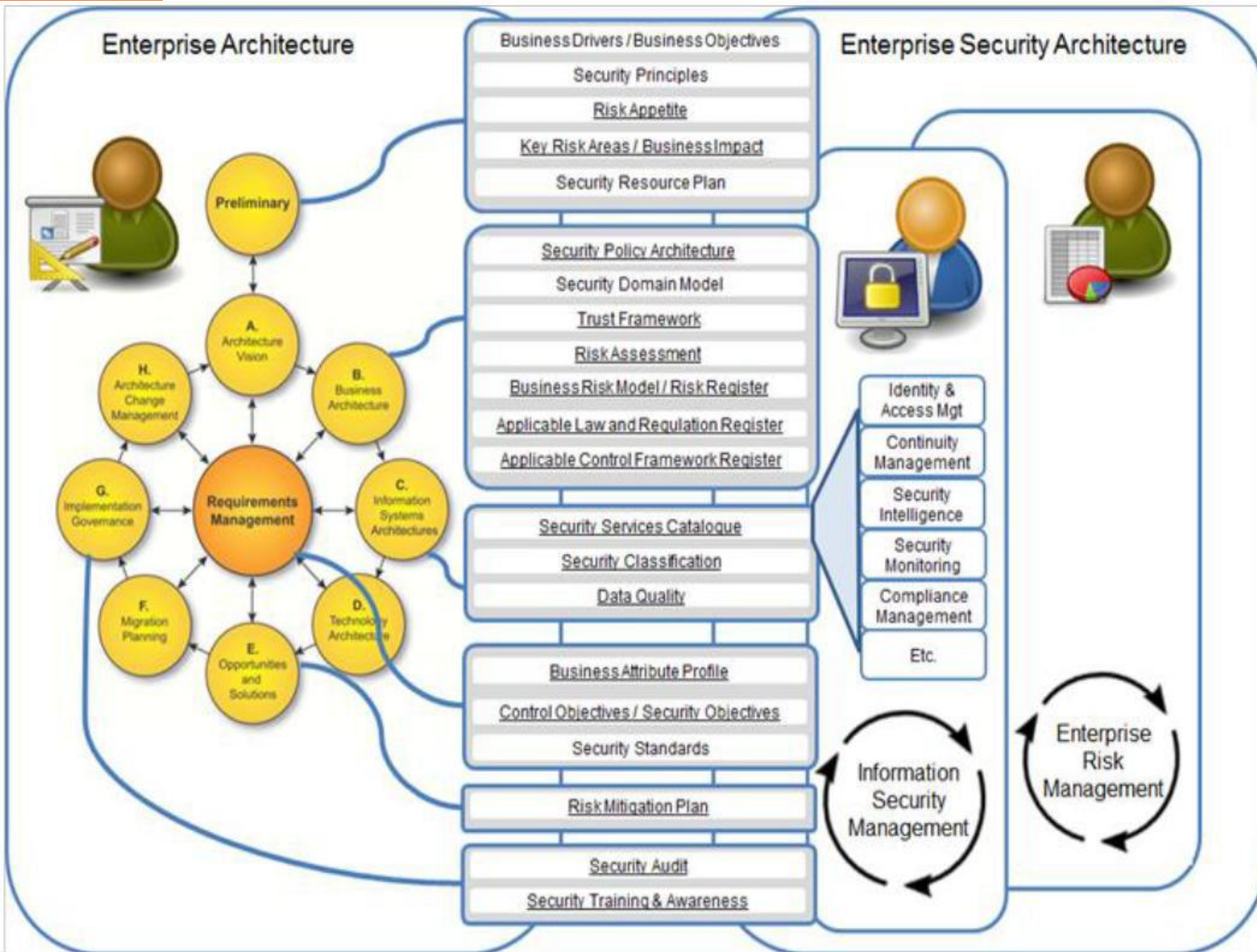
Free use, open source, global standard

Demonstrates compliance

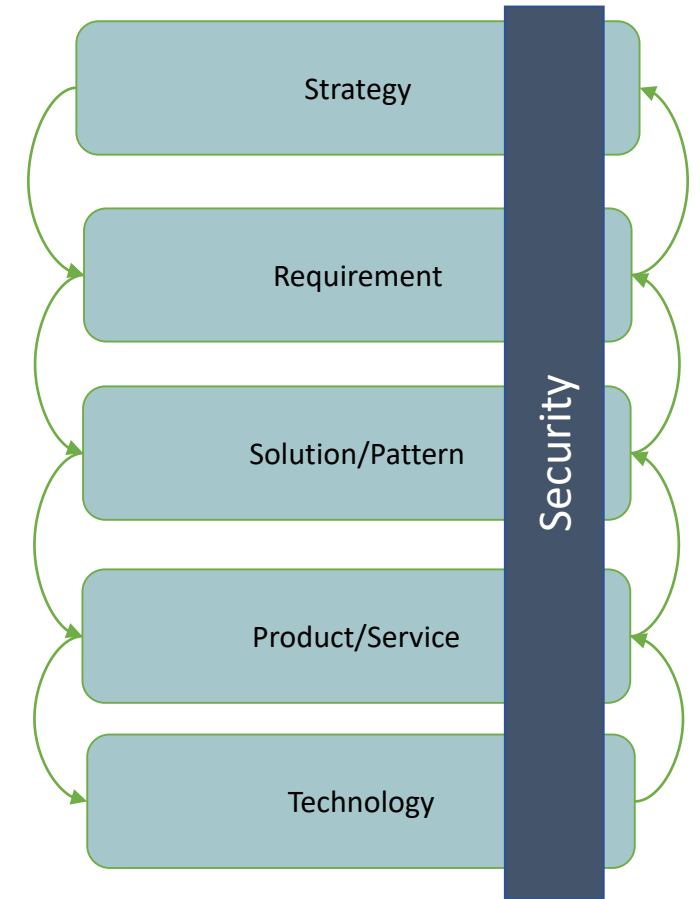
Two-way traceability

Seamless alignment to TOGAF, ITIL, ISO27000, NIST, CobIT, etc...

