orbus software

# Information Security Integration Within the Enterprise Reference Architecture Model

## *Part 1 - Foundation*

**Guy B. Sereff**

15 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

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

# Agenda

**Fundamental Definitions and Relationships**

- Enterprise Architecture
- Enterprise Architecture Framework
- Enterprise Reference Architecture Model

**Information Security Architecture Considerations**

- Information Security Architecture
- Industry Certifications and Standards
- Information Security Architecture Framework Tools

**Case Study**

**Recommended Next Steps**

**Questions and Comments**

# Enterprise Architecture

**Holistic 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**

**Amalgamation of various architecture disciplines and domains, typically with an emphasis on technology and process optimization**

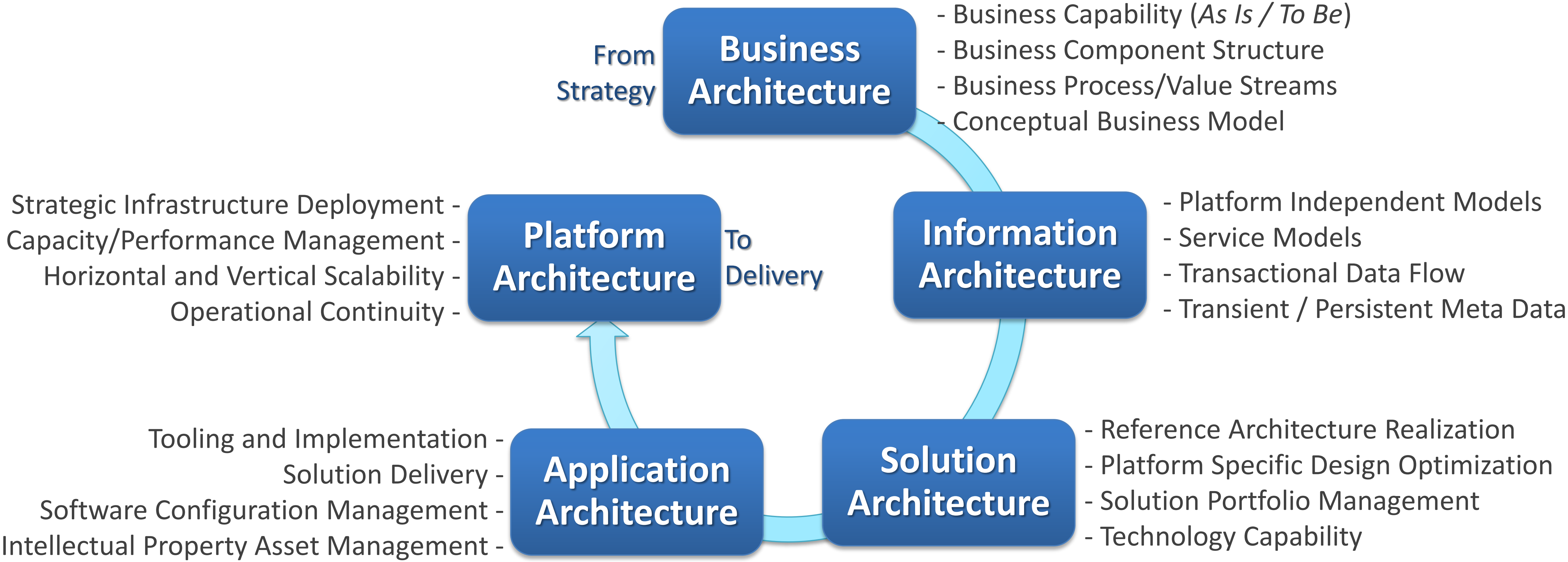
The purpose of **Enterprise Architecture** is to optimize across the enterprise the often fragmented legacy of processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the delivery of the business strategy.*

**Enterprise Architecture** (EA) is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes. EA delivers value by presenting business and IT leaders with signature-ready recommendations for adjusting policies and projects to achieve target business outcomes that capitalize on relevant business disruptions. EA is used to steer decision-making toward the evolution of the future state architecture.**

**Strategy-Centric *versus* Technology-Centric**

*TOGAF 9, © 2009; **Gartner Group, *Gartner IT Glossary - Defining the Industry, © 2012*

# Common Enterprise Architecture Domains*



From Strategy

**Business Architecture**

- Business Capability (*As Is / To Be*)
- Business Component Structure
- Business Process/Value Streams
- Conceptual Business Model

**Information Architecture**

- Platform Independent Models
- Service Models
- Transactional Data Flow
- Transient / Persistent Meta Data

**Solution Architecture**

- Reference Architecture Realization
- Platform Specific Design Optimization
- Solution Portfolio Management
- Technology Capability

**Application Architecture**

Tooling and Implementation -
Solution Delivery -
Software Configuration Management -
Intellectual Property Asset Management -

**Platform Architecture**

Strategic Infrastructure Deployment -
Capacity/Performance Management -
Horizontal and Vertical Scalability -
Operational Continuity -

To Delivery

*Sereff, *Launching an Enterprise Business Architecture Practice - A Playbook for Getting Started, © 2012*

# Enterprise Architecture Frameworks

Recognized best practices have evolved over time, encapsulated as *Enterprise Architecture Frameworks* that can help organizations bring proven structure and discipline to their Enterprise Architecture practice

Industrial Strength EA Frameworks have emerged from both the public and private sectors based on repeatable patterns of success

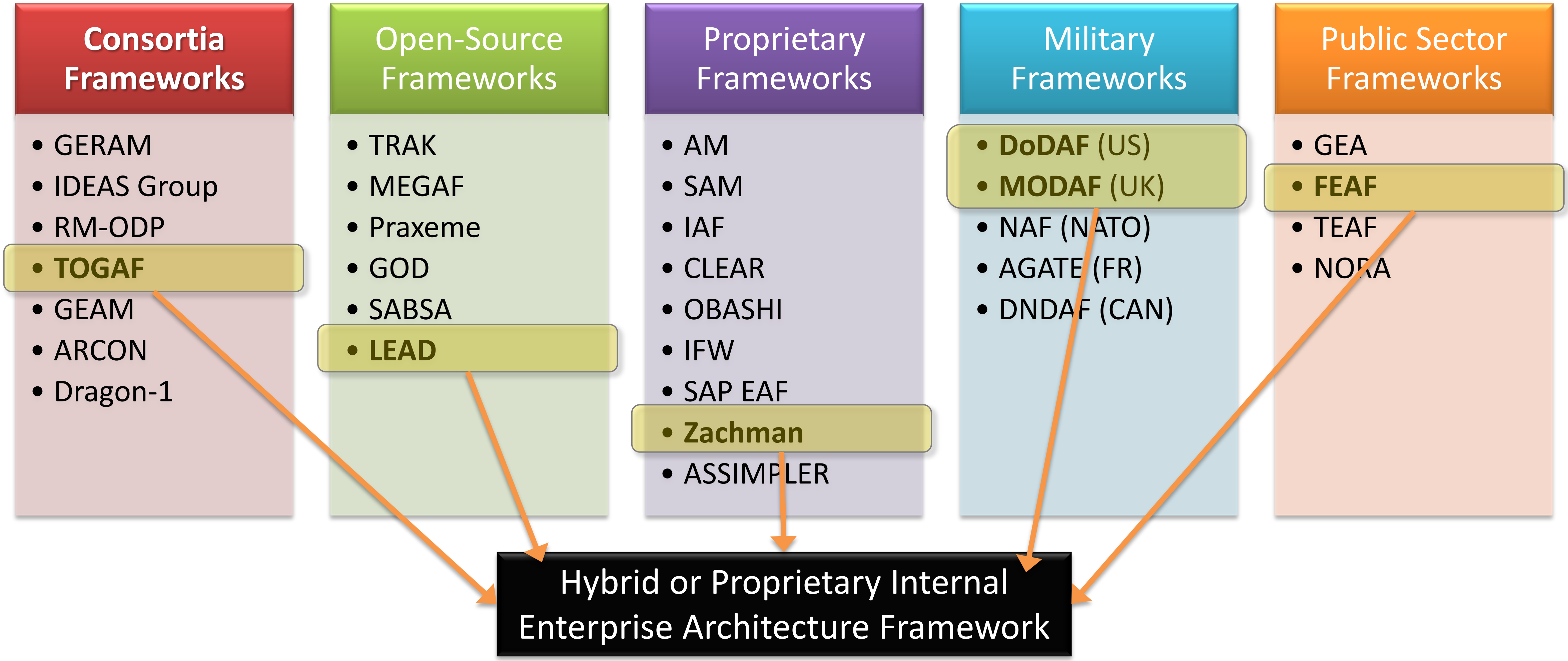
Primary Sources of EA Frameworks:

