CE879 - Information Security Mng. & Eng.

Lecture 6: Enterprise Security Architecture

Seyedeh Atefeh Musavi / Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology
Spring 1404

S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content.

What is the problem?

S4Lab

- Enterprise security is a challenging task.
- Technical complexity
- None-technical problems:
  - Organizational complexities
  - Cultural complexities
  - Evolving nature of protection solutions
  - Different jurisdiction
  - Continuous progress/competence vs compliance
- Enterprise security architecture frameworks help in handling these complexities.

Technical complexities

Different security requirements

S4Lab

- A majority of organizations are quoting between two and five solutions on average, while 25% report having over five solutions in place.
- Complexity and cost of managing hybrid (on-premises and cloud/ mobile) network connectivity and security result in either paralysis or sub-optimal investments.

[Image: https://www.enmarq.com/services/enterprise-security/]

[Top Networking and Security Challenges in the Enterprise, Global Industry Report,2016]

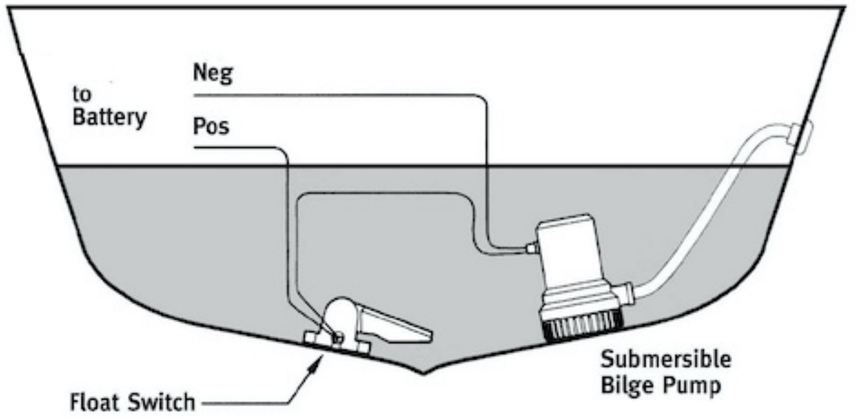
New technological needs

S4Lab

- Faded enterprise perimeters:
  - Distributed through multiple buildings in multiple countries
  - Cloud services and outsourced computations
  - Mobile devices and BYOD policies
  - Multiple partnership with other enterprises and interactions
- Legacy technologies are not designed for such dynamic businesses.
- Lack of skilled employees: e.g. How much you know about using these technologies to secure an enterprise network?
  - VPN?
  - MPLS?
  - SD-WAN (MPLS and internet) ?

Evolving nature of protection solutions

S4Lab



[Image: https://www.discoverboating.com/]

- Let's start with boat design philosophy.
- The original simple design philosophy:
  - Separate the water from the interior of the boat.
  - A single tree trunk.
  - Joints were sealed with pitch or other sealants.
  - Boats still leaked, but was tolerable.
- Boats got more complex.
  - Still leaked, not much, but just enough that it limited the range or speed, or time in the water without maintenance.
- Then an epiphany occurred.
  - Drains and channels were added to funnel water to an area, the bilge.
  - A well-sealed boat was still required because a high-leakage rate could overwhelm bilge capacity.

[Simpson, W. R., Enterprise level security: securing information systems in an uncertain world, CRC Press, 2016]

IT systems security design philosophy

S4Lab

- No security issues at first :)
- Then Intruders penetrated unprotected systems.
  - Boundary protection, boundary monitors, and boundary countermeasures improved.
- However as systems became more complex, these were not sufficient.
- Now is the time for an epiphany.
  - We need to design internal traps and funnels and move intruders toward discovery so they can be eliminated, and the doors and windows revealed by penetration can be closed.
- However, the system will be penetrated again through another unclosed door.

[Simpson, W. R., Enterprise level security: securing information systems in an uncertain world, CRC Press, 2016]

Organizational/cultural complexities

Organizational challenges

S4Lab

- Different teams (units) with different goals/deadlines.
  - Security is a non-functional goal, not in the goals of teams.
- No willingness to spend sufficient budget dedicated for security.
  - Small corporates have limited resources and outsource.
  - Big corporations require complex plans which is expensive.
- Change in large enterprises is slow and painful.
  - Hence, any security solution (a product/ a process) is not easy to apply.

Organizational challenges (con't)

S4Lab

- For many years, one of the biggest challenges facing a chief security officer (CSO) was "having a regular seat at the table." Dave Komendat, CSO of Boeing.
- Challenges between C-level executives.
- Chief financial officers (CFOs) and chief operating officers (COOs) are the most common executives in the C-suite.
- Chief information security officers (CISOs) are a unique C-level breed. Historically, they've been two-steps away from CEOs, reporting to CIOs.
  - Times are a changing for CISOs, and they are starting to receive C-suite invitations.

https://www.csoonline.com/article/3228886/should-cisos-join-ceos-in-the-c-suite.html

The root for the organizational challenge

S4Lab

- The reality is that a lack of visibility for CSOs within their company was not uncommon.
- Due to a general lack of understanding with the CEO about what a CSO should do and how security should be run, CSOs got a pass for many years.
- They were never expected to run security “like a business”.
- In many ways the adage “no news is good news” was all a CEO needed to believe that their CSO and security program was doing a good job.

[Campbell, George. Measuring and Communicating Security's Value: A Compendium of Metrics for Enterprise Protection. Elsevier, 2015.]

CSO’s horror stories!

S4Lab

- “What do you say to CXOs to help them understand security?
- Security horror story is a universal answer!
  - A well-defined tool of the trade.
- “FUD factor.” A FUD factor is the level of fear, uncertainty, and doubt that the audience for a security horror story feels upon hearing it.
- When CXO is motivated to spend on security?
  - Experience FUD (incidents), not listening to a story!
- Managers rose in the ranks precisely because they were not afraid of anything.
  - Most CXOs I know, don't really believe security horror stories will happen on their watch.

[Bayuk, J., Enterprise Security for the Executive: Setting the Tone from the Top, PSI Business Security, 2009]

Why many CXOs are now immune to FUD?

S4Lab

- A large institution had a huge problem with Social Security and credit card-number theft, and corresponding identity theft.
- The security group :
  - Business operations used un-secure methods of sending and receiving PII via the Internet.
  - Security product vendors advised deploying network listening devices between their internal network and everywhere it touched the Internet.
  - Talked to the CXO, who agrees to buy ($5 million) after incident report.
- Consulting the legal department for a procedure on what they should do:
  - They should automatically stop the transmission of the data.
  - However, the equipment could only report! To stop -> an additional $8 million☺
  - They also should turn off the reporting technology!
- CXO discovered this folly, all new security projects were put on hold.

[Bayuk, J., Enterprise Security for the Executive: Setting the Tone from the Top, PSI Business Security, 2009]

What to do?

S4Lab

- They gave the security department the benefit of the doubt to come up with solutions that would solve a business problem.
- While the security department was instead concentrating on projects to implement one type of security technology.
- CXOs demand more insight into the security solutions presented to them.
- CXOs are also often motivated by the belief that reasonable security should cost less than currently budgeted amounts.
- What to do ?
  - Simple risk assessment ? How to find accurate estimation.
  - Best practice approach? One fits all approach.
- On the opposite end of the security management spectrum is a holistic view of security, in which security management systemically aligns with business strategy.

