# Enterprise Security Architecture

Presented as part of
SENG 460 – Practice of Information Security and Privacy
University of Victoria
Spring 2014

## Roadmap

| | |
|---|---|
| *What* | What is enterprise security architecture? |
| *Why* | Sustaining motivations, why pursue enterprise security architecture? |
| *How* | How might we practice enterprise security architecture? |
| *Why not* | What opposes the practice of enterprise security architecture? |
| *Do* | Your turn: work through an example application of enterprise security architecture. |

Echo of the 6 basic interrogatives: *What, How, When, Who, Where, and Why*

The SABSA ordering is *What, Why, How, Who, Where, When*

# What is enterprise security architecture?

## What is the Enterprise?

Enterprise (noun):

- a project or undertaking, especially a bold or complex one; a business or company (Oxford)
- a unit of economic organization or activity, especially a business organization; a **systematic purposeful activity** (Merriam-Webster)
- A company, business, organization, or other **purposeful endeavor** (Wiktionary.org)

Without some definition and measure of value, it's hard to know what things need to be secured.

Enterprise
- Operating context for a set of subject assets and activities
- a set of people, processes, and technologies
- Holistic perspective
- Context for and definition of value

## What is Architecture?

An *architecture* is the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.

Source: ANSI/IEEE Std 1471-2000, Recommended Practice for Architectural Description of Software-Intensive Systems

An *architectural framework* is a tool for developing a range of different architectures.

- a way to and a coherent structuring the activities and interactions of people, organizational units, business processes, and IT systems and components

## What is Enterprise Architecture?

Enterprise architecture (EA) is the practice of developing integrated architectural perspectives of an enterprise to enable and ensure information systems support that organization's goals.

Typical elements in the practice of EA include:

- A framework
- A methodology, for applying the developing specific architectural descriptions, such as AS-IS and TO-BE
- Reference architectures and standards
- Portfolio management, for managing evolution of enterprise IT systems from the AS-IS state toward the TO-BE or desired state
- Enterprise Architects, individuals skills in the application of EA

As information systems have become tightly integrated with an organization's business processes, they have become key to the long-term success and sustainability of the organization. Information systems have become increasingly complex and difficult to manage, maintain, and keep relevant to the organization. Enterprise Architecture is a means of managing this complexity, of aligning information systems and the business objectives they enable, and providing the ability to manage a portfolio of IM/IT assets and change projects, long-term approach to ensuring that information systems support the organization's goals.

Examples of EA frameworks include Zachman Framework for Enterprise Architecture, The Open Group Architecture Framework (TOGAF), the Federal Enterprise Architecture Framework (FEAF).

# Example EA framework: Zachman

| | What (Data) | How (Function) | Where (Locations) | Who (People) | When (Time) | Why (Motivation) |
|---|---|---|---|---|---|---|
| **Scope {contextual} Planner** | List of things important to the business | List of processes that the business performs | List of locations in which the business operatses | List of organizations important to the business | List of events/ cycles important to the business | List of business goals/strategies |
| **Enterprise Model {conceptual} Business Owner** | e.g. Semantic Model | e.g. Business Process Model | e.g. Business Logistics System | e.g. Workflow Model | e.g. Master Schedule | e.g. Business Plan |
| **System Model {logical} Designer** | e.g. Logical Data Model | e.g. Application Architecture | e.g. Distributed System Architecture | e.g. Human Interface Architecture | e.g. Process Structure | e.g. Business Rule Model |
| **Technology Model {physical} Implementer** | e.g. Physical Data Model | e.g. System Design | e.g. Technology Architecture | e.g. Presentation Architecture | e.g. Control Structure | e.g. Rule Design |
| **Detailed Representation {out-of-context} Subcontractor** | e.g. Data Definition | e.g. Program | e.g. Network Architecture | e.g. Security Architecture | e.g. Timing Definition | e.g. Rule Definition |
| **Functioning System** | e.g. Data | e.g. Function | e.g. Network | e.g. Organization | e.g. Schedule | e.g. Strategy |

## What is Security?

- *Security* - the state of being free from danger or threat. (Oxford)
- *Information Security* - ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability). (ISACA)
- *Cybersecurity* - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. (Merriam-Webster)
- *Computer Security* - the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications). (NIST)

Security

- One perspective of the activities and concerns of an enterprise
- A category of the qualities of assets, entities, processes, systems, and environments
- A professional practice domain
- specific set of authority and accountability; e.g. organizational structure that produces groups with name like 'Security Operations'

See also:

* An Introduction to Computer Security: The NIST Handbook, SP 800-12, http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/

## Core Information Security Qualities: CIA

Confidentiality - the protection of information within systems so that unauthorized people, resources, and processes cannot access that information.