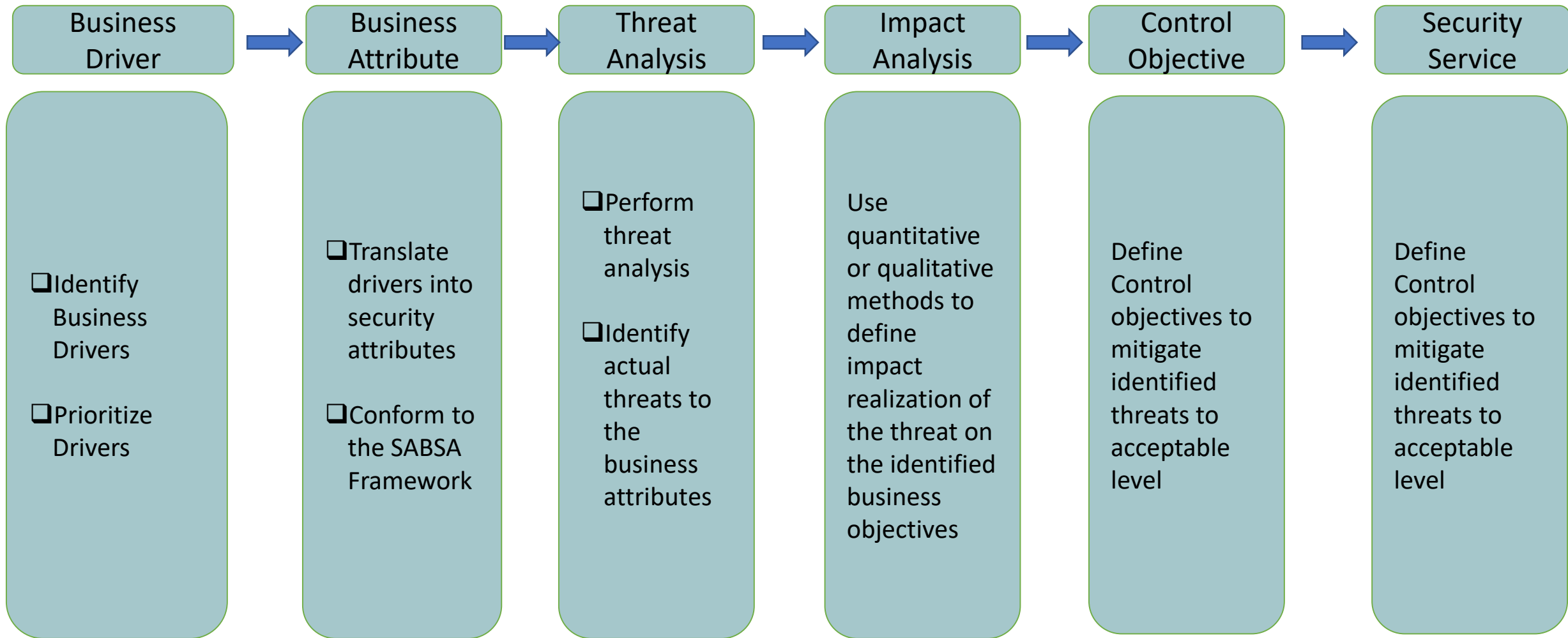
# EA in Practice : ADM phases



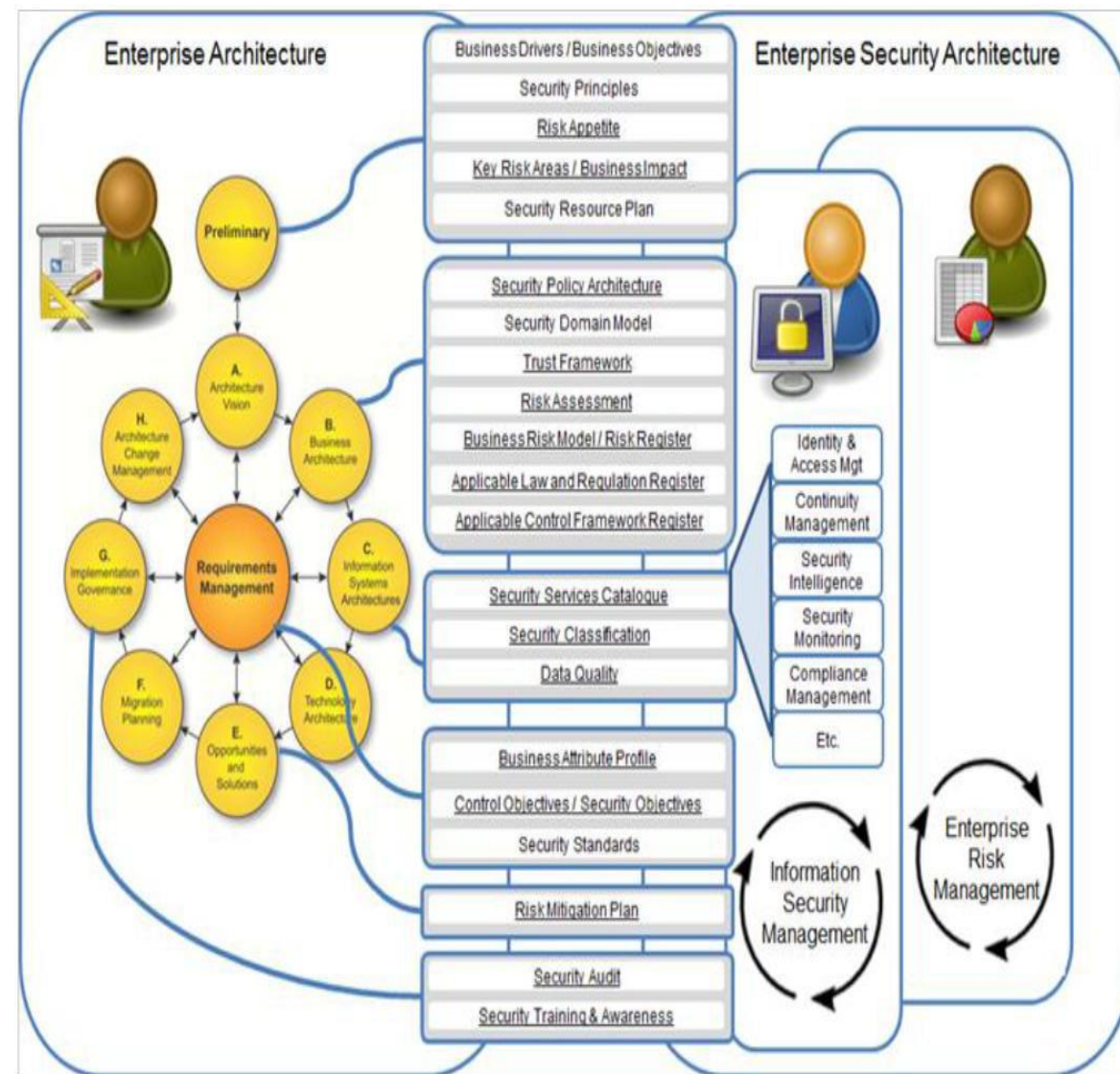