[Bayuk, J., Enterprise Security for the Executive: Setting the Tone from the Top, PSI Business Security, 2009]

Cultural complexities (1)

S4Lab

- Different people with different cultures see things differently.
  - How to respond and the level of transparency in handling incidents?
  - Individuals may live in a region with different regulations.
- Security policies are misunderstood in a special cultural context
  - Separating the office into different security zones, each requiring authentication, may be well received in Western countries such as the United States but Eastern countries like Japan may find this rude and untrustworthy.

[https://www.tcdi.com/culture-interfering-data-security/]

Cultural complexities(2)

S4Lab

- Different cultures in openness and sharing ideas.
  - Employees from multiple regions working on a single project or the same data will need to follow appropriate procedures to ensure they are complying.
- Language barriers can present difficulties if security procedures and policies are misunderstood in another country.

[https://www.tcdi.com/culture-interfering-data-security/]

Security compliance complexities

Security compliance

S4Lab

- Although for most businesses security is not a top business priority it remains as a constant item on the boardroom agenda.
- Security and risk management are often viewed by the business as a compliance chore.
- A cost to the business and/or an operational expense
  - May not bode well for their ability to secure investments from the business to support these activities.
- In fact, some enterprise security efforts are performed not because of its own need, but its due to regulations which is mandated on behalf of other stakeholders.

[Security – Enterprise Architecture, Deloitte, 2018]

Scandals started the story

S4Lab

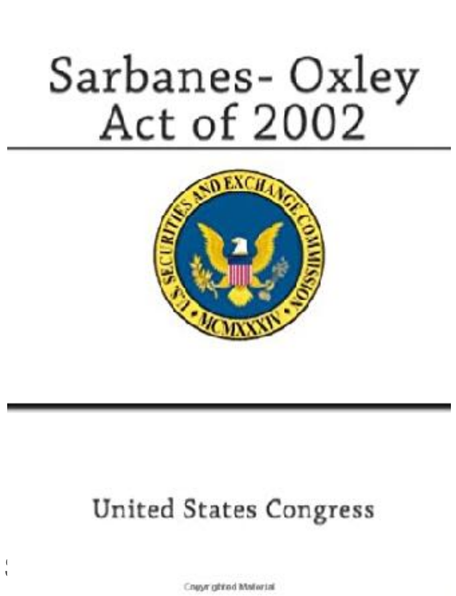
- Enron engaged in mark to market (MTM) accounting.
  - Allows companies to value their financial situation based on the"fair value" of the company's assets, which may change as market conditions change.
- Enron overinflated the company's estimated profits and mislead investors.
- To hide its mounting debt, Enron used special purpose vehicles (SPVs: shell companies capitalized entirely by Enron stock) to borrow money on Enron's behalf
- By 2001, Enron had used hundreds of SPVs to hide its debt.
- In the end, many of Enron's executives were charged for insider trading, securities fraud, and conspiracy,
- Enron's collapse prompted President George W. Bush to sign into law the Sarbanes-Oxley Act:
  - A law designed to protect investors from corporations' fraudulent accounting activities.

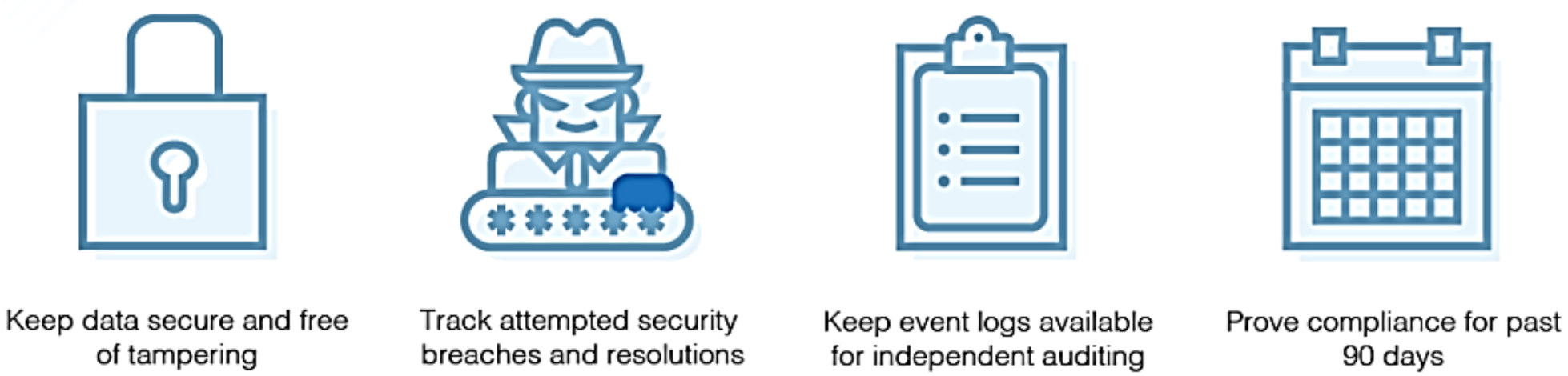
[http://large.stanford.edu/courses/2018/ph240/smith1/]

The Sarbanes-Oxley Act

S4Lab

- The damages associated with the burst of the dot-com bubble beginning in 2000, an event to which many of these fraud scandals contributed, “[destroyed] $6.2 trillion in household wealth over the next two years
- While the details of the Sarbanes-Oxley Act are complex, “SOX compliance” refers to the annual audit in which a public company is obligated to provide proof of accurate, data-secured financial reporting.





[https://www.dnsstuff.com/what-is-sox-compliance]

The Sarbanes-Oxley Act

S4Lab

- SOX sections 302, 404 and 409 require the following parameters and conditions must be monitored, logged, and audited:
  - Internal controls
  - Network activity
  - Database activity
  - Login activity (success and failures)
  - Account activity
  - User activity
  - Information Access
- SOX auditing requires that "internal controls and procedures" can be audited using a control framework like COBIT. Log collection and monitoring systems must provide an audit trail of all access and activity to sensitive business information.

[https://www.sarbanes-oxley-101.com/sarbanes-oxley-audits.htm]