- Industry Consortiums
- Collaborative Communities (Open Source)
- Private Sector Entities
- Public Sector Entities

An **architecture framework** is a foundational structure, or set of structures, which can be used for developing a broad range of different architectures. It should describe a method for designing a target state of the enterprise in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks.*

*The Open Group, *TOGAF® Version 9, © 2009*

# Enterprise Architecture Frameworks



**Consortia Frameworks**

- GERAM
- IDEAS Group
- RM-ODP
- **TOGAF**
- GEAM
- ARCON
- Dragon-1

Open-Source Frameworks

- TRAK
- MEGAF
- Praxeme
- GOD
- SABSA
- **LEAD**

Proprietary Frameworks

- AM
- SAM
- IAF
- CLEAR
- OBASHI
- IFW
- SAP EAF
- **Zachman**
- ASSIMPLER

Military Frameworks

- **DoDAF** (US)
- **MODAF** (UK)
- NAF (NATO)
- AGATE (FR)
- DNDAF (CAN)

Public Sector Frameworks

- GEA
- **FEAF**
- TEAF
- NORA

Hybrid or Proprietary Internal Enterprise Architecture Framework

# Enterprise Reference Architecture Model

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

**Discretely articulated set of constructs, or building blocks, that define particular functional and non-functional architectural models relevant to the entity**

**Benefits**

- Variation reduction across common platforms and capability solutions (reduce valueless complexity)
- Solution Delivery acceleration
- Available repository of pre-defined and pre-approved components
- Rapid deployment of realized Service Oriented Architecture (SOA) services in a flexible cloud or cloud-like environment.

Briefly, a **reference architecture** consists of information accessible to all project team members that provides a consistent set of architectural best practices. These can be embodied in many forms: prior project artifacts, company standards, design patterns, commercial frameworks, and so forth. The mission of the reference architecture is to provide an asset base that projects can draw from at the beginning of the project life cycle and add to at the end of the project*

*Reed, © *2002*

# Common Reference Architecture Components

### Domain Meta Data

- Description
- Version
- Stakeholders

### Business Capabilities

- Client-Facing Functionality
- Transactional Tasks
- Competitive Analysis

### Architectural Approach

- Guiding Principles/Patterns
- Platform Independent Models
- Applied Industry Model(s)

### Domain Scope

- In Scope / Out of Scope
- Cross-Domain Dependencies
- Critical Success Factors

### Operational Capabilities

- Process Mapping
- Workflow Integration
- Efficiency Drivers

### Technical Components

- Platform Specific Model
- Approved Components
- Buy/Hold/Sell Technical Assets

### Strategy

- Disruptive vs. Adoptive Approach
- Strategic End State
- Targeted Competency Level

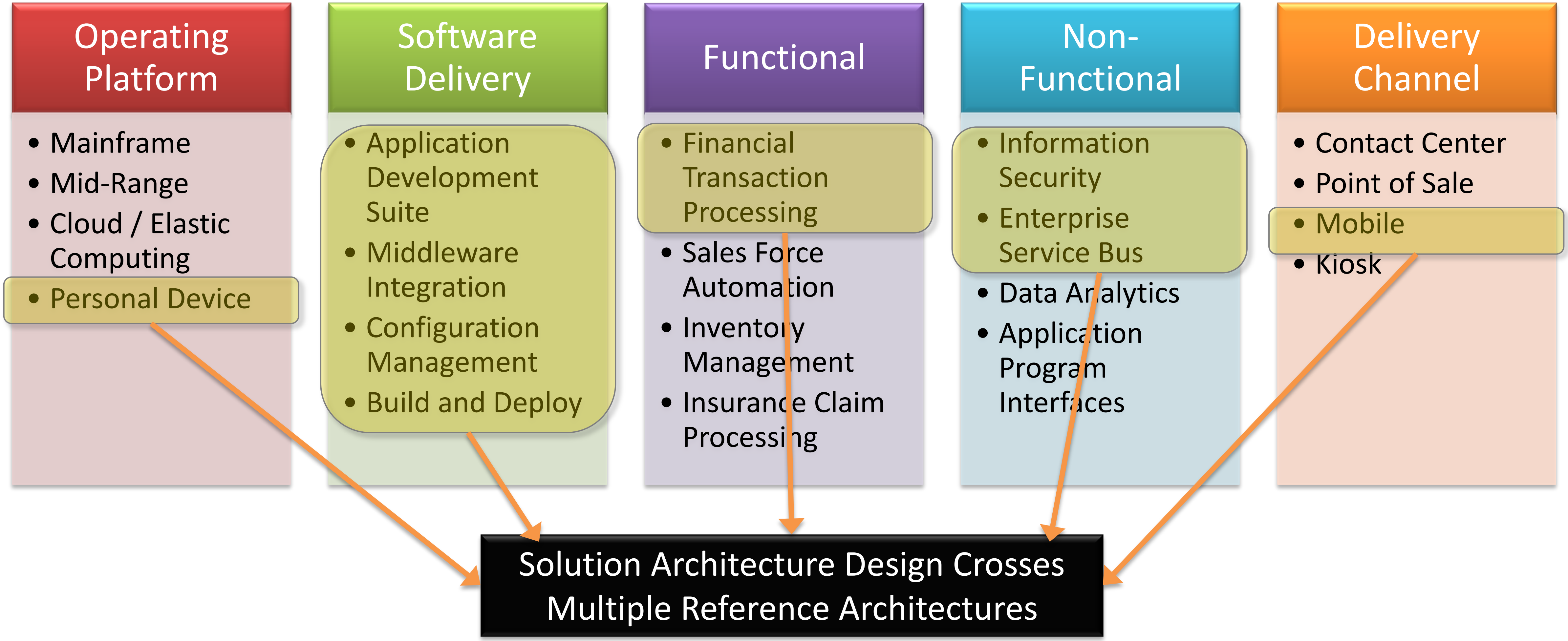
### System Capabilities

- Functional
- Non-Functional
- Information Flow

### Conformance Roadmap

- Current State Analysis
- End State Conformance Timeline
- Program Alignment

# Typical Reference Architecture Domains



## Operating Platform

- Mainframe
- Mid-Range
- Cloud / Elastic Computing
- Personal Device

## Software Delivery

- Application Development Suite
- Middleware Integration
- Configuration Management
- Build and Deploy