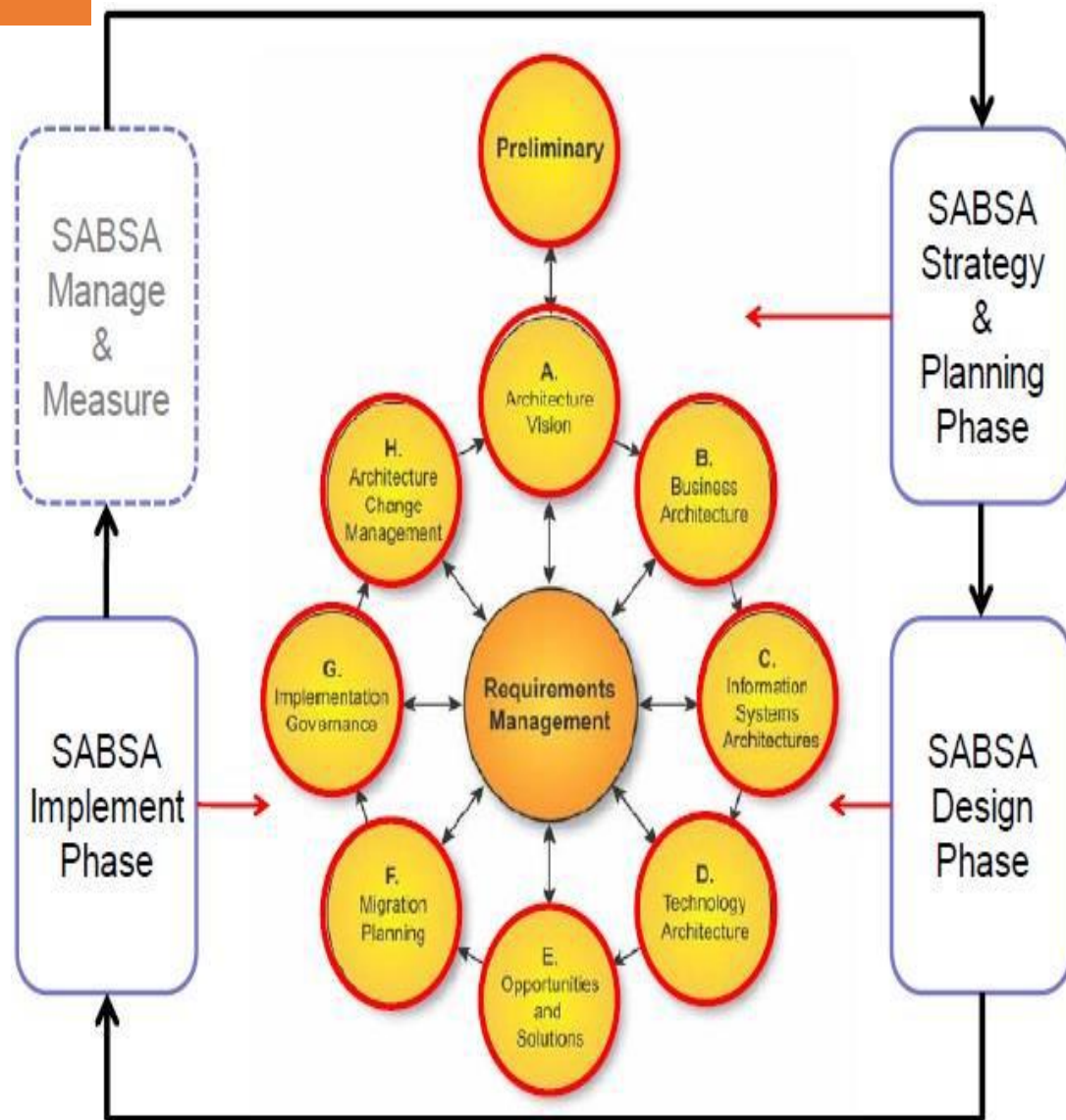
**Bidirectional  
traceability**