Similar requirements in EU

S4Lab

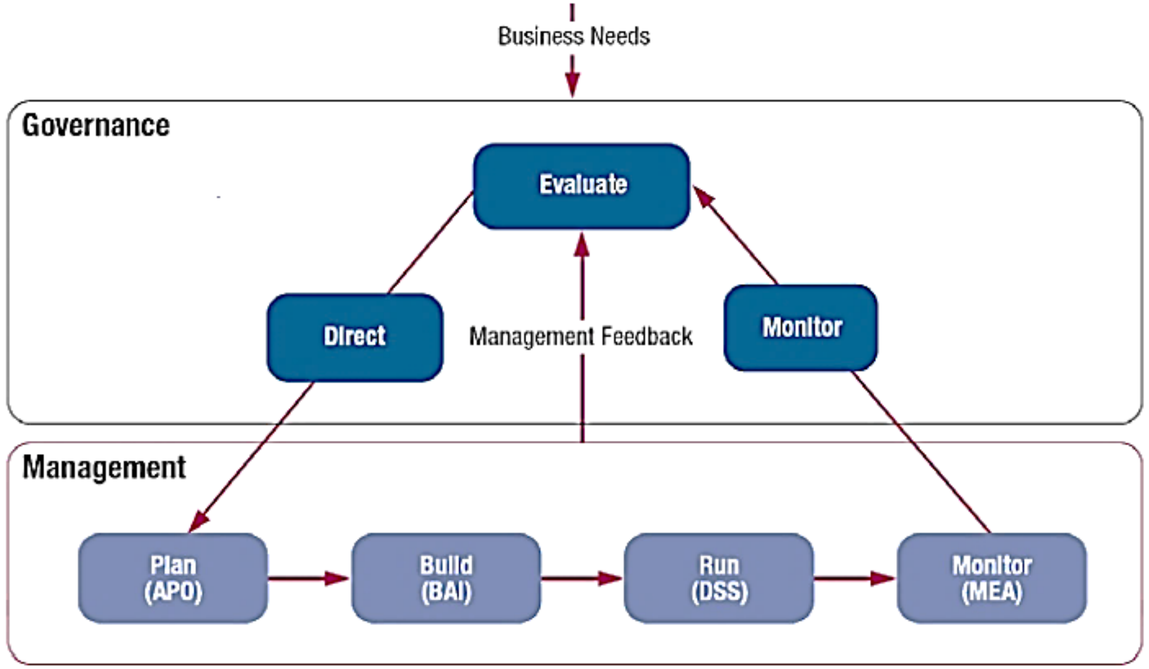
- EU Directives on the Award of Public Contracts.
- There are EU Directives that require vendors involved in Public Contracts to show that they are using formal enterprise architecture processes within their businesses when supplying products and services.

[Josey A., TOGAF® Version 9.1-A Pocket Guide. Van Haren, 2016]

IT Governance (ITG) frameworks

S4Lab

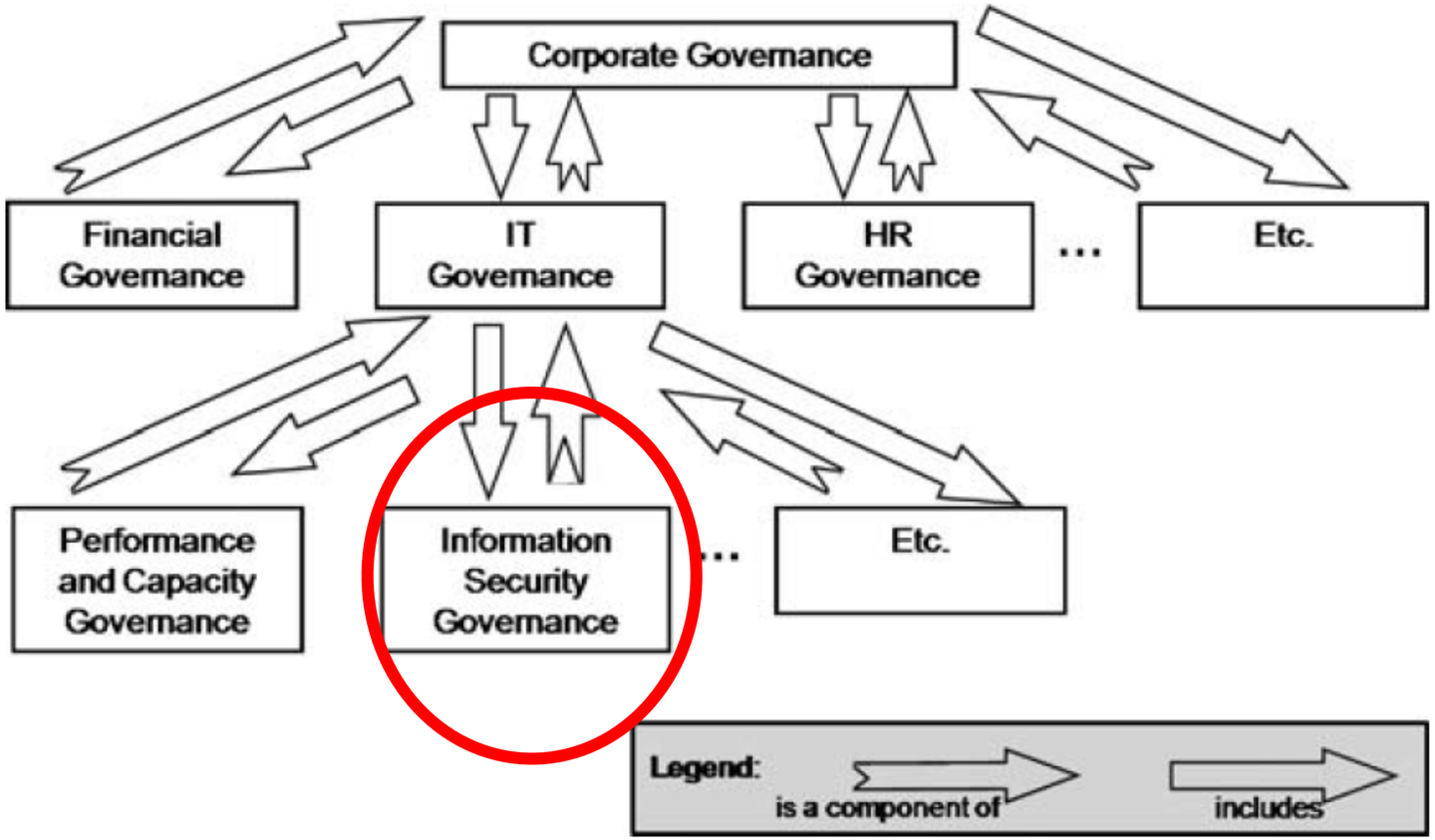
- IT management services provide day-to-day management and operation of IT assets and processes.
- IT governance (ITG) is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.



[White Paper COBIT 5 – An Introduction, Orbus Software, 2014]