Integrity - the protection of system information or processes from intentional or accidental unauthorized changes.

Availability - the assurance that information resources are accessible (by authorized users) as needed.

Source: $(ICS)^2$

**An information security program will ensure these qualities are maintained as required to ensure the ongoing operation of the organization and support of its mission.**

More generally,

- Confidentiality
  - containing information whose unauthorized disclosure could be prejudicial to the national interest (Merriam-Webster)
  - intention to keep private or secrete (Oxford)
- Integrity
  - the state of being complete or whole (Merriam-Webster)
  - internal consistency or lack of corruption in electronic data (Oxford)
- Availability

- the quality of being easy or possible to get or use (Merriam-Webster)
- able to be used or obtained (Oxford)

## Security, Safety and Risk

- Safety is the judgment of risk associated with foreseeable events, outcomes, and failures in a given situation: Something is judged ‘safe’ when the risk of negative outcomes is deemed acceptable.
  - does not mean that there is not any risk, just that the risk can be mitigated or controlled to an acceptable level.
- Engineering perspective: evidence-based quantifications; probabilities, likely consequences; e.g. structural load carrying tolerances used to build bridges and airframes.
- Management perspective: risk and reward; underlying willingness—indeed systemic incentives--to accept higher risk for larger rewards.

## What is appropriate use of an information asset, access to an information resource?

- right information
- right person
- right time
- right purpose

And increasingly,

- right system

Where 'right' is defined by policy and the context of a given business area.

**Violate any of these 'rights' and you have a security incident. (or worse)**

Why inclusion of 'right system'? Because enterprises are embodied by a system of systems.

Professional Nurses use mantra before administering medication, the so-called 7-Rights:

1. RIGHT drug
2. RIGHT client (Two Identifiers)
3. RIGHT dose
4. RIGHT time
5. RIGHT route
6. RIGHT reason
7. RIGHT documentation

The safe performance of any nursing task, such as the administration of medication, is not complete until *all* the required steps are performed.

Source: Practice Standard – Medication, 2014, College of Nurses of Ontario, 'rights of medication administration' -- http://www.cno.org/Global/docs/prac/41007_Medication.pdf

## An enabling view of information security: information sharing for better outcomes

- If government(s) could share the right information, among the right people, for the right purpose, and at the right time, then some better outcomes for citizens would result.
- Example: Sherry Charlie was a 1 ½ year old child under the protection of the BC Government who was battered and then killed by a family member in 2002. One of the systemic problems identified was insufficient information available to the people directly involved, resulting in Sherry being placed in an unsafe situation and with subsequent lack of intervention as the situation worsened.

Or information sharing for better outcomes. Parnas' perspective on this might be information hiding for better outcomes.

See also

- Summary Director's Case Review: S.C., Ministry of Children and Family Development, June 9, 2005 -- http://www.mcf.gov.bc.ca/about_us/pdf/summary_dcr_sc.pdf
- http://www.google.ca/search?q=sherry+charlie+case

A whole chapter of the subsequent Hughes Review, related to information sharing. For example:

- Recommendation 55: That the Representative for Children and Youth Act clearly provide for the creation, use and disclosure of linked data sets for purposes specified in the Act.
- Reason: The Representative needs to collect and link data about children so that it can monitor and evaluate the effectiveness, responsiveness and relevance of services provided to children, youth and families.

Source: Section 5.1 (Information Sharing), BC Children and Youth Review, Hon. Ted Hughes, April 2006 -- www.mcf.gov.bc.ca/about_us/pdf/BC_Children_and_Youth_Review_Report_FINAL_April_4.pdf

## What is enterprise security architecture?

*Security architecture* is the art and science of designing and supervising the construction of business systems, usually business information systems, which are:

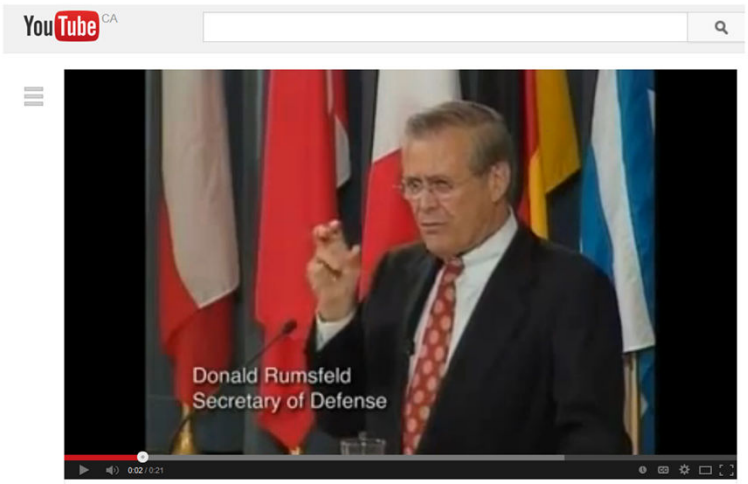
- free from danger, damage, etc;
- free from fear, care, etc.;
- in safe custody;
- not likely to fail;
- able to be relied upon;
- safe from attack.

