Security Architecture ⊆
Enterprise Architecture

An exploration of how Security Architecture fits within Enterprise Architecture
Duncan Unwin
Brisbane, 27th February 2013
Put your hand up if
In your work ....

— You conduct risk assessments?
— You write security policies?
— You developed an information security management system?
— Set up a information security governance mechanism e.g. a steering committee or user group?
— Design security controls for systems?

Congratulations!
You do Security Architecture
Keep you hand up if...

— You use a formal security architecture framework
— Your job title includes the word ‘Architect’
— You work within the Enterprise Architecture Team
— Your work is tightly integrated with the organisation’s enterprise architecture practices
— Your work drives the information security teams priorities

Hi, I’m Obi Wan and I’ll be your Security Architect today
The dilemma of Information Security

— Most people in your organisation do not understand your infosec risks
  — The Availability Heuristic (Tversky and Kahneman, 1971)
    — I have not been hacked so I will not be hacked
    — I have been hacked so I will be hacked again soon
    — Hacking is something that happens to others
  — Other cognitive biases
    — Security risks are hard to rate even for experts
  — Confusing consequences with threats
    — ‘If my data is lost I will suffer’ is not the same as ‘someone wants to steal my data’
The dilemma of information security

None of this should be a problem. They passed their PCI audit and have antivirus.
The dilemma of Information Security

— Information Security practices are not well understood by IT

Compliance Droids

Hackers on company payroll
The dilemma of Security Architecture

Most people in Infosec do not understand Architecture

- “I’m the Security Architect” “So you're writing the security policy, right?”
- “We will need a TRA for the new system to get through the CAB”
- “Our team lead said you’re looking after PCI”
- “So are you an architect or in Security?”
- “After we go live we will need you to document the firewall”
The Security Guy (or Gal) in Architecture
What an EA thinks of Security - an example

What the Security Architecture Team Built

How this was summarised to the CIO

And more than 30 other artefacts totalling more than 500 pages
Lets talk about Architecture....Shall we?

Instruction:
1. Cut out pieces
2. Attach Tab A to B
3. Wa-Lah!
Architecture – What is it?

Enterprise architecture is the organizing logic for business processes and IT infrastructure reflecting the integration and standardization requirements of the company’s operating model. The operating model is the desired state of business process integration and business process standardization for delivering goods and services to customers.
- MIT Center for Information Systems Research

All... must be built with due reference to durability, convenience, and beauty. Durability will be assured when foundations are carried down to the solid ground and materials wisely and liberally selected; convenience, when the arrangement of the apartments is faultless and presents no hindrance to use, and when each class of building is assigned to its suitable and appropriate exposure; and beauty, when the appearance of the work is pleasing and in good taste, and when its members are in due proportion according to correct principles of symmetry.

- Vitruvius, De Architectura (~ 15 BC), Chapter III
Lots of frameworks
Enterprise Architecture Frameworks

— Taxonomy
  – Zachman
— Process
  – TOGAF
— Unified
  – FEA
— Methodology-specific
  – ARIS, ArchiMate
— Practice-based
  – Gartner

Choosing between Zachman and TOGAF .. is like choosing between spinach and hammers.
- Roger Sessions, 2007
A Fresh Perspective

Architecture – What is it?
And another thing....
Security Architecture

It is the common experience of many corporate organisations that information security solutions are often designed, acquired and installed on a tactical basis.

The result is that the organisation builds up a mixture of technical solutions on an ad hoc basis, each independently designed and specified and with no guarantee that they will be compatible and interoperable.

Security architecture is business-driven and .. describes a structured inter-relationship between the technical and procedural security solutions to support the long-term needs of the business.

John Sherwood, Andrew Clark & David Lynas – SABSA.ORG
Security Architecture

SABSA

| Contextual | The Business Environment |
| Conceptual | Business Attributes Profile |
| Logical | Business Information Model |
| Physical | Business Model |
| Component | Detailed Service Structure |
| Operational | Assurance, Operation, Continuity |

Figure 16: Overview of Security-Related Artifacts in the TOGAF ADM
Mid-way summary

— Security Architecture is hard and often misunderstood
— Security Architecture often struggle to find meaning within Enterprise Architecture for this reason
— Architecture is about high-level design
— Lots of frameworks – Taxonomies, Processes & Methods
— TOGAF – Process to do EA with candidate taxonomy (BIAT)
Explaining Information Security Architecture to Architects