The Components of IT Governance

S4Lab

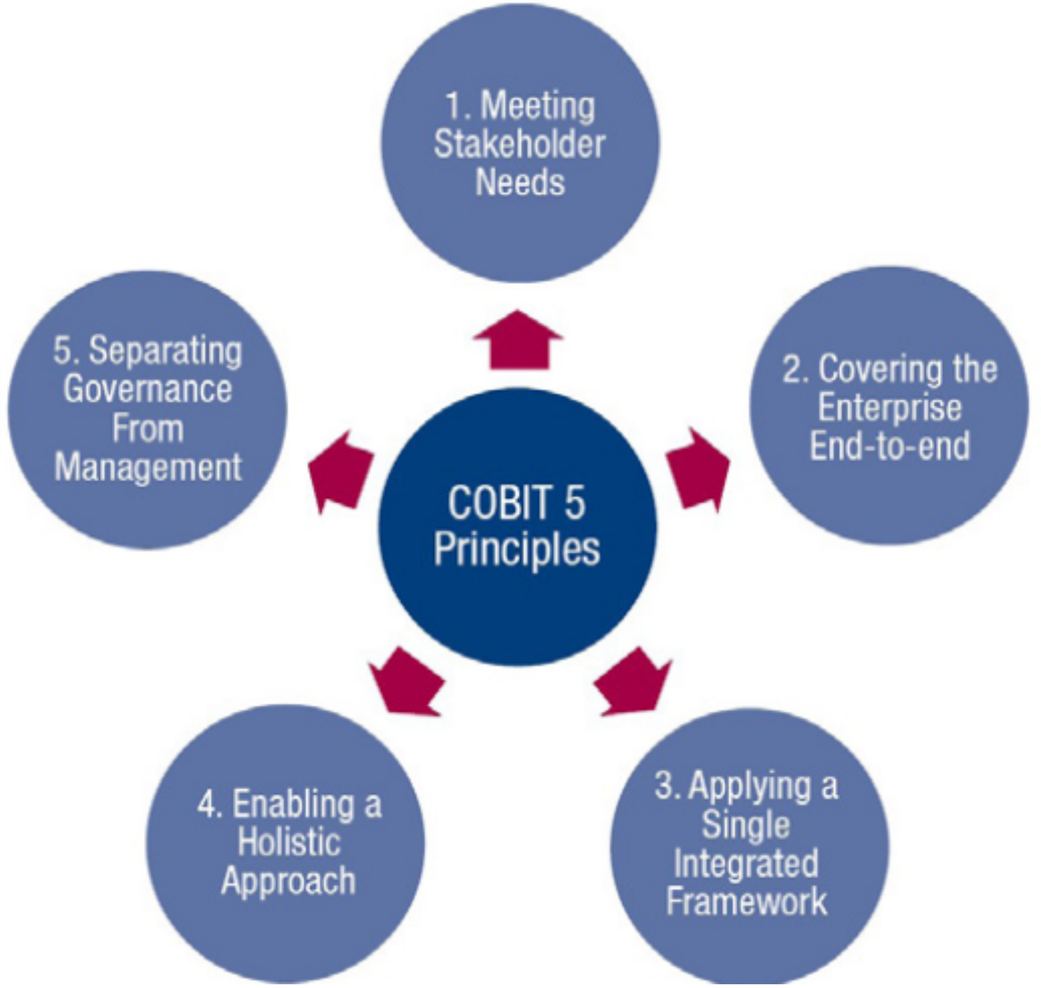


[Solms S. V., & Solms R., Information security governance. Springer Science & Business Media, 2008]

COBIT

S4Lab

- COBIT stands for Control Objectives for Information and Related Technology.
- Created by the ISACA (Information Systems Audit and Control Association) .
- ISACA is an international professional association focused on IT governance.



[White Paper COBIT 5 – An Introduction, Orbus Software, 2014]

COBIT processes

S4Lab

- Basic idea behind COBIT, is to divide the ITG into 34 high-level IT processes.
- Each of these 34 high-level processes is again divided into a set of supporting Control Objectives (COs).
  - COs are the more detailed ‘actions’ which must be managed to properly manage the relevant high level process.
- These processes are divided into four domains:
  - Plan and Organize (PO)
  - Acquire and Implement (AI)
  - Deliver and Support (DS)
  - Monitor and Evaluate (ME)
- COBIT sees Information Security as an integral part of ITG.

[Solms S. V., & Solms R., Information security governance. Springer Science & Business Media, 2008]

COBIT domain 1

S4Lab

- Domain 1: Plan and Organize with ten processes (PO 1 to PO 10):
  - PO1 Define a Strategic IT Plan
  - PO2 Define the Information Architecture
  - PO3 Determine Technological Direction
  - PO4 Define the IT Processes, Organization and Relationships
  - PO5 Manage the IT Investment
  - PO6 Communicate Management Aims and Direction
  - PO7 Manage IT Human Resources
  - PO8 Manage Quality
  - PO9 Assess and Manage IT Risks
  - PO10 Manage Projects.

[Solms S. V., & Solms R., Information security governance. Springer Science & Business Media, 2008]

COBIT domain 2

S4Lab

- Domain 2: Acquire and Implement with seven processes (AI 1 to AI 7):
  - AI1 Identify Automated Solutions
  - AI2 Acquire and Maintain Application Software
  - AI3 Acquire and Maintain Technology Infrastructure
  - AI4 Enable Operation and Use
  - AI5 Procure IT Resources
  - AI6 Manage Changes
  - AI 7 Install and Accredit Solutions and Changes.

[Solms S. V., & Solms R., Information security governance. Springer Science & Business Media, 2008]

COBIT domain 3

S4Lab

- Domain 3: Deliver and Support with 13 processes (DS 1 to DS 13):
  - DS1 Define and Manage Service Levels
  - DS2 Manage Third-Party Services
  - DS3 Manage Performance and Capacity
  - DS4 Ensure Continuous Service
  - DS5 Ensure Systems Security
  - DS6 Identify and Allocate Costs
  - DS7 Educate and Train Users
  - DS8 Manage Service Desk and Incidents
  - DS9 Manage the Configuration
  - DS10 Manage Problems
  - DS11 Manage Data
  - DS12 Manage the Physical Environment

[Solms S. V., & Solms R., Information security governance. Springer Science & Business Media, 2008]

COBIT domain 4

S4Lab

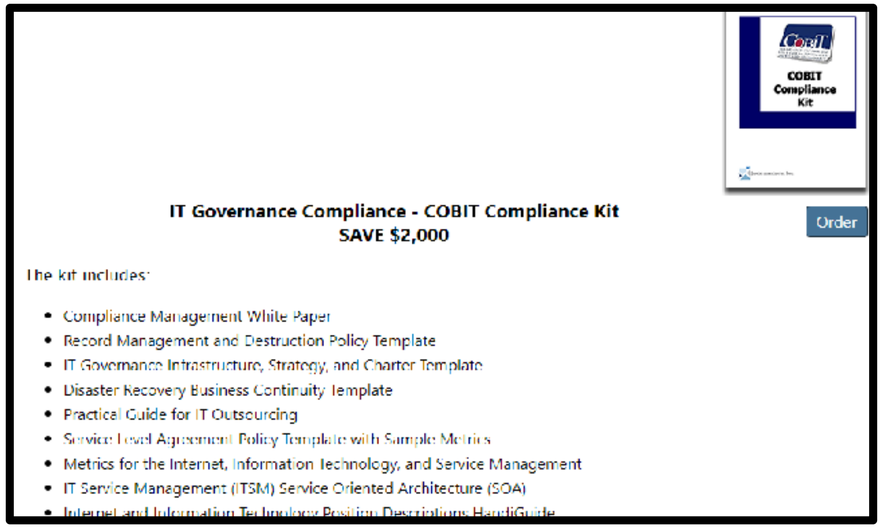
- Domain 4: Monitor and Evaluate with four processes (ME 1 to ME 4):
  - ME1 Monitor and Evaluate IT Performance
  - ME2 Monitor and Evaluate Internal Control
  - ME3 Ensure Compliance with External Requirements
  - ME4 Provide IT Governance.

[Solms S. V., & Solms R., Information security governance. Springer Science & Business Media, 2008]

IT Governance Compliance Kits

S4Lab

- Include different items:
  - Record Management and Destruction Policy Template
  - IT Governance Infrastructure, Strategy, and Charter Template
  - Disaster Recovery Business Continuity Template
  - Practical Guide for IT Outsourcing
  - Service Level Agreement Policy Template with Sample Metrics
  - Metrics for the Internet, Information Technology, and Service Management
  - Internet and Information Technology Position Descriptions HandiGuide
  - Security Policies and Procedures Template
  - Security Audit Program
  - ….