## Functional

- Financial Transaction Processing
- Sales Force Automation
- Inventory Management
- Insurance Claim Processing

## Non-Functional

- Information Security
- Enterprise Service Bus
- Data Analytics
- Application Program Interfaces

## Delivery Channel

- Contact Center
- Point of Sale
- Mobile
- Kiosk

Solution Architecture Design Crosses Multiple Reference Architectures

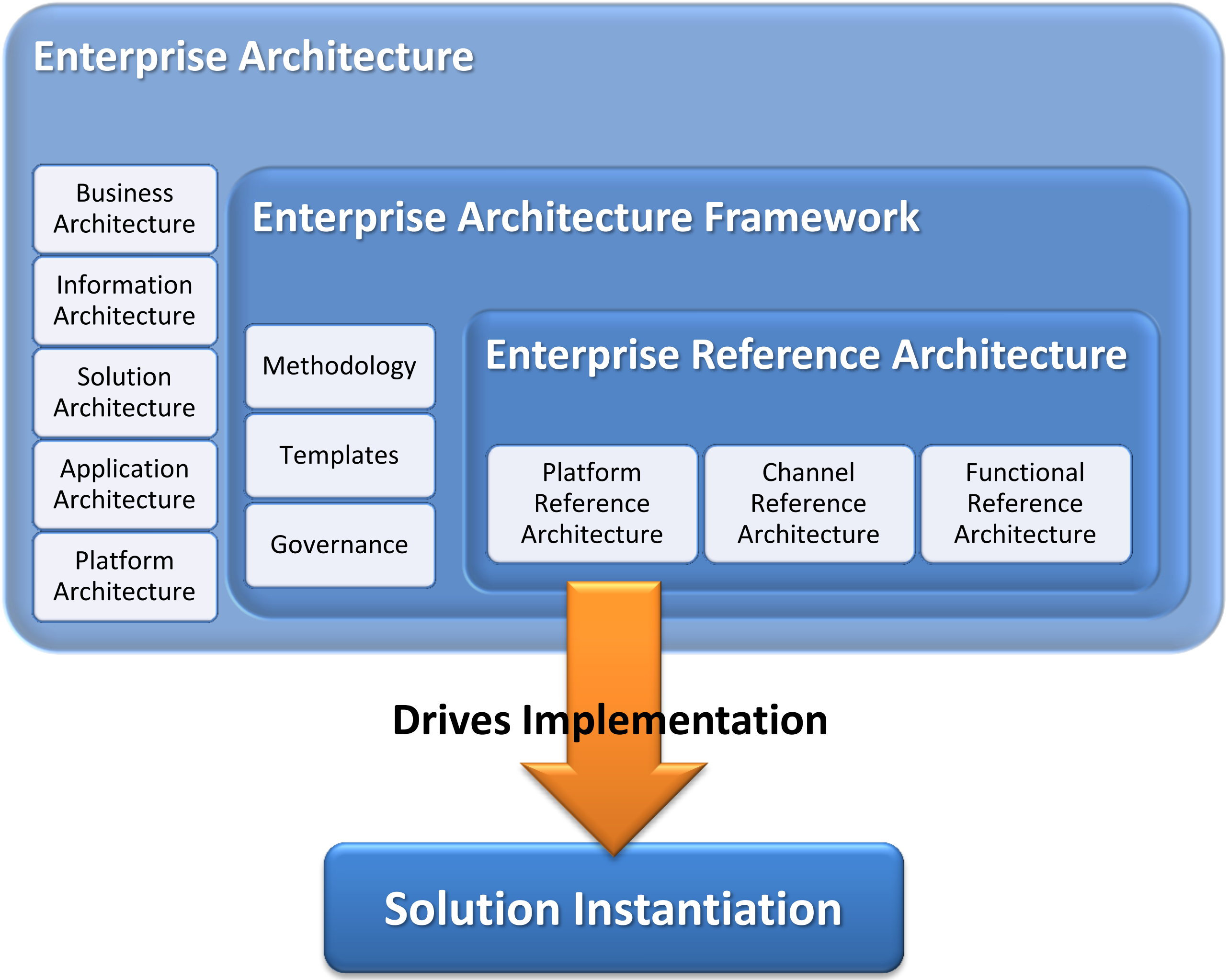
# Contextual View

*Enterprise Architecture* domains provide strategic points of view through various lenses

*Enterprise Architecture Frameworks* support the Enterprise Architecture Practice with consistent methodologies, templates and governance mechanisms

*Enterprise Reference Architecture* models provide consumable design accelerants and implementation standards to guide and govern solution delivery

Advancement towards the *Enterprise Reference Architecture Roadmap* can be measured and tracked over time to assess conformance velocity and missed opportunities



# Enterprise Information Security Architecture

**Holistic view of Information Security across all aspects of the enterprise and risk mitigation, both from outside the digital perimeter and from within**

**Critical to understand, establish and execute an effective risk assessment, prioritization and threat neutralization strategy**

**How secure is *secure enough*?**

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 Information Security Architecture (EISA)** is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well.**