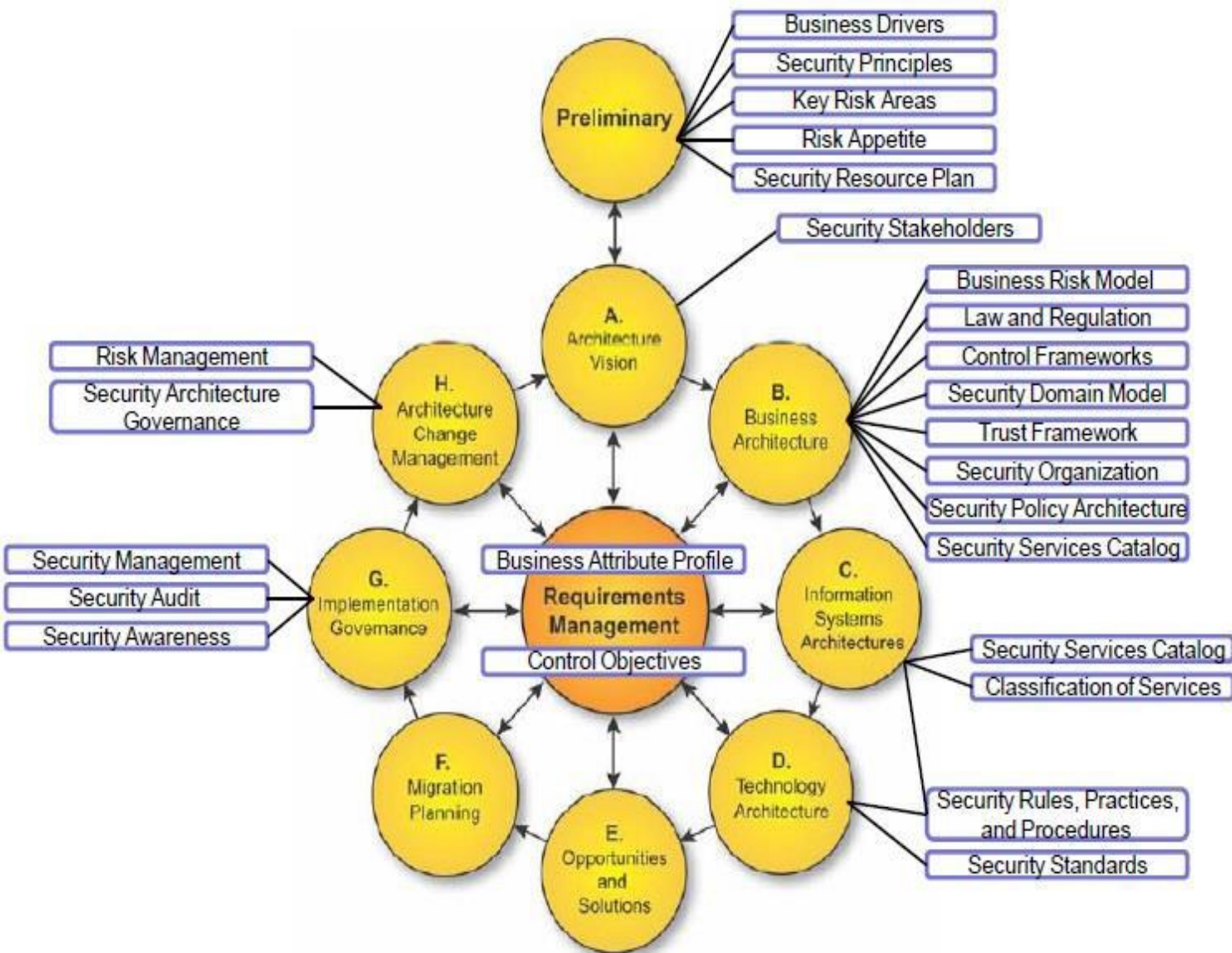
# SABSA Approach Step by Step



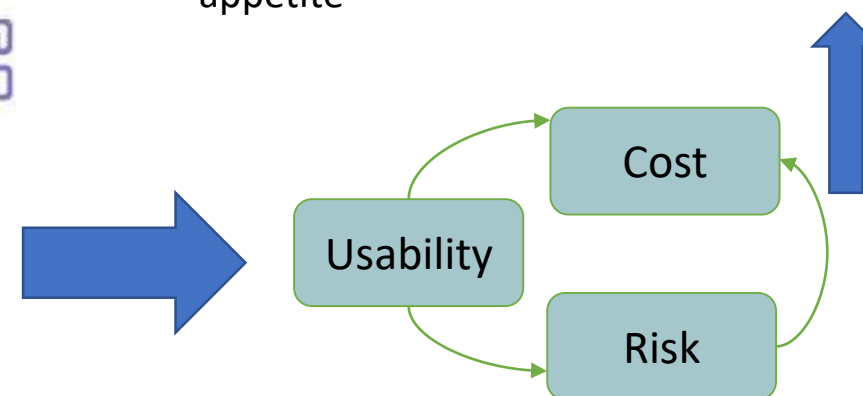
# Putting it all together: SbD in EA



# Putting it all together: SbD in EA



- 1 Security is driven by business requirements rather than technical consideration
- 2 Directly traceable to business objectives
- 3 Cost Effective
- 4 Meet legal, regulatory and policy compliance requirement by design
- 5 Alignment of business risk and organizations risk appetite



A world map in a light yellow color serves as the background. Overlaid on this map is a complex network of dark grey lines and dots. The dots, representing nodes, are distributed across the continents, with some appearing as small circles and others as larger, more prominent hubs. These nodes are interconnected by thin, dark grey lines, creating a web-like structure that spans the entire globe. The network is denser in some regions, such as North America and Europe, and sparser in others, like South America and Africa. The overall effect is one of global connectivity and data flow.

# Conclusion

# Security by Design – Benefits



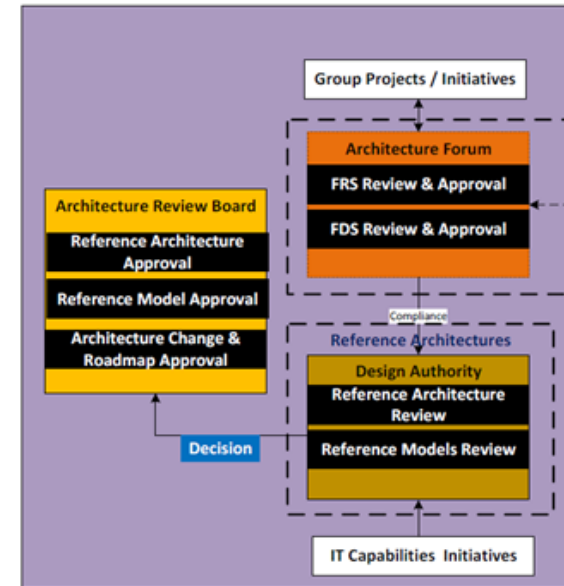
- Business and Risk-Driven approach
- Traceability for completeness & Justification
- Provide structured framework for compliance purpose
- Create foundation for assessment of security ROI