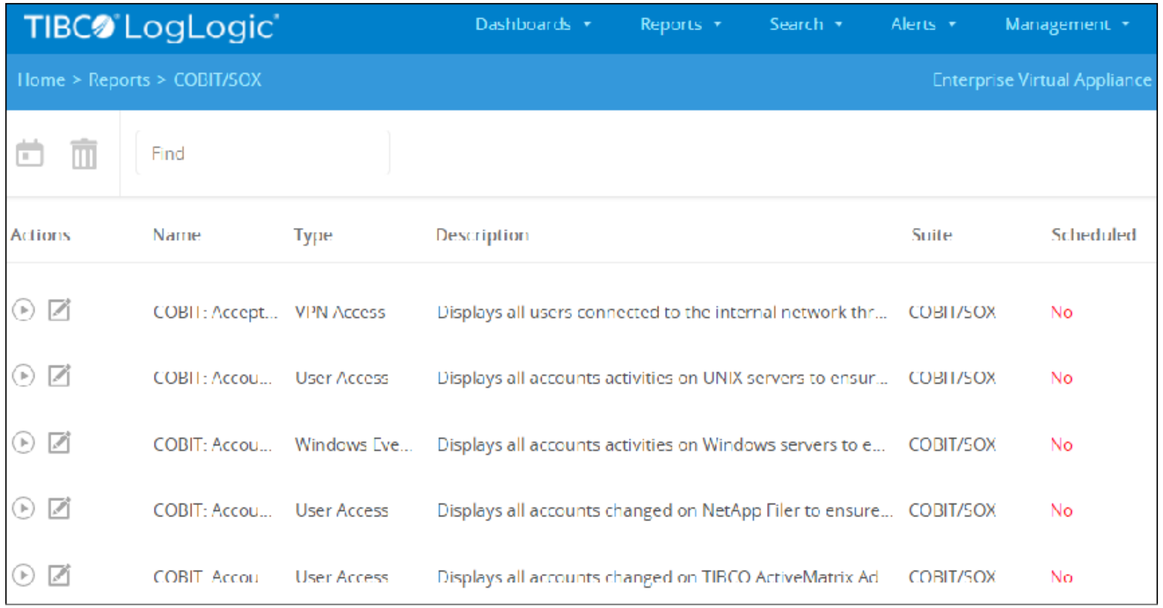


[ISO 27001 Toolkit]

SIEM tools

S4Lab

- SIEM: SIM & SEM
- SIM: System Information Management.
- SEM: Security Event Management
- CAN BE used as compliance tool for different standards and frameworks.
  - Often Include predefined templates for each framework.



[Image:LogLogic Compliance Suite - SOX Edition Guidebook]

Enterprise architecture frameworks

A way to manage complexities in big enterprises

Definitions

- Enterprise: as any collection of organizations that has a common set of goals.
  - A government agency, a whole corporation, a division of a corporation, a single department, or a chain of geographically distant organizations linked together by common ownership
- Architecture: 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

[TOGAF - Frequently Asked Questions]

What is the problem?

S4Lab

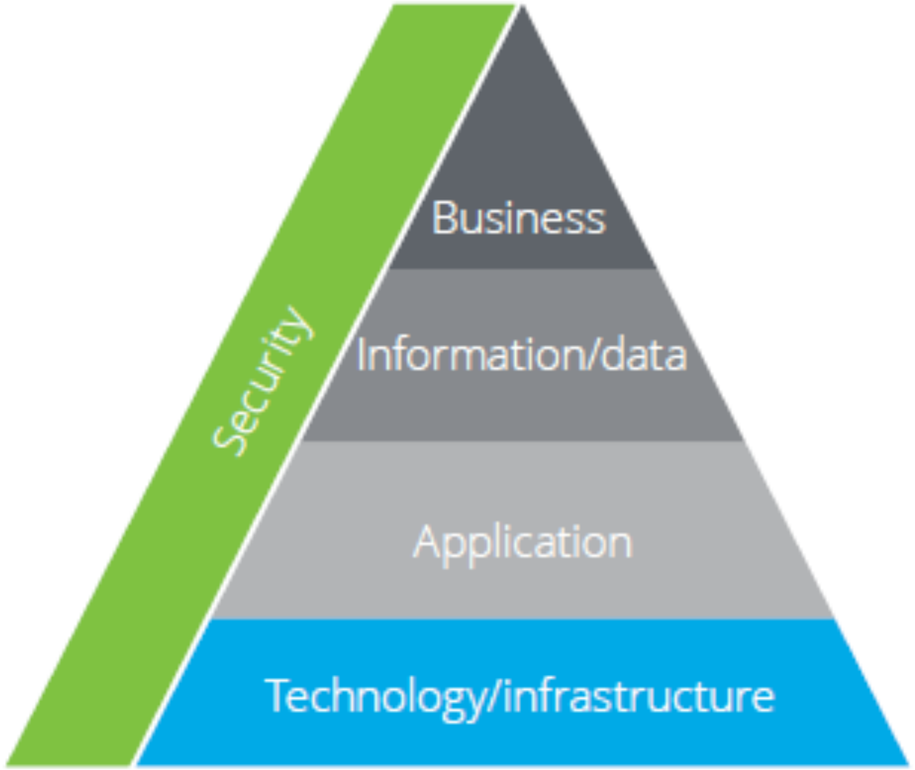
- Security teams aim to protect digital assets in any enterprise.
- In practice, they should solve a number of problems:
  - There are plethora of security tools for different defensive tools with low/null integration.
  - We need a mechanism to see the relations of these tools with regards to their placement throughout the enterprise to be able to find holes.
  - Business layer chiefs decide at the end where to spend money and which solution is more important.
  - So there should be a shared language.

[Security – Enterprise Architecture, Deloitte, 2018]

Why security + business?

S4Lab

- Where are digital assets ?
  - Pervasive throughout the enterprise different at layers.
  - Difficult to be identified, protected, or to perform risk assessment without knowledge on business layers.
- As commonly seen in enterprises, the information security capability functions separately from the Enterprise Architecture of the organization.
- To achieve this, it is necessary to include security in Enterprise Architecture approach.
- Plans are nothing; planning is everything!



[Security – Enterprise Architecture, Deloitte, 2018]

Architecting a city or an enterprise?

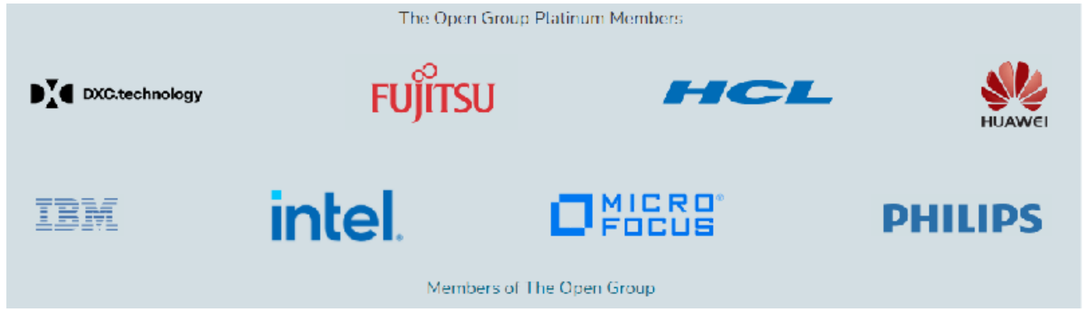
S4Lab

- Complexity in planning for buildings and cities similar to information systems.
- Building a simple, single-user, non distributed system, no architects needed.
- Building an enterprise-wide, mission critical, highly distributed system, you might need:
  - A database architect, a solutions architect, an infrastructure architect, a business architect, and an enterprise architect.
- Building a large, complex, enterprise-wide information system without an enterprise architect is like trying to build a city without a city planner.
- Can you build a city without a city planner? Probably.
  - Would you want to live in such a city? Probably not.
  - Hiring a city planner/enterprise architect does not guarantee a livable city/ successful enterprise; it merely improves your chances.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