An *enterprise security architecture* is a business-driven description of a structured inter-relationship between the technical and procedural solutions to support the long-term needs of the business. (SABSA)

Source: John Sherwood, Andrew Clack, David Lynas. *Enterprise security architecture: a business-driven approach*. 2005. CMP Books

(Why) Sustaining motivations, why pursue enterprise security architecture?

## Known Knowns, Known Unknowns, and Unknown Unknowns




... there are known knowns; there are things we know that we know. There are known unknowns; that is to say, there are things that we now know we don't know. But there are also unknown unknowns – there are things we do not know we don't know. -- Donald Rumsfeld, United States Secretary of Defense, February 12, 2002 11:30 AM EDT -- http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636

Donald Rumsfeld YouTube Video

## Using ESA and Frameworks to address Meta-Ignorance

**To not be meta-ignorant,**

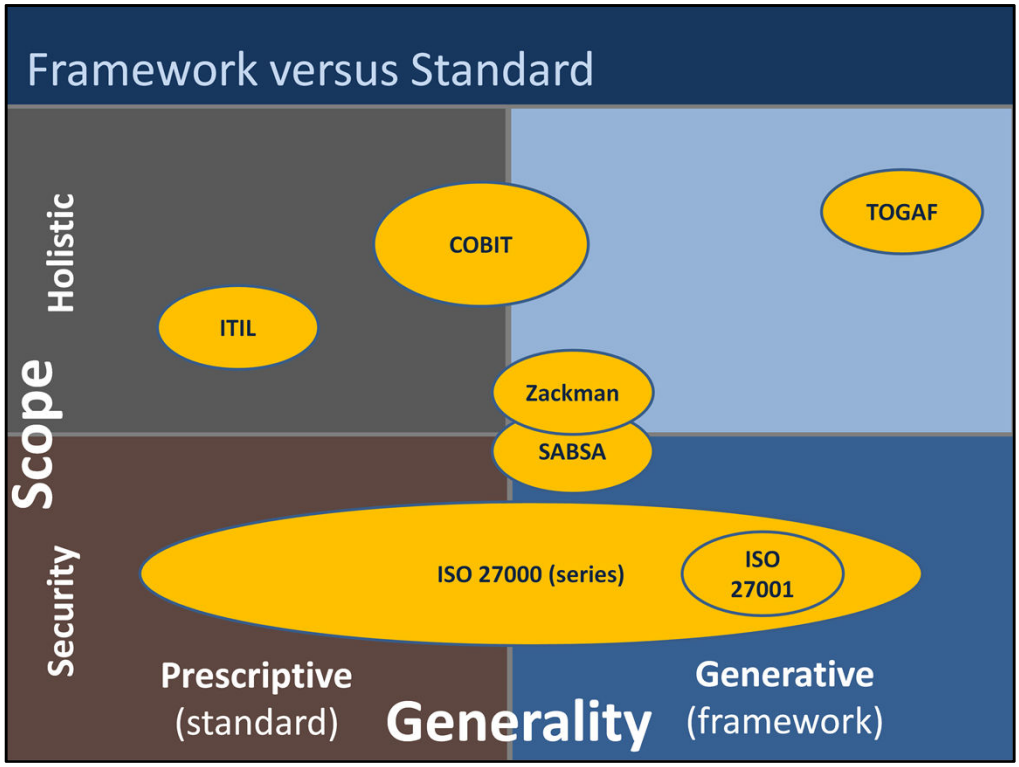
we must have some suitably efficient process (not only trial and error)

to find out that we don't know that we don't know something.

(here, civilization and the education system generally help us to avoid this state.)