Risk-Centric *versus* Technology-Centric

*Sherwood *et al*, © 2005; **World Wizzy, © *2012*

# Common Information Security Strategy Components

Communication Channels

Acquisition Integration / Divestiture Segregation

Operational Business Processes

Discrete Security Operations

Disaster Recover / Business Continuity

Compliance and Policies

Projects and Change Management

Physical Security

Security Architecture and Design

Platform / Channel Specific Considerations

Identity Verification / Entitlement Management

Vulnerability Management

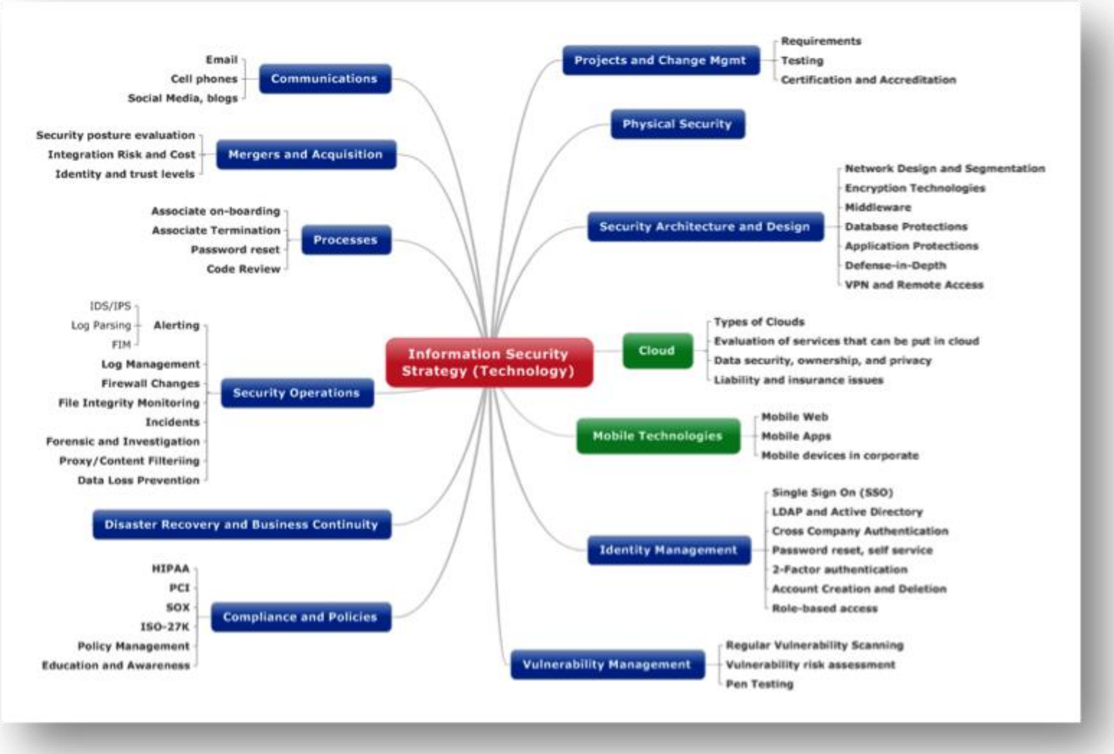


Image: Rehman, © 2011

# Information Security Certifications

Several bodies of Information Security knowledge have emerged, resulting in documented *best practices* and professional certifications

Certified resources can help an organization quickly establish an *Enterprise Information Security Center of Excellence*

*Note:* Information Security certifications are generally *not* industry specific or business contextually aware

Example Certifications: International Information Systems Security Certification Consortium, or (ISC)2®*

- **CISSP**: *Certified Information Security Professional*
- **CAP**: *Certified Authorization Professional*
- **SSCP**: *Systems Security Certified Practitioner*
- **CSSLP**: *Certified Secure Software Lifecycle Professional*
- **CCFP:** *Certified Cyber Forensic Professional*

**CISSP Domains**

- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

**CAP Domains**

- Understand the Security Authorization of Information Systems
- Categorize Information Systems
- Establish the Security Control Baseline
- Apply Security Controls
- Assess Security Controls
- Authorize Information System
- Monitor Security Controls

**CCFP Domains**

- Legal and Ethical Principles
- Investigations
- Forensic Science
- Digital Forensics
- Application Forensics
- Hybrid and Emerging Technologies

**SSCP Domains**

- Access Controls
- Security Operations and Administration
- Monitoring and Analysis
- Risk, Response and Recovery
- Cryptography
- Networks and Communications
- Malicious Code and Activity

**CSSLP Domains**

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design

*(ISC)²®, © 1996-2013

# Information Security Architecture and TOGAF®*

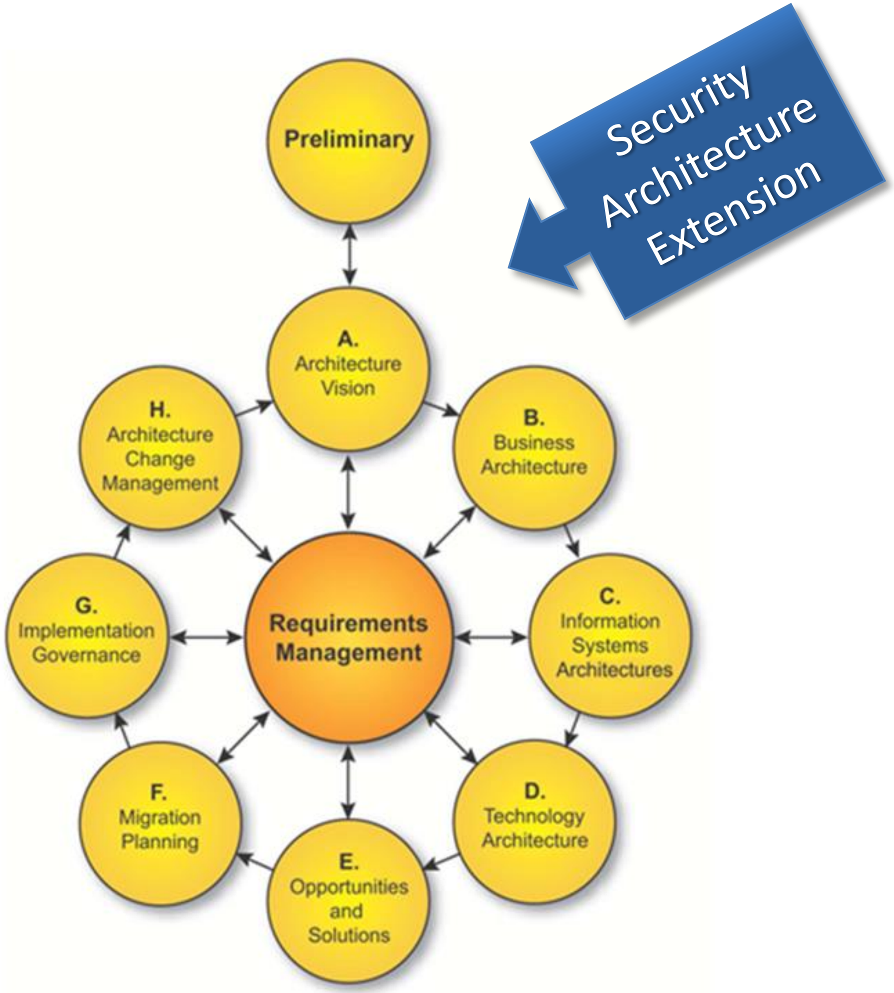
***Security Architecture*** **first introduced into TOGAF 8 as a supplemental white paper**
*(Guide to Security Architecture in TOGAF ADM - 2005)*

**Security Architecture formally added to TOGAF 9**
*(See Chapter 21)*

**Specific *Security Architecture* steps are defined for each of the nine TOGAF phases, including Key Considerations, Inputs and Outputs**

**TOGAF further defines eight suggested areas Security Architects should focus on when considering *Security Architecture***

***Note*** **- TOGAF addresses *Security Architecture* as an *extension* to each phase, which may not convey the high level of criticality to the overall Enterprise Architecture definition**


Security Architecture Extension
Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

*TOGAF 9, © 2009

# TOGAF Recommended Security Architecture Areas*

**Authentication**

- The substantiation of the identity of a person or entity related to a system in some way

**Authorization**

- The definition and enforcement of permitted capabilities for a person or entity whose identity has been established

**Audit**

- The ability to provide forensic data attesting that the system was used in accordance with stated security policies

**Assurance**

- The ability to test and prove that the system has the security attributes required to uphold the stated security policies

**Availability**

- The ability of the system to function without service interruption or depletion despite abnormal or malicious events.

**Asset Protection**

- The protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use.