TOGAF

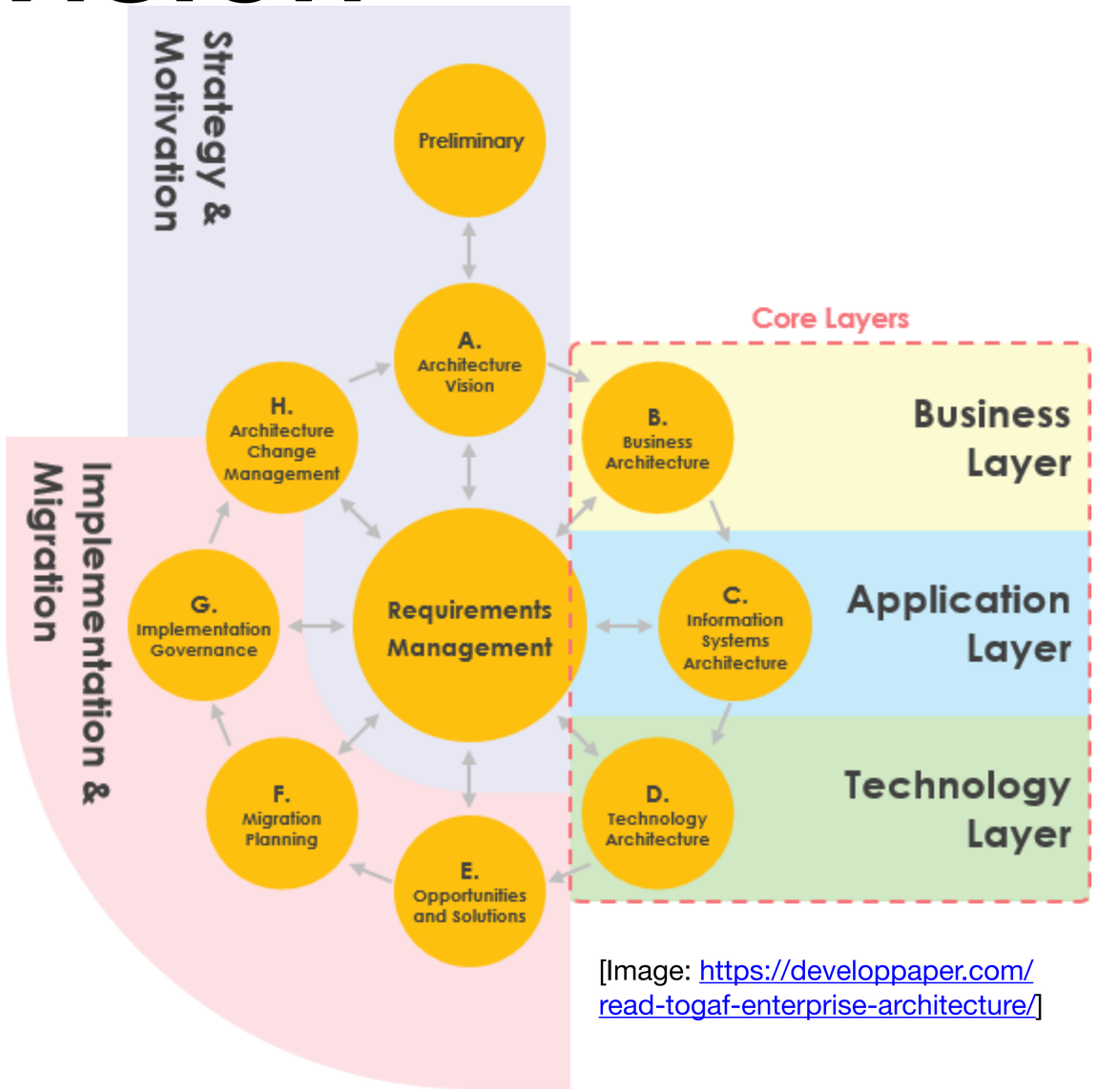
- The TOGAF standard has been developed through the collaborative efforts of more than 300 Architecture Forum member companies from some of the world's leading companies and organizations.
- The components of TOGAF 9 are as follows:
  - Architecture Development Method (ADM)
  - ADM Guidelines and Techniques
  - The Architecture Content Framework
  - The Enterprise Continuum and Tools
  - TOGAF Reference Models
  - The Architecture Capability Framework



[https://www.opengroup.org/our-members]

TOGAF vision

S4Lab



[Image: https://developpaper.com/read-togaf-enterprise-architecture/]

For which corporations?

S4Lab

- As of 2015, TOGAF was implemented in 60% of Fortune 500 companies.
  - i.e. Cognizant, HP, Cisco, Oracle, IBM, and SPARX Systems.
- TOGAF has the highest adoption rate among large international companies.
- This trend suggests that TOGAF compliance is costly.

[Karpf, B. A., Dead reckoning: where we stand on privacy and security controls for the Internet of Things, Massachusetts Institute of Technology, 2017]

TOGAF by a case study

S4Lab

- MedAMore is a chain of drug stores. It started as a regional chain in 1960.
- In 1995, it developed an innovative software system MedAManage, or MAM.
  - MAM/Store, which ran on a small computer at a drug store.
  - MAM/Warehouse, which ran on a server in a regional warehouse.
  - MAM/Home, which ran on a large server at the home office.

MEDAMOR HEALTH INC.

- These three programs communicated through files that were transferred from one location (for example, a store) to another (for example, a regional warehouse).
- When reliable communications lines existed, file transfers could occur through FTP. The system was also flexible enough to accommodate transfers through courier, where necessary.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

MedAMore case

S4Lab

- By 2002, it was clear that the same software systems that had initially fueled MedAMore's success were now hampering its future.
  - MAM/Store required regional specializations.
  - The regional warehouses that had been acquired through acquisition each had different ways of receiving orders from the retail stores and different procedures from ordering supplies from the wholesalers.
  - Files were often delivered late, sometimes not at all, and occasionally multiple times.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

MedAManage becomes MedANightmare

S4Lab

- The modules had grown to over 1 million lines of code each.
- MedAManage had become MedANightmare.
- These technical problems soon created internal conflicts within the home office of MedAMore. The business side of MedAMore wanted to acquire two more regional chains, but IT was still struggling to bring the existing acquisitions online
- By 2005,The business side distrusted IT and tried to circumvent it at every opportunity. The technical side built its IT systems with little input from the business folks. Several large and expensive IT initiatives were ignored by the business side and were eventually abandoned.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

Hearing about EA

S4Lab

- A company that only five years earlier was an industry leader in profitability, in large part because of its innovative use of IT was now struggling to stay out of the red in large part, because of the inflexibility of those same IT systems.
- Decides to create a common enterprise architecture for MedAMore that would unite its technical and business people.
- This common enterprise architecture would be named MedAMore-Enterprise Architecture, or MAM-EA. After it was completed, MAM-EA would drive all new IT investment and ensure that every dollar invested in IT was delivering the maximum value to the business.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