**The five orders of ignorance**
By Phillip G. Armour
Communications of the ACM, Vol. 43 No. 10, Pages 17-20
10.1145/352183.352194 -- URL; http://cacm.acm.org/magazines/2000/10/7556-the-five-orders-of-ignorance/

- 0th Order Ignorance (0OI)—Lack of Ignorance: I know something and can demonstrate my lack of ignorance in some tangible form, such as by building a system that satisfies the user.
- 1st Order Ignorance (1OI)—Lack of Knowledge. I don't know something and can readily identify that fact.
- 2nd Order Ignorance (2OI)—Lack of Awareness: I don't know that I don't know something.
- 3rd Order Ignorance (3OI)—Lack of Process: lack a suitably efficient way to find out I don't know that I don't know something
- 4th Order Ignorance (4OI)—Meta Ignorance




Generative frameworks: tools you use to design architectures to meet your needs
Perspective standards: ways to audit and compare your systems with others

Holistic still assumes underlying IT orientation

## Standards Compliance through an ESA

- ISO 27001 – " A management framework should be established to initiate and control the implementation of information security within the organization"
- COBIT V.4.2, Delivery and Support Control Objective #5 -- "Consider whether a strategic security plan is in place providing centralized direction and control over information system security"
- CICA ITCG V3 , Control Objective T1 -- "The enterprise should design, develop and approve and enterprise wide security architecture"

## Proof that ESA works

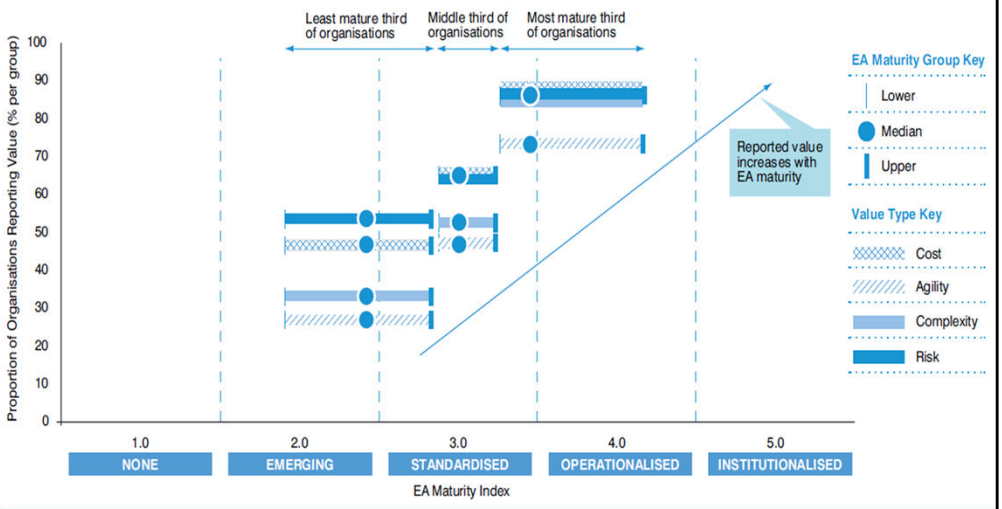
Essentially, all models are wrong, but some are useful. -- *G.E.P. Box*

In a survey of organizations with mature EA programs, over 70% reported value realized across areas: decreased cost, reduced complexity, reduced risk, and increased agility. In less mature organizations, at least 50% reported value in reduced risk. – 2009, Booz&Co

Subtext: we lack good evidence around many of these claims.

# Enterprise Architecture Delivers Business Value

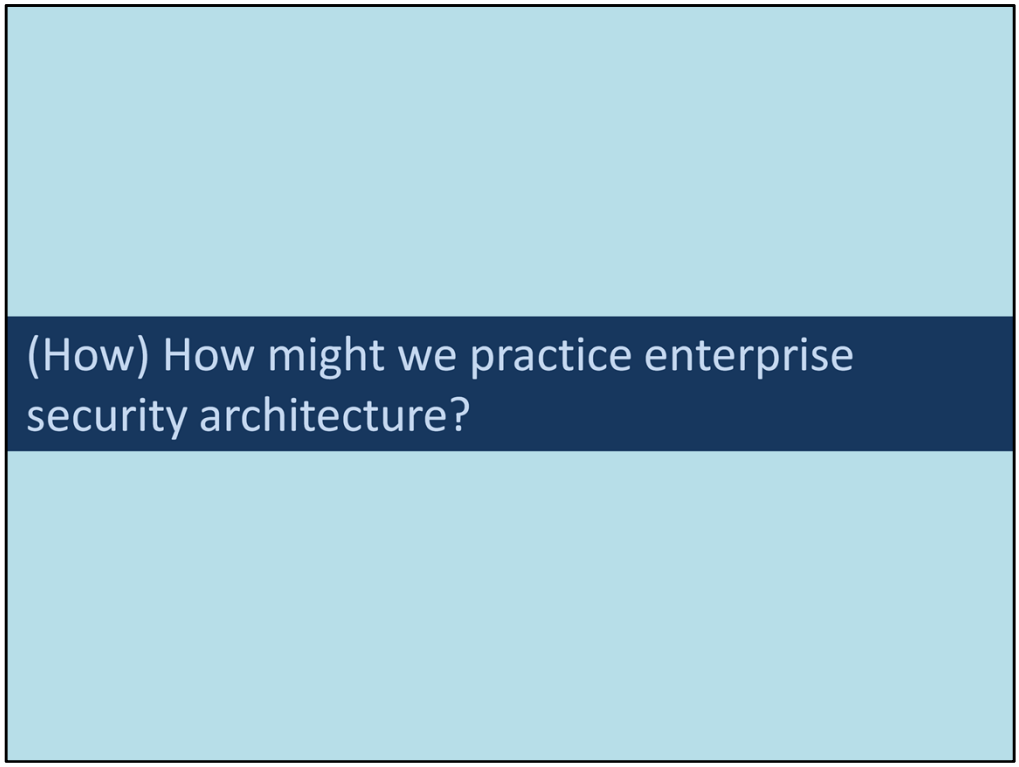
*Exhibit 2*
*The Relationship between EA Maturity and Value*