**Administration**

- The ability to add and change security policies, add or change how policies are implemented in the system, and add or change the persons or entities related to the system.

**Risk Management**

- The organization's attitude and tolerance for risk. (This risk management is different from the special definition found in financial markets and insurance institutions that have formal risk management departments)

*TOGAF 9, © 2009

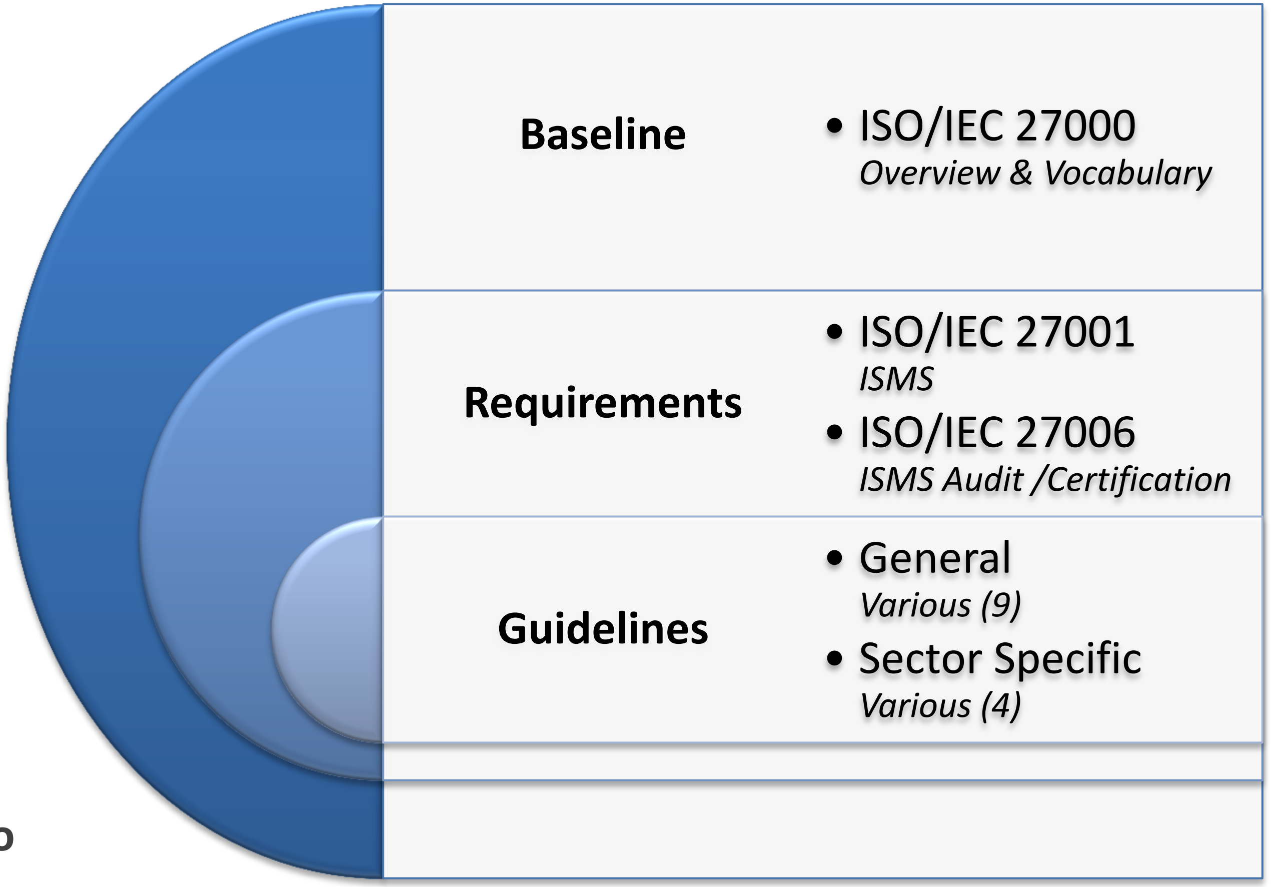
# ISO / IEC 27000 Information Security Management Systems*

ISO/IEC jointly published Information Security standards based on best practices observed across industries and geographic boundaries

Represents a body of information security knowledge referred to as the *Information Security Management System* (ISMS) family of standards

These standards include audit and certification criteria, which may be an important consideration or distinction in certain industries or settings – No guarantee but provides an objective Information Security assessment

*Suggestion*: Review ISO/IEC 27000:2012 to get an overview of each of the subsequent standards to determine their applicability to your organization and to glean best practices



**Baseline**

- ISO/IEC 27000
  *Overview & Vocabulary*

**Requirements**

- ISO/IEC 27001
  *ISMS*
- ISO/IEC 27006
  *ISMS Audit /Certification*

**Guidelines**

- General
  *Various (9)*
- Sector Specific
  *Various (4)*

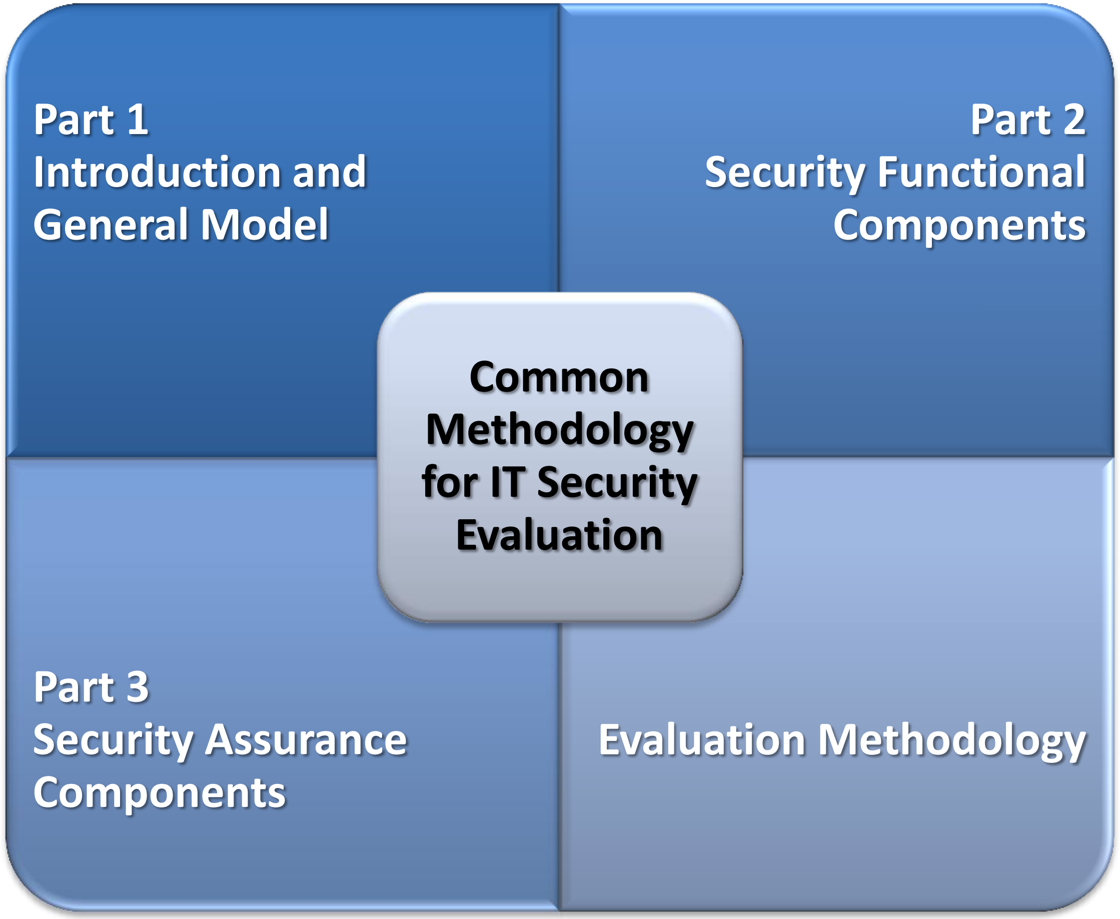
*ISO/IEC, © 2012

# National Information Assurance Partnership*

Established as a coalition between the public and private sectors to validate how well IT products adhere to certain security-related international Information Security standards