TOGAF phase A

S4Lab

- Phase A begins, at least in theory, with a Request for Architecture Work from some organization within MedAMore.
- This document includes the business reasons for the request, budget and personnel information, and any constraints that need to be considered.
- As soon as the Request for Architecture Work (or some equivalent) has been received, the TOGAF consultant starts MedAMore on Phase A.
- Phase A, will ensure that the project has the necessary support within MedAMore, define the scope of the project, identify constraints, document the business requirements, and establish high-level definitions for both the baseline (starting) architecture and target (desired) architecture.
- These baseline and target definitions will include high-level definitions on all four of the EA sub-architectures: business, technology, data, and application architectures.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

TOGAF phase B

S4Lab

- The Architectural Vision created in Phase A will be the main input into Phase B.
- Goal in Phase B is to create a detailed baseline and target business architecture and perform a full analysis of the gaps between them.
- Phase B is quite involved involving business modeling, highly detailed business analysis, and technical-requirements documentation.
- A successful Phase B requires input from many stakeholders. The major outputs will be a detailed description of the baseline and target business objectives, and gap descriptions of the business architecture.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

TOGAF phase C

S4Lab

- Phase C does for the information-systems architecture what Phase B does for the business architecture.
- TOGAF defines nine specific steps, each with multiple sub-steps:
  - Develop baseline data-architecture description.
  - Review and validate principles, reference models, viewpoints, and tools.
  - Create architecture models:
    - logical data models, data-management process models, and relationship models that map business functions to CRUD (Create, Read, Update, Delete) data operations
  - Select data-architecture building blocks.
    - Conduct formal checkpoint reviews of the architecture model and building blocks with stakeholders.
    - Review qualitative criteria (for example, performance, reliability, security, integrity).
  - Conduct checkpoint/impact analysis.
  - Perform gap analysis.
- The most important deliverable from this phase will be the Target Information and Applications Architecture.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

Phase D to E

- Phase D completes the technical architecture the infrastructure necessary to support the proposed new architecture. This phase is completed mostly by engaging with technical team.
- Phase E evaluates the various implementation possibilities, identifies the major implementation projects that might be undertaken, and evaluates the business opportunity associated with each.
- The TOGAF standard recommends that first pass at Phase E "focus on projects that will deliver short-term payoffs and so create an impetus for proceeding with longer-term projects."

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

TOGAF phase F to H

S4Lab

- Phase F is closely related to Phase E. In this phase, MedAMore's governance body prioritizes projects identified in Phase E.
- In Phase G, prioritized list of projects is employed to create architectural specifications for the implementation projects.
- In Phase H, the architectural change-management process is modified with any new artifacts created in this last iteration and with new information that becomes available.
- Start the cycle again.

[Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc., 2007]

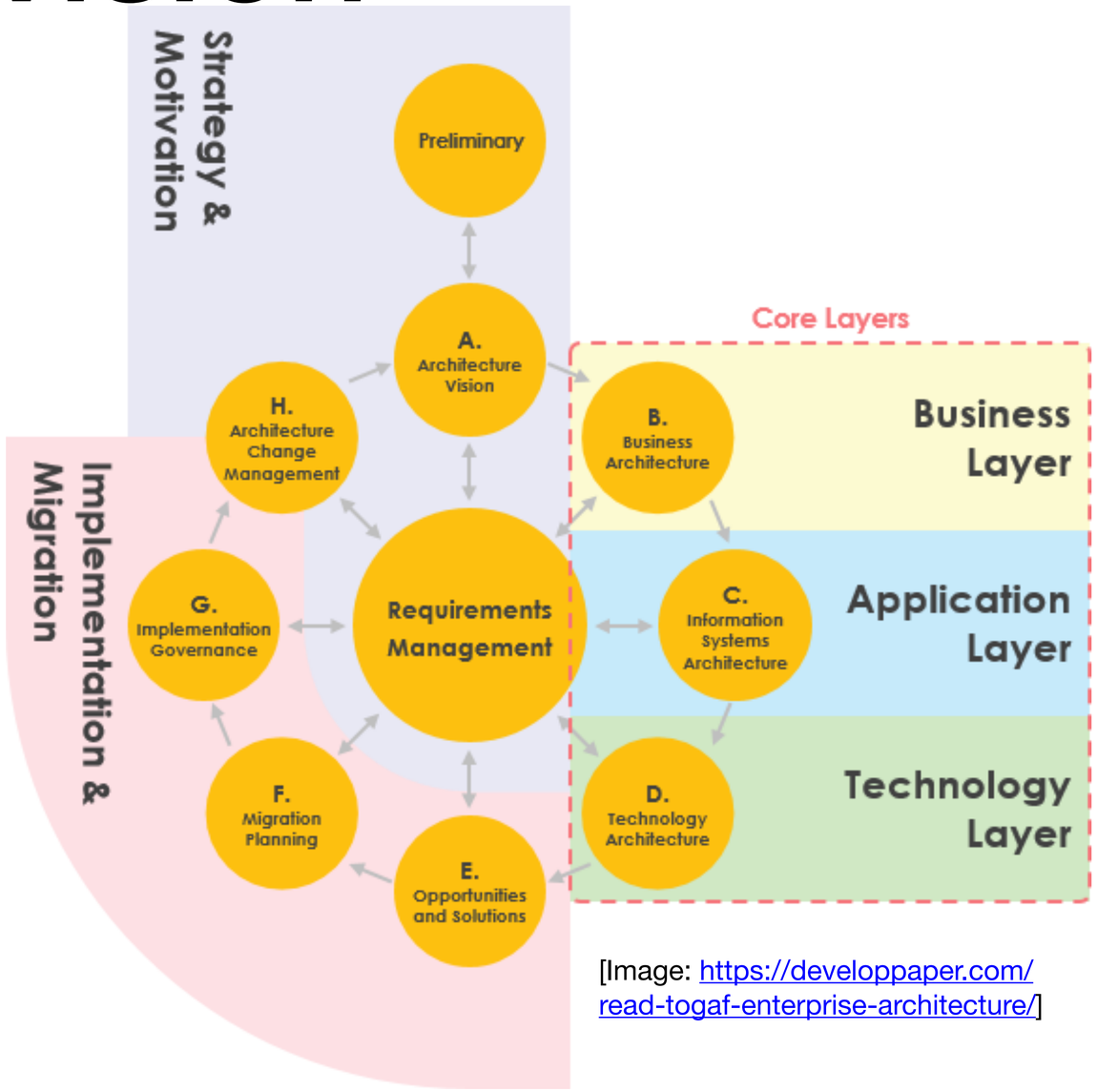
Security in TOGAF

S4Lab

Security Architecture and the ADM, TOGAF® Version 9.1, an Open Group Standard [https://pubs.opengroup.org/architecture/togaf91-doc/arch/chap21.html]

TOGAF vision

S4Lab



[Image: https://developpaper.com/read-togaf-enterprise-architecture/]

Security in phase A

S4Lab

- Phase A: Architecture Vision
- Security Inputs
  - List of applicable security policies
  - List of applicable jurisdictions
  - Complete disaster recovery and business continuity plans
- Security Outputs
  - Physical security environment statement
  - Business security environment statement
  - Regulatory environment statement
  - Security policy cover letter signed by CEO or delegate
  - List of architecture development checkpoints for security sign-off
  - List of applicable disaster recovery and business continuity plans
  - Systems criticality statement

[Security Architecture and the ADM, TOGAF® Version 9.1, an Open Group Standard]