- Blueprint of reference for Solution Architects
- Includes policies, controls, procedure and guidelines
- Meet compliance and align with risk appetite
- Driven by organization business requirement

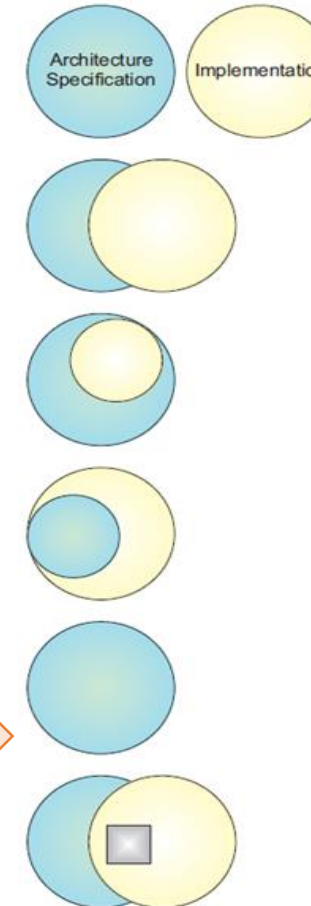
- Eliminate redundant controls
- Reduce Ad hoc implementation
- Provides agreed security requirement
- Tracible security requirement to business requirement

# EA & ESA: Reference architecture compliance

- A Solution Design process initiated by business
- B Solution Design presented to Design Authority for approval
- C Design Authority select relevant architecture under governance
- D Design Authority checks high level conformance, either “approve” or refers back for “revision” by solution team



Checks



## Irrelevant:

The implementation has no features in common with the architecture specification (so the question of conformance does not arise).

## Consistent:

The implementation has some features in common with the architecture specification, and those common features are implemented in accordance with the specification. However, some features in the architecture specification are not implemented, and the implementation has other features that are not covered by the specification.

## Compliant:

Some features in the architecture specification are not implemented, but all features implemented are covered by the specification, and in accordance with it.

## Conformant:

All the features in the architecture specification are implemented in accordance with the specification, but some more features are implemented that are not in accordance with it.

## Fully Conformant:

There is full correspondence between architecture specification and implementation. All specified features are implemented in accordance with the specification, and there are no features implemented that are not covered by the specification.

## Non-conformant:

Any of the above in which some features in the architecture specification are implemented not in accordance with the specification.



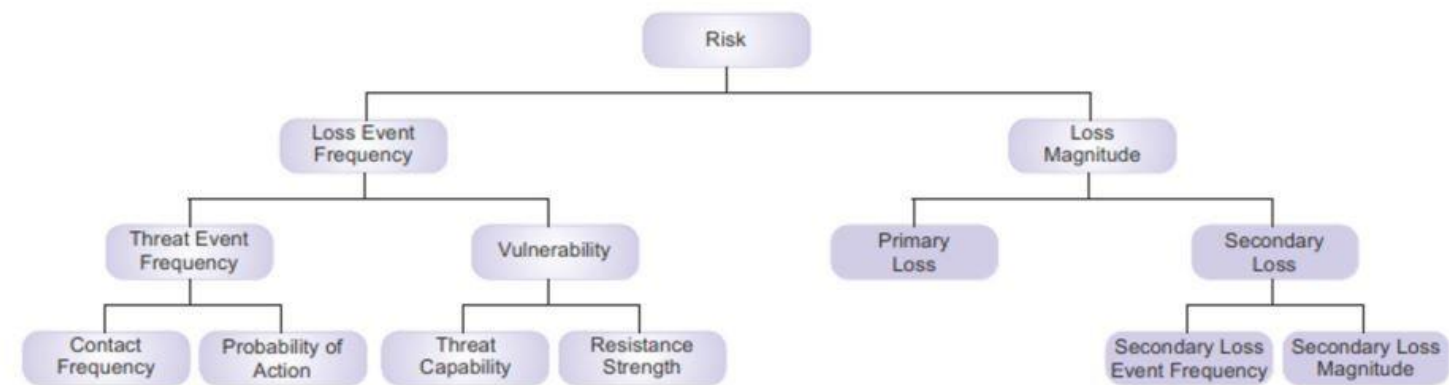
**Thank you**

A world map with a network overlay. The map is yellow, and the network consists of black dots (nodes) connected by black lines (edges). The nodes are distributed across the continents, with a higher density in North America and Europe. The network structure is complex, with many interconnected nodes and lines, suggesting a global network or communication system. A dark brown horizontal bar is positioned across the middle of the map, containing the text "Bonus round?".