*Common Criteria Evaluation and Valuation Scheme* (CCEVS) published as a series of documents that provide a means of evaluating the security capabilities of software products

Organizations can evaluate and potentially enhance the software-related components of their Information Security Architecture by reviewing NAIP's CCEVS publications and applying the specified criteria to their own platforms



Part 1
Introduction and General Model

Part 2
Security Functional Components

Common Methodology for IT Security Evaluation

Part 3
Security Assurance Components

Evaluation Methodology

*NAIP, © 2012

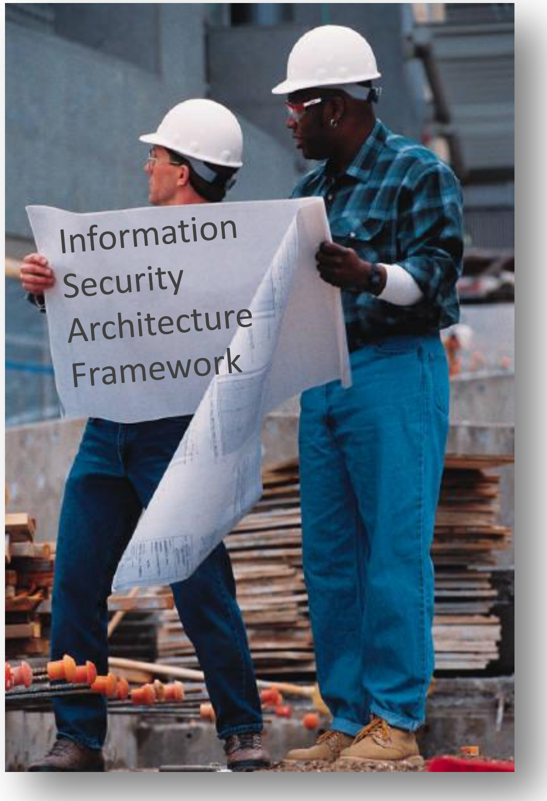
# Information Security Architecture Frameworks

Just as there are *Enterprise Architecture Frameworks* available, there are also *Information Security Architecture Frameworks* as well

Some *Information Security Frameworks* are industry-centric, such as the *HITRUST Common Security Framework (CFS)*, which is focused on Healthcare, while other frameworks are more universal, such as IBM's *Information Security Framework (ISF)*

Some Information Security Frameworks, such as the *Sherwood Applied Business Security Architecture (SABSA)* are aligned to and designed for a particular Enterprise Architecture Framework (i.e. Zachman)

No framework works right out of the box – there is a significant amount of work ahead, but the framework acts as a blueprint to establishing the Information Security Architecture content (policies, practices, procedures and oversight)



# SABSA: Sherwood Applied Business Security Architecture[*]

**SABSA model is an independent extension of the *Zachman Framework* metamodel**

**Thoroughly describes and defines risks and threats from an Information Security perspective**

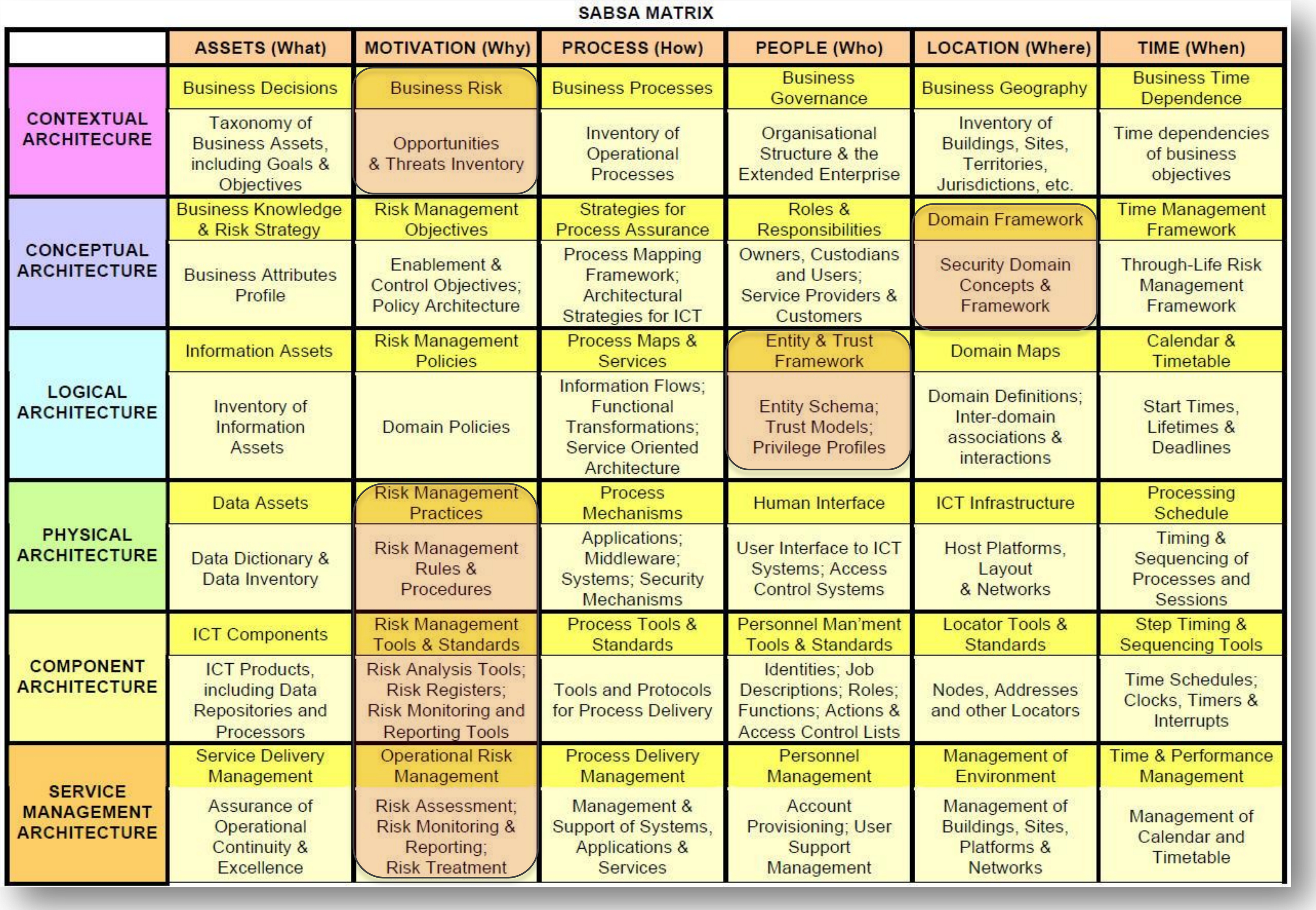
**The SABSA Matrix applies ‘what-why-how-who-where-when’ points of view to each architectural layer**