Source: Booz & Company analysis

Key message: architecture delivers more benefits the more disciplined and mature are your practices; but even newbies can realize better risk management.

Source: Building Value through Enterprise Architecture -- A Global Study. 2009. Booz & Company -- http://www.booz.com/global/home/what-we-think/reports-white-papers/ic-display/45946254




Remember the thing about unknown-unknowns? Key to meta-ignorance in the security space is select and use some framework.

## Overview of the practice elements of enterprise security architecture

- Governance and Organizational Structures
- Policies, Standards, and Procedures
- Software engineering
- Risk Management, Security Assessment
- Security Controls Design, Infrastructure, and Operation
- Reporting and Compliance

Let’s look at one of these: risk management

## Risk Management

- Risk: “a function of the likelihood of a given threat source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.” NIST SP 800-30
- Risk management is the balancing of the risks taken by the organization providing an optimal overall balance between cost, risk, and revenue.

Limits: the risk was acceptable, the loss was not. But sometimes we can only see this in hindsight.

## Risk (Impact) Categorization

| Security Objective | **Impact** of loss of security on organizational operations, organizational assets, or individuals | | |
|---|---|---|---|
| | **Low** | **Medium** | **High** |
| **Confidentiality**<br>- Prevent unauthorized disclosure of information. | Limited | Serious | Severe or catastrophic |
| **Integrity**<br>- Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. | Limited | Serious | Severe or catastrophic |
| **Availability**<br>- Ensuring timely and reliable access to and use of information. | Limited | Serious | Severe or catastrophic |

Define the criticality/sensitivity of information system or asset according to potential impact of loss of security qualities.

Source: Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100 -- http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

## NIST Risk Level

| Thread Likelihood | **Impact** of loss of security on organizational operations, organizational assets, or individuals | | |
|---|---|---|---|
| | Low (10) | Medium (50) | High (100) |
| High (1.0) | 10 | 50 | 100 |
| Medium (0.5) | 5 | 25 | 50 |
| Low (0.1) | 1 | 5 | 10 |

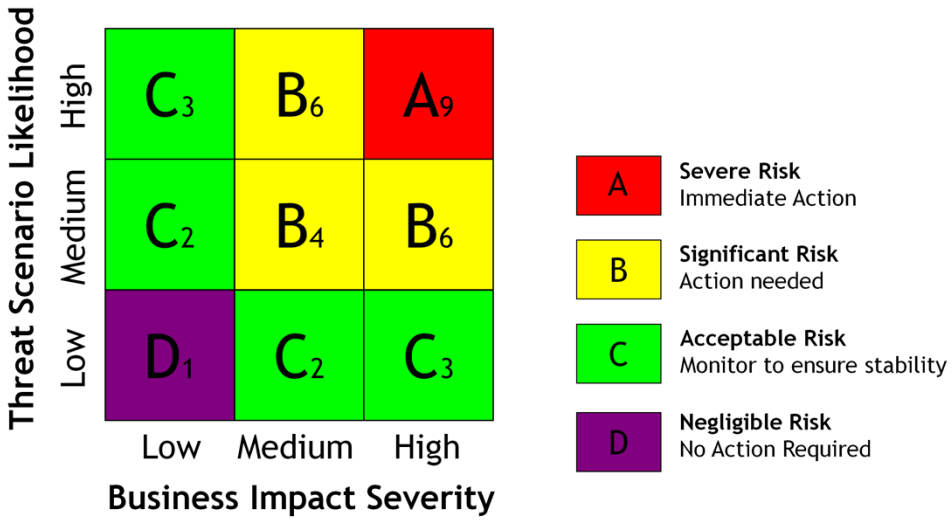
- Calculate risk level: likelihood * impact
- Risk scale (degree of risk):
  Low: 1 to 10
  Medium: >10 to 50
  High: >50 to 100

NIST goes on to prescribe different degrees of controls depending on the risk level.