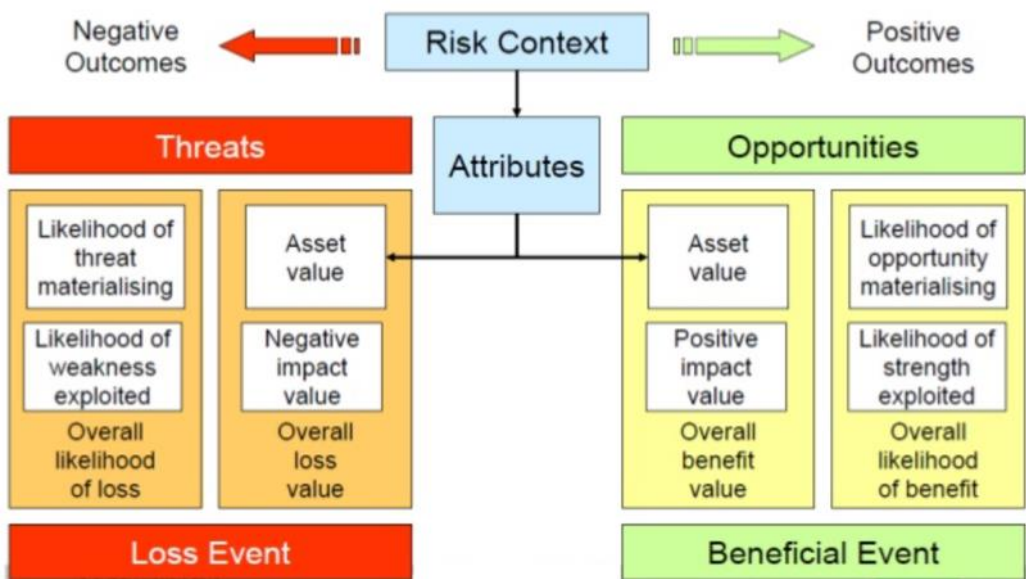
**Bonus round?**

# Risk assessment methods

## OpenFAIR



## SABSA Risk & Opportunity Model