Security in phase B

S4Lab

- Phase B: Business Architecture
- Security Inputs
  - Initial business and regulatory security environment statements
  - List of applicable disaster recovery and business continuity plans
  - List of applicable security policies and regulations
- Security Outputs
  - List of forensic processes
  - List of new disaster recovery and business continuity requirements
- Validated business and regulatory environment statements
- List of validated security policies and regulations
- List of target security processes and list of baseline security processes
- List of security actors
- List of interconnecting systems
- Statement of security tolerance for each class of security actor
- Asset list with values and owners
- List of trust paths
- Availability impact statement(s)
- Threat analysis matrix

[Security Architecture and the ADM, TOGAF® Version 9.1, an Open Group Standard]

Security in phase C

S4Lab

- Phase C: Information Systems Architectures
- Security Inputs
  - Threat analysis matrix
  - Risk analysis
  - Documented forensic processes
  - Validated business policies and regulations
  - List of interconnecting systems
  - New disaster recovery and business continuity requirements

[Security Architecture and the ADM, TOGAF® Version 9.1, an Open Group Standard]

Security in phase C

S4Lab

- Security Outputs
  - Event log-level matrix and requirements
  - Risk management strategy
  - Data lifecycle definitions
  - List of configurable system elements
  - Baseline list of security-related elements of the system
  - New or augmented security-related elements of the system
  - Security use-case models:
    - Normative models
    - Non-normative models
- List of applicable security standards:
  - Protocols
  - Object libraries
  - Others ...
- Validated interconnected system list
- Information classification report
- List of asset custodians
- Function criticality statement
- Revised disaster recovery and business continuity plans
- Refined threat analysis matrix

[Security Architecture and the ADM, TOGAF® Version 9.1, an Open Group Standard]

Security in phase D

S4Lab

- Phase D: Technology Architecture
- Security Inputs
  - List of security-related elements of the system
  - List of interconnected systems
  - List of applicable security standards
  - List of security actors
  - Risk management strategy
  - Validated security policies
  - Validated regulatory requirements
  - Validated business policies related to trust requirements
- Security Outputs
  - Baseline list of security technologies
  - Validated interconnected systems list
  - Selected security standards list
  - Resource conservation plan
  - Security metrics and monitoring plan
  - User authorization policies
  - Risk management plan
  - User trust (clearance) requirements

[Security Architecture and the ADM, TOGAF® Version 9.1, an Open Group Standard]

Asset Discovery

What is the problem?

S4Lab

- Legacy organization
- Merger and Acquisition
- Messy Admin
- No central IT department
- ….

Lost Server (2001)

S4Lab

- University of North Carolina has finally located one of its most reliable servers - which nobody had seen for FOUR years.
- One of the university's Novell servers had been doing the business for years and nobody stopped to wonder where it was - until some bright spark realized an audit of the campus network was well overdue.
- After they couldn't find the server. Attempts to follow network cabling to find the missing box led to the discovery that maintenance workers had sealed the server behind a wall.

[https://www.theregister.com/2001/04/12/missing_novell_server_discovered_after/]

Hardware Assets

S4Lab

- Servers
- WorkStations
- Switches
- Routers
- Links
- IP Phones
- AP
- Camera
- Smart TV
- ….

Soft Assets

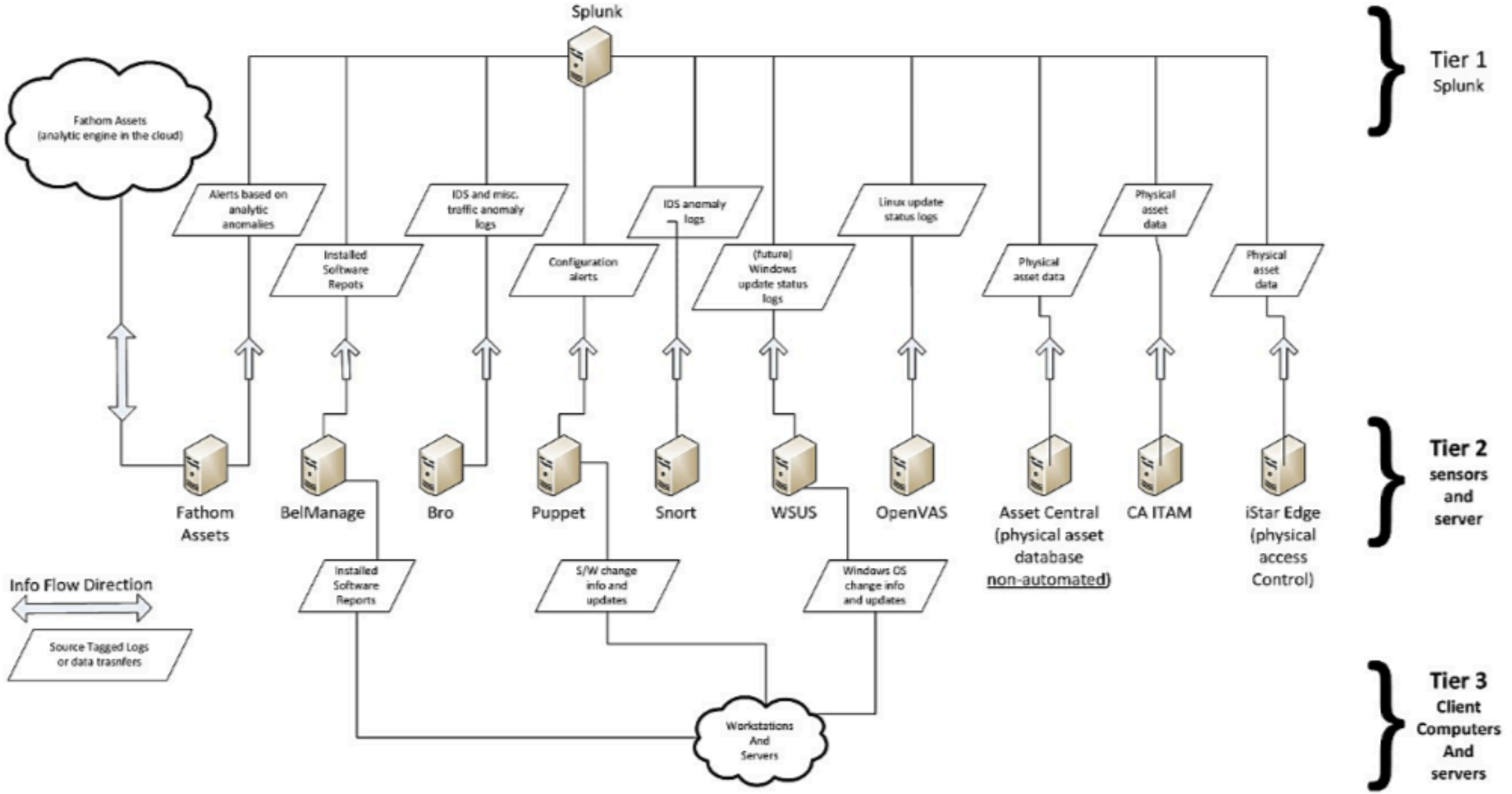
S4Lab

- OS(s)
- Different software used/Different versions
- Identities
- Credentials
- Accesses
- IP addresses
- Licenses
- Domains
- ….

IT Asset Management

S4Lab

Figure 5-10 ITAM Data Flow



[Image: NIST SP 1800-5A: IT Asset Management]

Asset Discovery example

S4Lab

- https://www.youtube.com/watch?v=sGqg8vS04v0