We've not talked much about controls; key to remember is that when designing controls you should seek a breadth of capability that spans

- prevention,
- detection, and
- response.

# SABSA Risk Model



# The SABSA Architecture Framework

| Perspective (View) | Architectural Layer |
|---|---|
| Business | Contextual |
| Architect's | Conceptual |
| Designer's | Logical |
| Builder's | Physical |
| Tradesman's | Component |
| Service Manager's | Operational |

**SABSA is a business-driven framework to produce an enterprise security architecture**

## The SABSA Matrix

| | Assets (What) | Motivation (why) | Process (How) | People (Who) | Location (Where) | Time (When) |
|---|---|---|---|---|---|---|
| **Contextual** | The Business | Business Risk Model | Business Process Model | Business Organization and Relationships | Business Geography | Business Time Dependencies |
| **Conceptual** | Business Attributes Profile | Control Objectives | Security Strategies and Architectural Layering | Security Entity Model and Trust Framework | Security Domain Model | Security-related Lifetimes and Deadlines |
| **Logical** | Business Information Model | Security Policies | Security Services | Entity Schema and Privilege Profiles | Security Domain Definitions and Associations | Security Processing Cycle |
| **Physical** | Business Data Model | Security Rules, Practices and Procedures | Security Mechanisms | Users, Applications, and the User Interface | Platform and Network Infrastructure | Control Structure Execution |
| **Component** | Detailed Data Structures | Security Standards | Security Products and Tools | Identities, Functions, Actions, and ACLs | Processes, Nodes, Addresses, and Protocols | Security Step Timing and Sequencing |
| **Operational** | Assurance of Operational Continuity | Operational Risk Management | Security Services Management and Support | Application and User Management Support | Security of Sites, Networks, and Platforms | Security Operations Schedule |

SABSA (Sherwood Applied Business Security Architecture)

A variant of the Zachman framework.

## Enterprise Assessment Tools

Carnegie Mellon's Capability Maturity model:

| | |
|---|---|
| 0 Non-Existent | Management processes are not applied at all |
| 1 Initial | Processes are ad-hoc and disorganized |
| 2 Repeatable | Processes follow a regular pattern; tend to have project scope; reactive |
| 3 Defined | Processes have organization scope; are documented and communicated; proactive |
| 4 Managed | Processes are monitored and measured |
| 5 Optimized | Continuous improvement |

- Can also be applied to IT security controls

http://www.sei.cmu.edu/cmmi/

Similar to the COBIT 4.1 Maturity Model.

## Professional Certifications

| Certification | Organization |
|---|---|
| Professional Engineer | Association of Professional Engineers and Geoscientists of British Columbia |
| CISSP | International Information Systems Security Certification Consortium (ISC)[2] |
| CISM | Information Systems Audit and Control Association (ISACA) |
| SABSA | SABSA Limited |
| TOGAF | The Open Group |
| Enterprise Architect | various |

* Not an exhaustive list.

In the end security will be about people, especially about your.

A word about the security mindset:
* engineers tend to think about how to build things, how to make them work.
* security analyst thinks about how could things break, how to break them, and then what un-intended capabilities might be produced as a result.