## NIST800-30

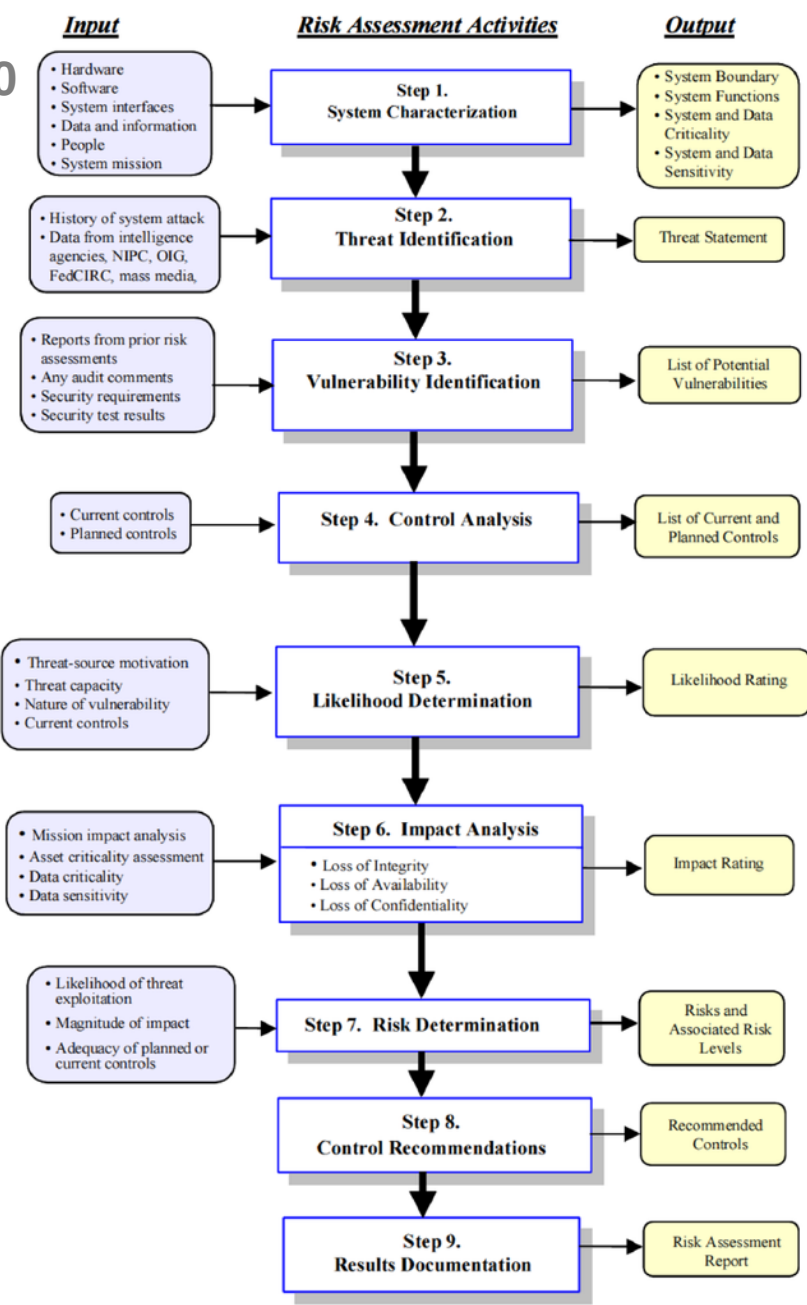
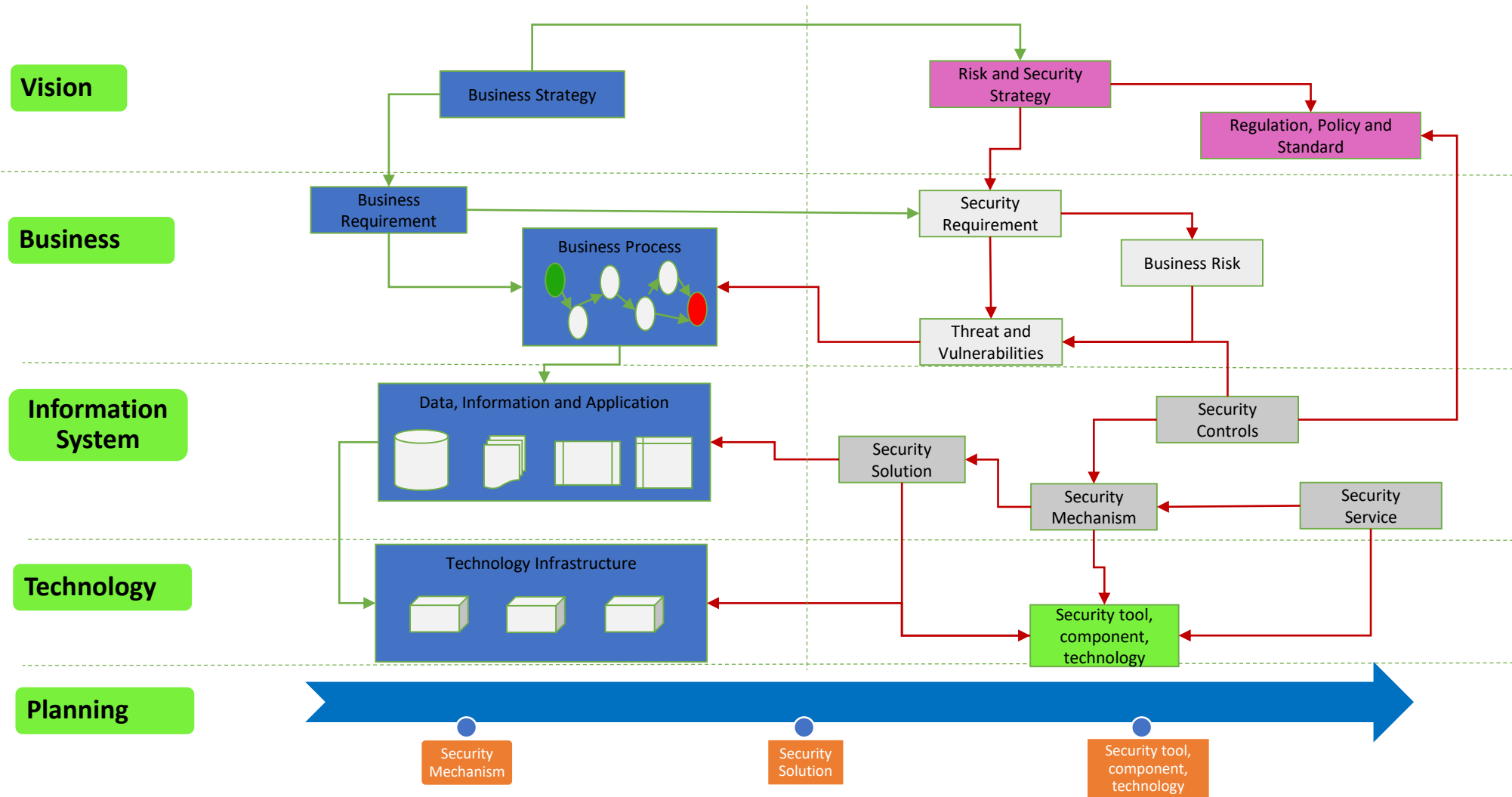
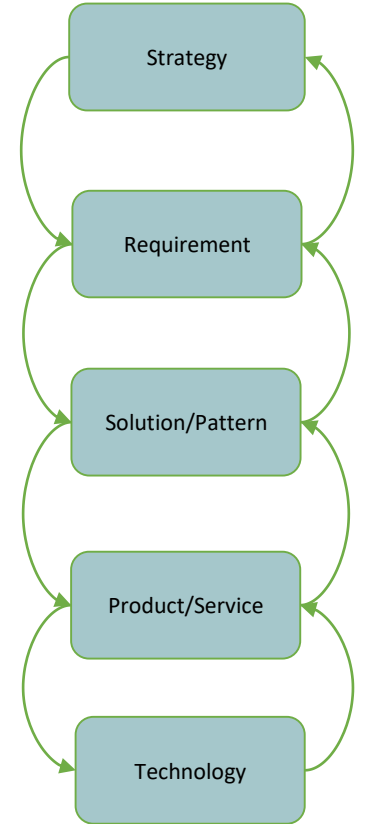


