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

[Submit to our EA FORUM DATABASE]

[Follow the EA Forum on Twitter...]

[Our upcoming events]

[Subscribe to our EA FORUM DATABASE]

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

Twitter: @EAforumSA
#ogza
Leading the development of open, vendor-neutral IT standards and certifications

http://opengroup.org/

http://opengroup.co.za
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.

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.
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**
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

- How to align to business Risk?
- How do we keep business and security aligned?
- How do we minimize security gaps and remediations costs?
- How do we embed security in the wider business?
- What strategy can be used to develop security architecture as part of the enterprise architecture?
- How do we ensure security support the business?
Risk-Based metamodeling: First try x 11

✓ Business Driven Architecture
✓ Bi-Directional Traceability
✓ Context sensitive control compliance
✓ Multi-domain policy architecture
✓ Impact and cost traceability
✓ Planning and change Management
✓ Efficiency
✓ Multiple viewpoints
... but does not live in a vacuum
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

Enterprise Security

- Confidentiality
- Availability
- Inter-operability
- Integrity
- Compliant
- Profitability

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

- Strategy
- Requirement
- Solution/Pattern
- Product/Service
- Technology
SABSA Approach Step by Step

- Identify Business Drivers
- Prioritize Drivers
- Translate drivers into security attributes
- Conform to the SABSA Framework
- Perform threat analysis
- Identify actual threats to the business attributes
- Use quantitative or qualitative methods to define impact realization of the threat on the identified business objectives
- Define Control objectives to mitigate identified threats to acceptable level
- Define Control objectives to mitigate identified threats to acceptable level

Business Driver → Business Attribute → Threat Analysis → Impact Analysis → Control Objective → Security Service
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

Usability → Cost → Risk
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
Solution Design process initiated by business

Solution Design presented to Design Authority for approval

Design Authority select relevant architecture under governance

Design Authority checks high level conformance, either “approve” or refers back for “revision” by solution team
Thank you
Bonus round?
Risk assessment methods

OpenFAIR

SABSA Risk & Opportunity Model

NIST800-30

Figure 3-1. Risk Assessment Methodology Flowchart
EA Metamodeling: an example
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.

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.

Security Sub-service

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

   *the 2009 ACM symposium on Applied Computing (SAC ’09),* pp. 265-272.
4. [https://whatis.techtarget.com/definition/security-by-design](https://whatis.techtarget.com/definition/security-by-design)