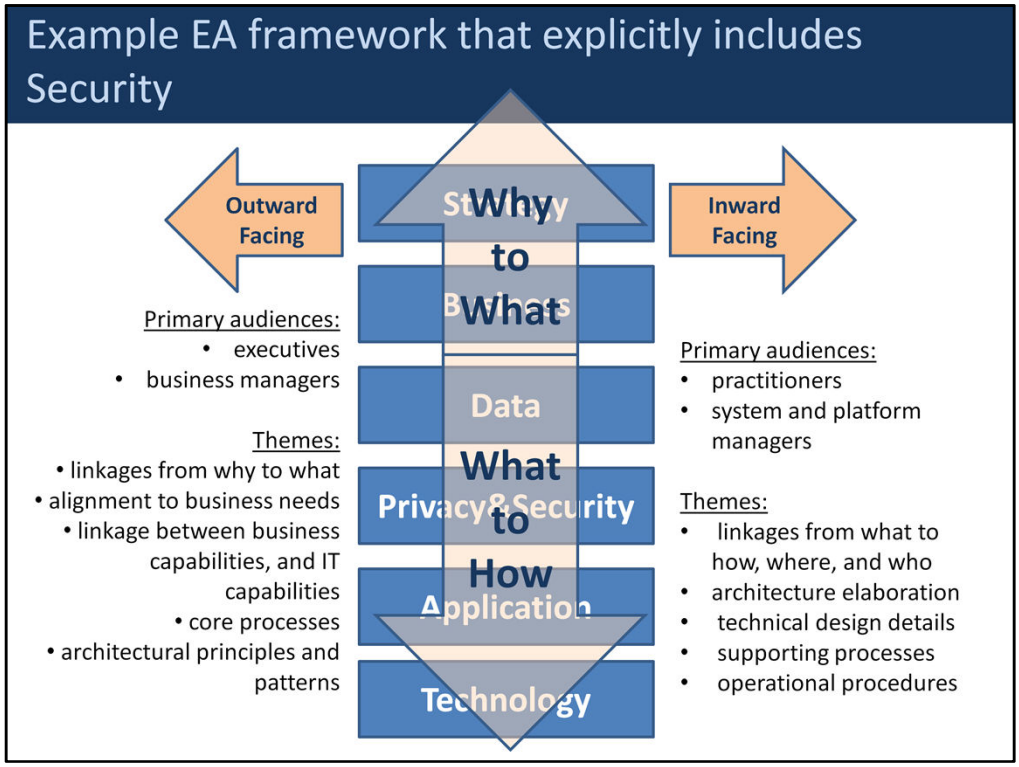
## SOAP BOX: Can you have ESA without an EA?

Given: ESA is derived from EA

Can you have an ESA without an EA?

My belief: No; security is a key perspective integrated within an EA

For example…




This EA framework developed by Glenn Mahoney; used within the Information Systems Branch, Ministry of Justice, BCGov.

(Why not) What opposes the practice of enterprise security architecture?

## We understand risk and security (and ESA)

So,

Information security is a relatively mature field with standards and effective practices emerging in the 1980's and earlier.


And yet, even with our understanding of how to secure systems, shit still happens.

## The Reality of Prevalence of Systemic Failure

- 1986: Space Shuttle Challenger disaster
- 2001: Enron Bankruptcy
- 2007/8: Subprime Mortgages and Global Financial Market Collapse
  - Structural causes of the global financial crisis: a critical assessment of the 'new financial architecture
- 2010: BP Deepwater Horizon Oil Spill
  - http://ccrm.berkeley.edu/deepwaterhorizonstudygroup/
- 2012: Algo Centre Mall Roof Collapse
- 2013: Lac-Mégantic Train Explosion
  - http://www.theglobeandmail.com/topic/Quebec%20Train%20Explosion

**Recurring theme: individuals (engineers, technologists, specialists) knew/saw problems but were not able to avert the failure**

Each of us could create such a list, and make it arbitrarily long.

James Crotty
Structural causes of the global financial crisis: a critical assessment of the 'new financial architecture' *Camb. J. Econ. (2009) 33 (4): 563-580 doi:10.1093/cje/bep023 URL: http://cje.oxfordjournals.org/content/33/4/563.short*

## What opposes the practice of enterprise security architecture?

- Denial and it's bad cousin wilful blindness -- some people don't care about security and will work till the end to preserve their (and the organization's) ignorance of the risks.
- Complication and complex systems –accumulation of technical debt from chronically insufficient engineering discipline
- Systemic lack of understanding and professional competence (see orders of ignorance)
- No risk management . (unknown unknowns)
- Consistent focus on the short-term
- Weak business leadership and naïve project management mindset that places all risk as externalities (risk dumping)
- Perverse incentives, both internal and globally

"[T]he management of information security is a much deeper and more political problem than is usually realized; solutions are likely to be subtle and partial, while many simplistic technical approaches are bound to fail"

-- Ross Anderson, *Why Information Security is Hard-An Economic Perspective*

*Why Information Security is Hard-An Economic Perspective*
By Ross Anderson, University of Cambridge, United Kingdom
Presented at 17th Annual Computer Security Applications Conference, December 10-14, 2001, New Orleans, Louisiana
URL: http://www.acsac.org/2001/papers/110.pdf

## (Why Us?) How can enterprise security architecture practitioners enable their organizations to succeed in the face of such opposition?