Figure 3-1. Risk Assessment Methodology Flowchart

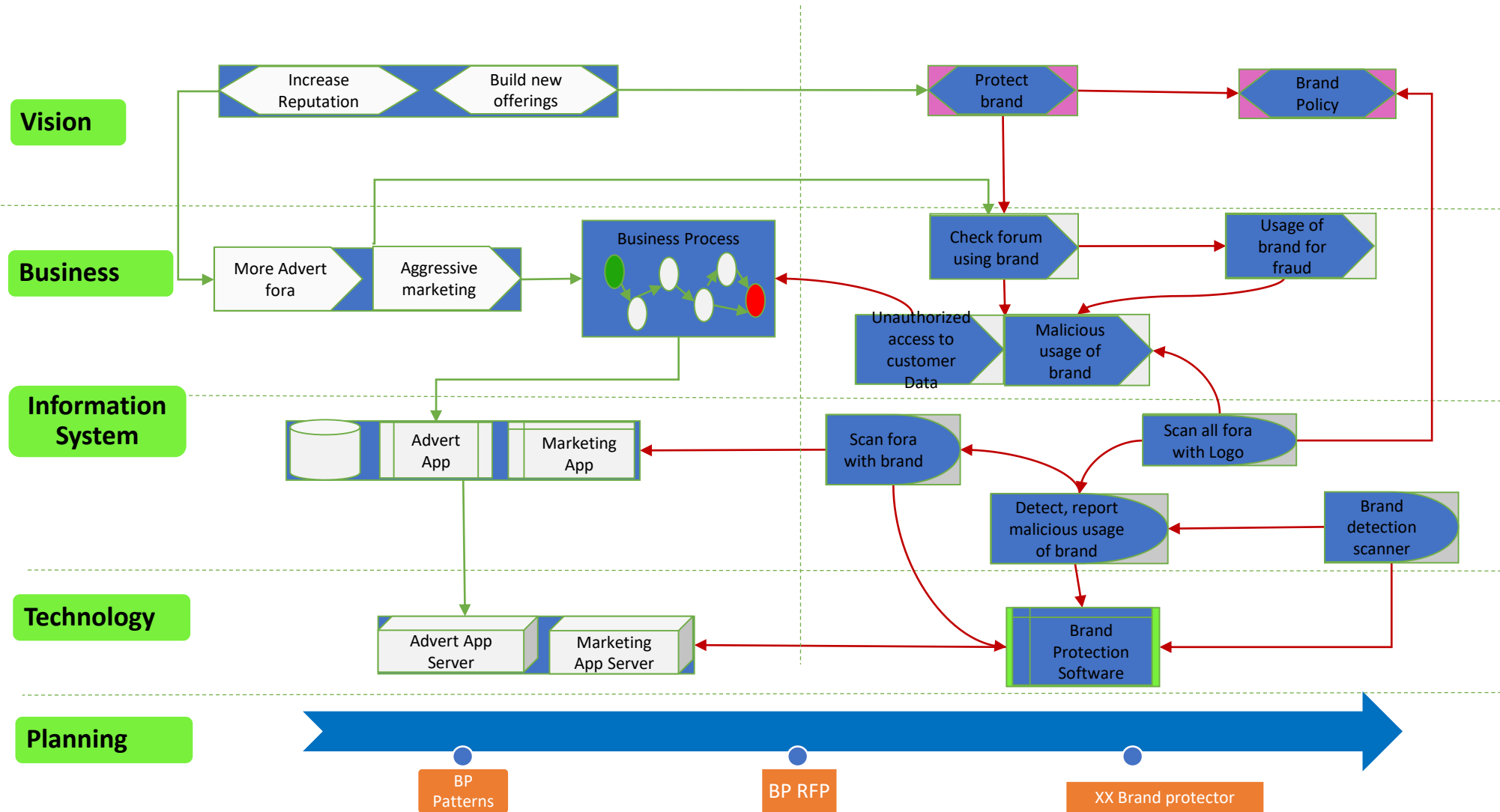
# EA Metamodeling: an example



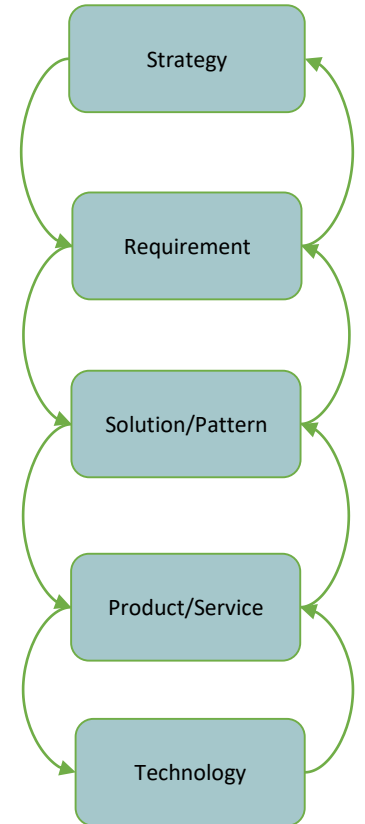
## Bidirectional traceability



# EA Metamodeling: Views & Business attributes



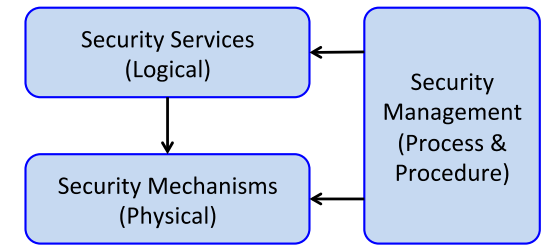
## Bidirectional traceability



# Preliminaries for Integration: Some Key security Concepts

## Security Service

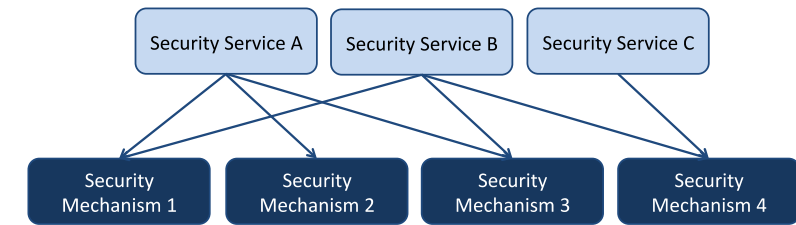
- A fundamental logical building block for constructing security solution architectures
- Creating a repository of standardised security services is part of an enterprise security architecture, providing security architects with a library of security service definitions for use 'off-the-shelf' when synthesising solution security architectures.



Copyright © The SABSA Institute 1995-2016

## Security Mechanism

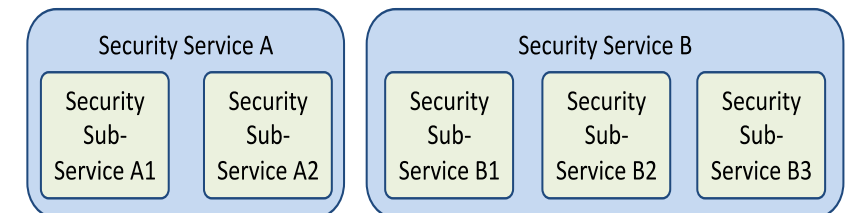
- A security mechanism is a type of technology or process that can deliver a security service.
- Different mechanisms may be used to provide the same service, depending on the actual context.



Copyright © The SABSA Institute 1995-2016

## Security Sub-service

- Some services may be sub-services of higher-level services.
  - **Service:** Access Control; **sub-service:** Authentication;  
**Mechanism:** ID and password.



Copyright © The SABSA Institute 1995-2016

# References

1. Kurpjuweit, S. and Winter, R., 2009. Concern-oriented business architecture engineering. *In Proceedings of the 2009 ACM symposium on Applied Computing (SAC '09)*, pp. 265-272.
2. Kvale, S. and Brinkmann, S., 2009. *InterViews: Learning the Craft of Qualitative Research Interviewing*. 2nd ed. SAGE publications.
3. Langenberg, K. and Wegmann, A., 2004. *Enterprise Architecture: What Aspects is Current Research*
4. <https://whatis.techtarget.com/definition/security-by-design>
5. [https://www.owasp.org/index.php/Security by Design Principles](https://www.owasp.org/index.php/Security_by_Design_Principles)
6. Amer, H.S. and Hamilton, J.A., 2008. Understanding Security Architecture. *Proceedings of the 2008 Spring simulation multiconference (SpringSim '08)*, pp. 335-342