- Builds a comprehensive set of artifacts that essentially outline the organization’s Information Security Architecture
- Solid tool for assessing and defining the organization’s Information Security model from a business and risk management perspective
- Whether SABSA is formally adopted or not, it can be used to compare an organization’s existing approach to confirm topical coverage and to identify potential gaps that need to be addressed

| **SABSA** | **Zachman Framework[**]** |
|---|---|
| Contextual Security Architecture | Scope (Contextual) Planner |
| Conceptual Security Architecture | Business Model (Conceptual) Owner |
| Logical Security Architecture | System Model (Logical) Designer |
| Physical Security Architecture | Technology Model (Physical) Builder |
| Component Security Architecture | Detailed Representations (Out-of-Context) Subcontractor |
| Operational Security Architecture | Functioning Enterprise |

*Sherwood *et al*, © 2009; ** Zachman, © 2013

# SABSA Matrix



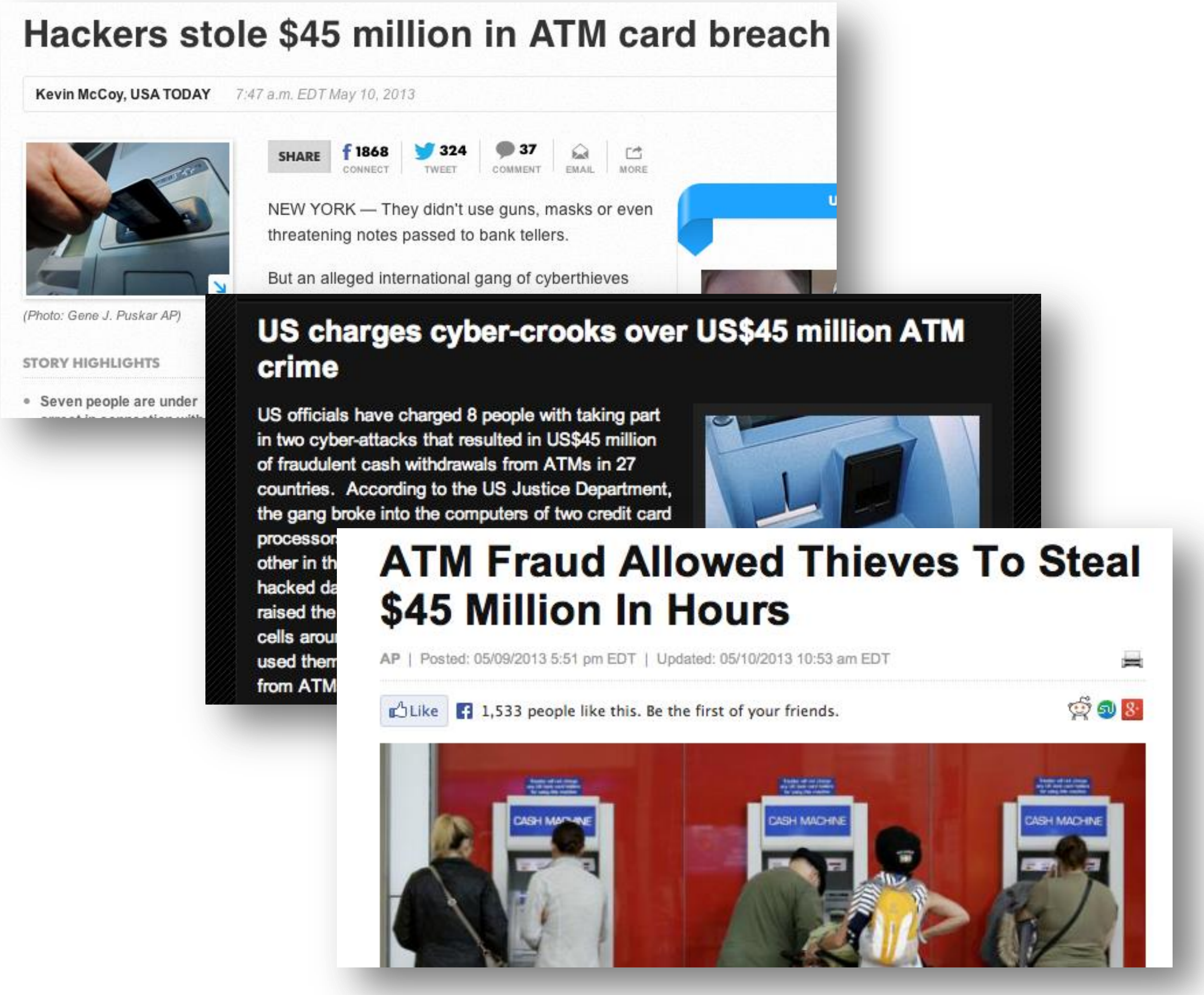
SABSA MATRIX

| | ASSETS (What) | MOTIVATION (Why) | PROCESS (How) | PEOPLE (Who) | LOCATION (Where) | TIME (When) |
|---|---|---|---|---|---|---|
| CONTEXTUAL ARCHITECURE | Business Decisions | Business Risk | Business Processes | Business Governance | Business Geography | Business Time Dependence |
| | Taxonomy of Business Assets, including Goals & Objectives | Opportunities & Threats Inventory | Inventory of Operational Processes | Organisational Structure & the Extended Enterprise | Inventory of Buildings, Sites, Territories, Jurisdictions, etc. | Time dependencies of business objectives |
| CONCEPTUAL ARCHITECTURE | Business Knowledge & Risk Strategy | Risk Management Objectives | Strategies for Process Assurance | Roles & Responsibilities | Domain Framework | Time Management Framework |
| | Business Attributes Profile | Enablement & Control Objectives; Policy Architecture | Process Mapping Framework; Architectural Strategies for ICT | Owners, Custodians and Users; Service Providers & Customers | Security Domain Concepts & Framework | Through-Life Risk Management Framework |
| LOGICAL ARCHITECTURE | Information Assets | Risk Management Policies | Process Maps & Services | Entity & Trust Framework | Domain Maps | Calendar & Timetable |
| | Inventory of Information Assets | Domain Policies | Information Flows; Functional Transformations; Service Oriented Architecture | Entity Schema; Trust Models; Privilege Profiles | Domain Definitions; Inter-domain associations & interactions | Start Times, Lifetimes & Deadlines |
| PHYSICAL ARCHITECTURE | Data Assets | Risk Management Practices | Process Mechanisms | Human Interface | ICT Infrastructure | Processing Schedule |
| | Data Dictionary & Data Inventory | Risk Management Rules & Procedures | Applications; Middleware; Systems; Security Mechanisms | User Interface to ICT Systems; Access Control Systems | Host Platforms, Layout & Networks | Timing & Sequencing of Processes and Sessions |
| COMPONENT ARCHITECTURE | ICT Components | Risk Management Tools & Standards | Process Tools & Standards | Personnel Man'ment Tools & Standards | Locator Tools & Standards | Step Timing & Sequencing Tools |
| | ICT Products, including Data Repositories and Processors | Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools | Tools and Protocols for Process Delivery | Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists | Nodes, Addresses and other Locators | Time Schedules; Clocks, Timers & Interrupts |
| SERVICE MANAGEMENT ARCHITECTURE | Service Delivery Management | Operational Risk Management | Process Delivery Management | Personnel Management | Management of Environment | Time & Performance Management |
| | Assurance of Operational Continuity & Excellence | Risk Assessment; Risk Monitoring & Reporting; Risk Treatment | Management & Support of Systems, Applications & Services | Account Provisioning; User Support Management | Management of Buildings, Sites, Platforms & Networks | Management of Calendar and Timetable |