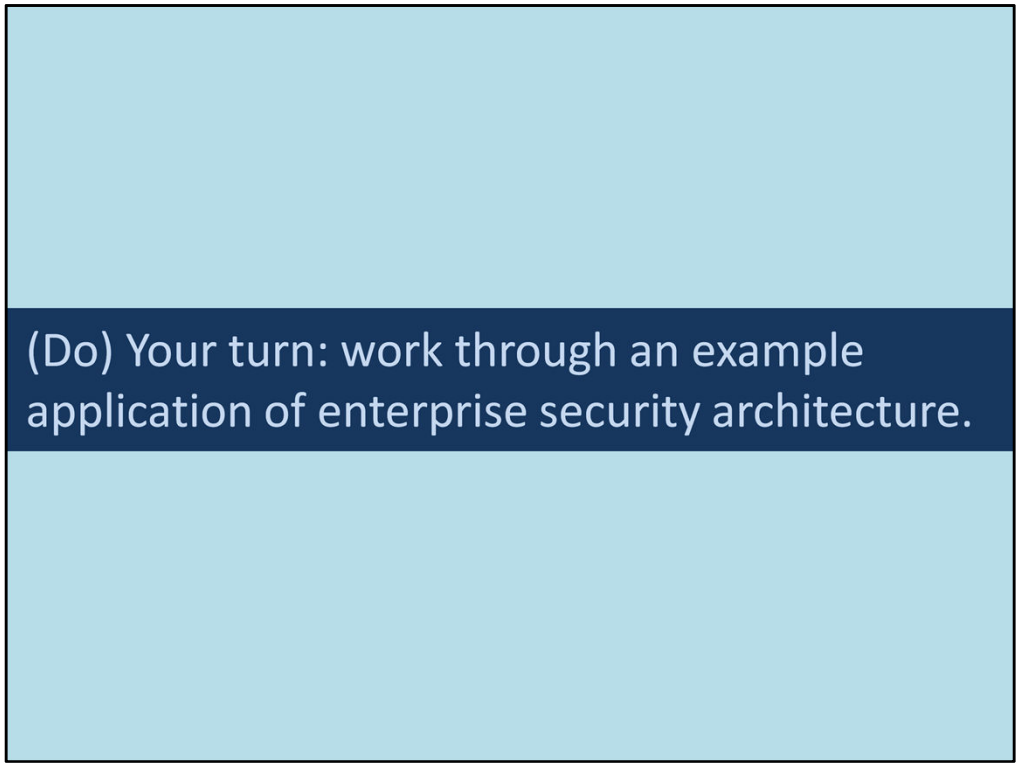
- Assume good faith, but focus on evidence of performed activities
- Be part of, in relationship with, 'the business'
- Enable 'safe' failure
- Help your auditors connect all the dots
- Be able to clearly communicate the value to whatever stakeholder you're in front of – here your ESA and associated framework is your key tool

Thus, the 'art' part of the practice of ESA.

Other resources:

- Principles for Information Security Practitioners (ISACA) - http://www.isaca.org/Knowledge-Center/Standards/Documents/Principles-for-Info-Sec-Practitioners-poster.pdf

Safe failure: when driven by demonstrated business demand, create small-scale, isolated business experiments that encapsulate excessive risk; capture the learning and demonstrated positive results in more mature follow-on changes




Enterprise

- Operating context for a set of subject assets and activities
- a set of people, processes, and technologies
- Holistic perspective
- Context for and definition of value

# Additional Material

Steven, John, "Adopting an enterprise software security framework," Security & Privacy, IEEE , vol.4, no.2, pp.84,87, March-April 2006, doi: 10.1109/MSP.2006.33

Abstract: Most organizations no longer take for granted that their deployed applications are secure. But even after conducting penetration tests, network and hosting security personnel spend considerable time chasing incidents. Your organization might be one of the many that have realized the "secure the perimeter" approach doesn't stem the tide of incidents because the software it's building and buying doesn't resist attack. A new approach offers help across the enterprise.

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1621068&isnumber=33953

Also available at http://www.cigital.com/papers/download/j2bsi.pdf

Internal controls requirements, whether federal or state, are incoherent unless and until one articulates clearly for whose benefit they exist, and to what end. There are, in fact, a number of competing articulations. The failure to identify a single and coherent rationale creates significant uncertainty, which has been exploited by players in the legal, accounting, consulting, and information technology fields.

p.950. Donald C. Langevoort. Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care as Responsibility for Systems", 31 J. Corp. L. 949-973 (2006). URL http://scholarship.law.georgetown.edu/facpub/144/