— What is it

— Why it matters

— Their role
Business Requirements

— Enterprise Architecture
  — Goals
  — Rules
  — Requirements

— Security Architecture
  — Laws and Regulations
  — Compliance standards
  — Contracts
  — Explicit mandates
  — Risk-based control requirements

“Ask the business”

“Ask the business” + “Ask the World”
Business Requirements

— Enterprise Architecture
  — Capabilities
  — Services

— Security Architecture
  — Attributes
  — Control Objectives
Business Architecture

— Two Common Focus

  — Information Security Processes and Organisation
    — Developing the capability to be secure
    — Think ITIL Security
    — Think ISMS

  — Security within general business processes
    — What assets to be protected?
    — How, who and what will protect them?
    — How, who and what will address incidents?
    — What security governance is required?
Information Architecture

— Enterprise Information Architecture
  – Subject Area Model
  – Conceptual Information Model
  – Logical Information Model
  – Physical Information Model

— Security Architecture
  – Assets
  – Information Inventories
  – Information Classification
  – Information Usage (CRUD)
Application Architecture

- Application Architecture
  - Information Systems
  - Conceptual App Architecture
  - Software Architecture
  - SOA
- Security Concerns
  - Common security services
    - Identity Management and Access Control
    - Audit & Logging
    - Vulnerability management
    - Etc...
  - Information flows
  - Threat modelling
  - Control design
  - Operational management concepts
  - SDLC
Technology

— Technology Architecture
  – Standards and Reference Models
  – Logical & physical topologies
  – Dependencies
  – Capacity and Availability

— Security Architecture
  – Approved products / EPL
  – C.I.A. of design
    — FMEA
    — Design and build assurance
  – Configuration standards
  – Operational standards
  – Alignment with ISMS, policies & standards
Transformation & Governance

— Program Management Office
  — Program reporting and governance
  — Project reporting and governance
  — Time, Cost, Quality BUT NOT Security

— Security Architect
  — Ensuring Security goals and requirement in the Business Case
  — Providing tools to measure delivery
  — Identifying dependencies within the program and project
  — Helping with prioritisation decisions
  — Linkage to security governance
TOGAF Security Architecture

SECURITY

Business Requirements
Business
Information
Applications
Technology

Transition
Governance
Doing Security Architecture well (or better)... 

— Understand the EA Process
Doing Security Architecture well (or better)...

— Understand the EA Process
— Bond with the team
Doing Security Architecture well (or better)...

— Understand the EA Process
— Bond with the team
— Align your language
Doing Security Architecture well (or better)…

— Understand the EA Process
— Bond with the team
— Align your language
— Be pragmatic
Doing Security Architecture well (or better)...

— Understand the EA Process
— Bond with the team
— Align your language
— Be pragmatic
— Use evidence
Doing Security Architecture well (or better)...

— Understand the EA Process
— Bond with the team
— Align your language
— Be pragmatic
— Use evidence
— Be a Boundary Rider
The End

These are not the requests you are looking for.
About Business Aspect

Business Aspect assists clients with the execution of their business strategy through either large scale business transformation or through the addressing of smaller challenges in specific areas of the business. We focus on the business first, and then address technology needs as an enabler of required business outcomes. We have skills, experience and expertise in; business and technology strategy, architecture, risk, control, planning, design and governance. In delivering services, we address all layers of the business, including people, organisational change, process change, information management, information and communications technology (ICT) applications and technology infrastructure.

We solve complex business problems through the collaborative efforts of our team of highly experienced personnel, and through the application of proven intellectual property. One of our key strengths is the diversity of the background and skills our senior consultants bring to planning initiatives involving people, process and systems.

Our ability to extend from business focused domains into architecture and complex program management builds a bond of trust with our clients and fosters more effective relationships. For our clients, we serve as the interpreter between ICT and the demands of individual business units, translating business needs into ICT outcomes. We complement this with our ability to work with all parts of the organisation, therefore maximising the benefits collectively gained from ICT.

We believe the use of senior consultants for the delivery of our clients’ projects is the cornerstone of our success. We also hand pick specialists from our extensive network of associates and industry partners to complement our consulting teams. We guarantee senior people with the right balance of qualifications and real-world industry experience, and our delivery capability extends across Australia.