# Case Study - 2013 Global ATM Heist

**Sophisticated crime involving alleged *insider system manipulation* and *fraudulent exploitation* of known vulnerabilities**

- Global Network of operatives in nearly 30+ Countries
- Orchestrated Timeline
  - October 2012 - System Breach Prep Work
  - December 2012 - ‘Trial Run’ nets USD 5MM
  - February 2013 - ‘Synchronized Assault’ nets an additional USD 40MM
- Targeted Institutions had transactional security mechanisms that were known to be weak within a ‘secure’ ecosystem
- Sophistication increased up through the crime perpetrator pyramid, including global transaction monitoring and funds recovery tracking
- Swift synchronized concurrent attacks on the system took hours to detect and prevent both times



Hackers stole $45 million in ATM card breach

Kevin McCoy, USA TODAY 7:47 a.m. EDT May 10, 2013

(Photo: Gene J. Puskar AP)

STORY HIGHLIGHTS

- Seven people are under

NEW YORK — They didn't use guns, masks or even threatening notes passed to bank tellers.

But an alleged international gang of cyberthieves

US charges cyber-crooks over US$45 million ATM crime

US officials have charged 8 people with taking part in two cyber-attacks that resulted in US$45 million of fraudulent cash withdrawals from ATMs in 27 countries. According to the US Justice Department, the gang broke into the computers of two credit card processor other in th hacked da raised the cells arou used them from ATM

ATM Fraud Allowed Thieves To Steal $45 Million In Hours

AP | Posted: 05/09/2013 5:51 pm EDT | Updated: 05/10/2013 10:53 am EDT

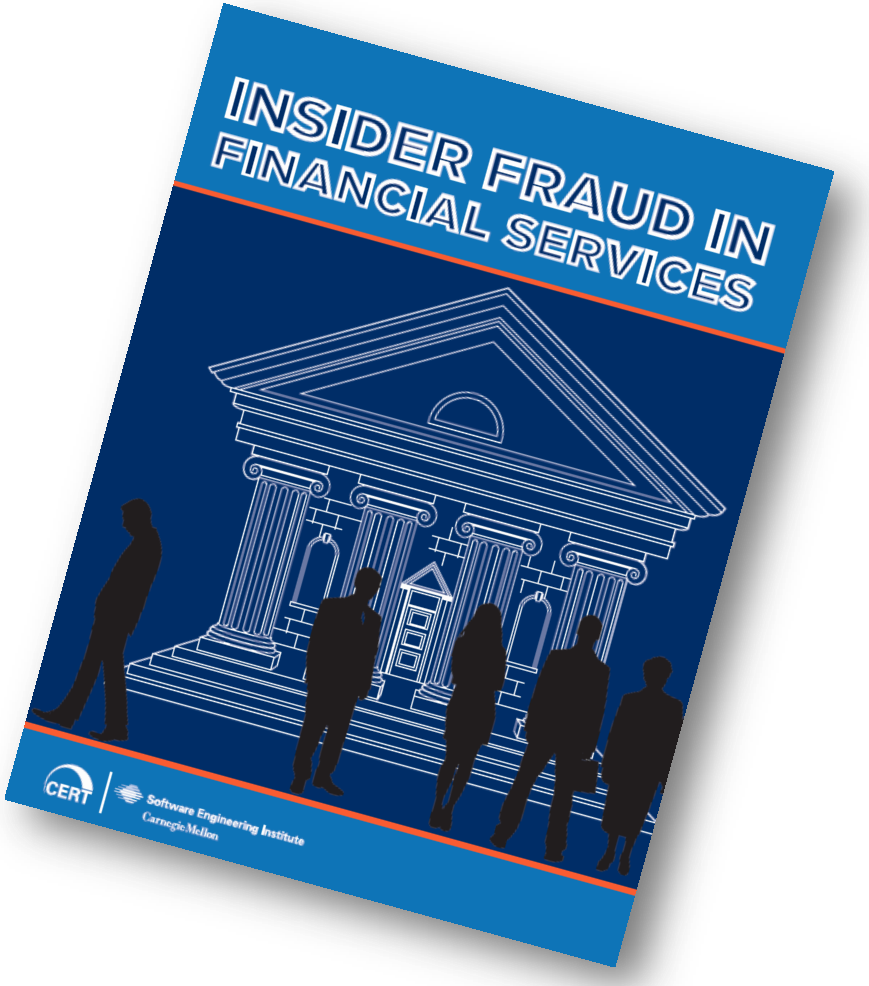
Like 1,533 people like this. Be the first of your friends.

Sources: USA Today, ATM Security Pro, Huffington Post, © 2013

# Too Late for Them; What About Your Organization?

**In 2012, Carnegie Mellon's *Software Engineering Institute* offered the following recommendations related to insider fraud management:***

- Clearly document and consistently enforce policies and controls
- Institute periodic security awareness training for all employees
- Include unexplained financial gain in any periodic reinvestigations of employees
- Log, monitor, and audit employee online actions
- Pay special attention to Accountants and Managers
- Restrict access to personally identifiable information
- Develop an *Insider Incident Response Plan*


INSIDER FRAUD IN FINANCIAL SERVICES
CERT
Software Engineering Institute
Carnegie Mellon

*SEI, Insider Fraud in Financial Services, © 2012

# Recommended Next Steps

- Evaluate existing Enterprise Architecture practices and governance mechanisms
- Evaluate the existing Information Security Architecture definitions, polices and procedures – shore up critical risks and vulnerabilities
- Ensure security fraud prevention and fraud detection techniques address threats from both outside <u>*and*</u> inside the organization's perimeter
- Join us for ***Part 2 – Implementation***, where we'll we'll put these foundational principles to work in the form of the *Enterprise Reference Architecture Model* and as an integral part of the *Solution Delivery Process*

Remember the words of John Grisham's fictional character Bill DeVasher from *The Firm*:
**"I get paid to be suspicious when I've got nothing to be suspicious about"**[*]

*Grisham, *The Firm*, © 1992

# Any Questions?

Orbus Software Group

@OrbusSoftware

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

# Thank You!