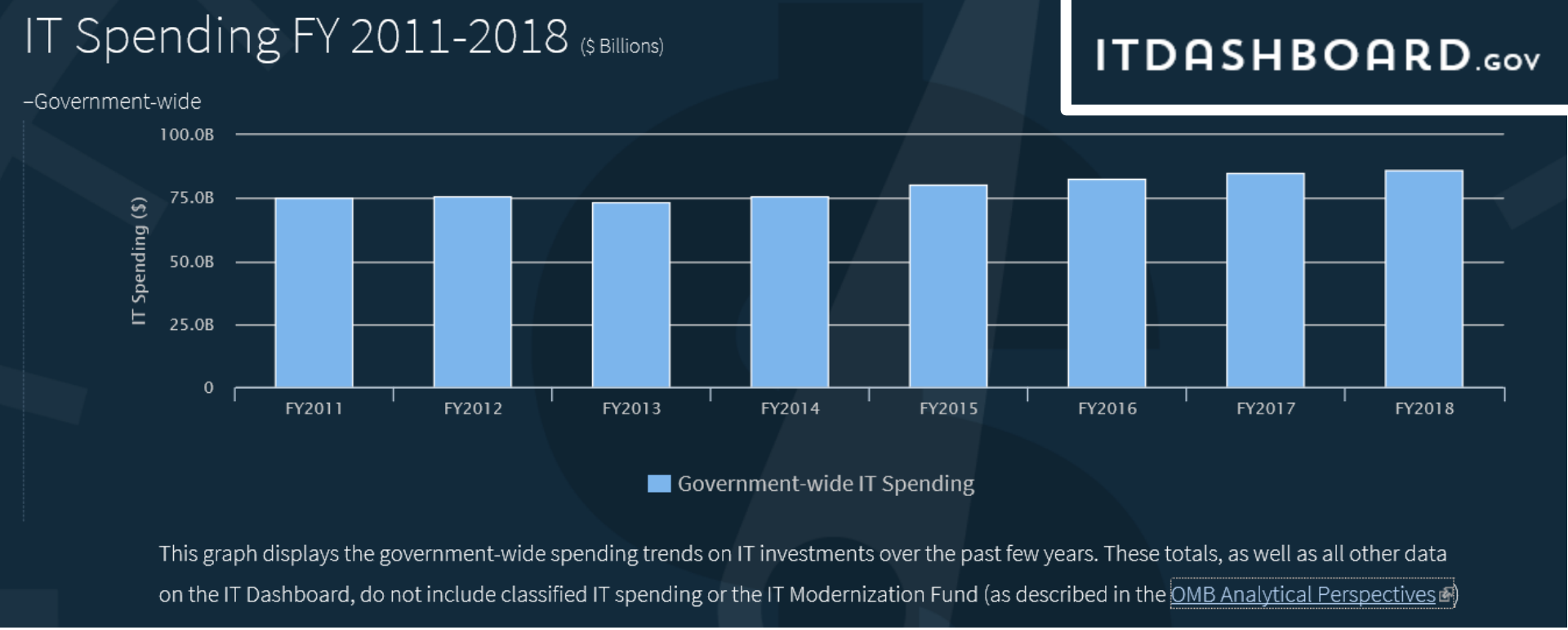
ISSA
Information Systems Security Association

ISSA, Colorado Springs Chapter

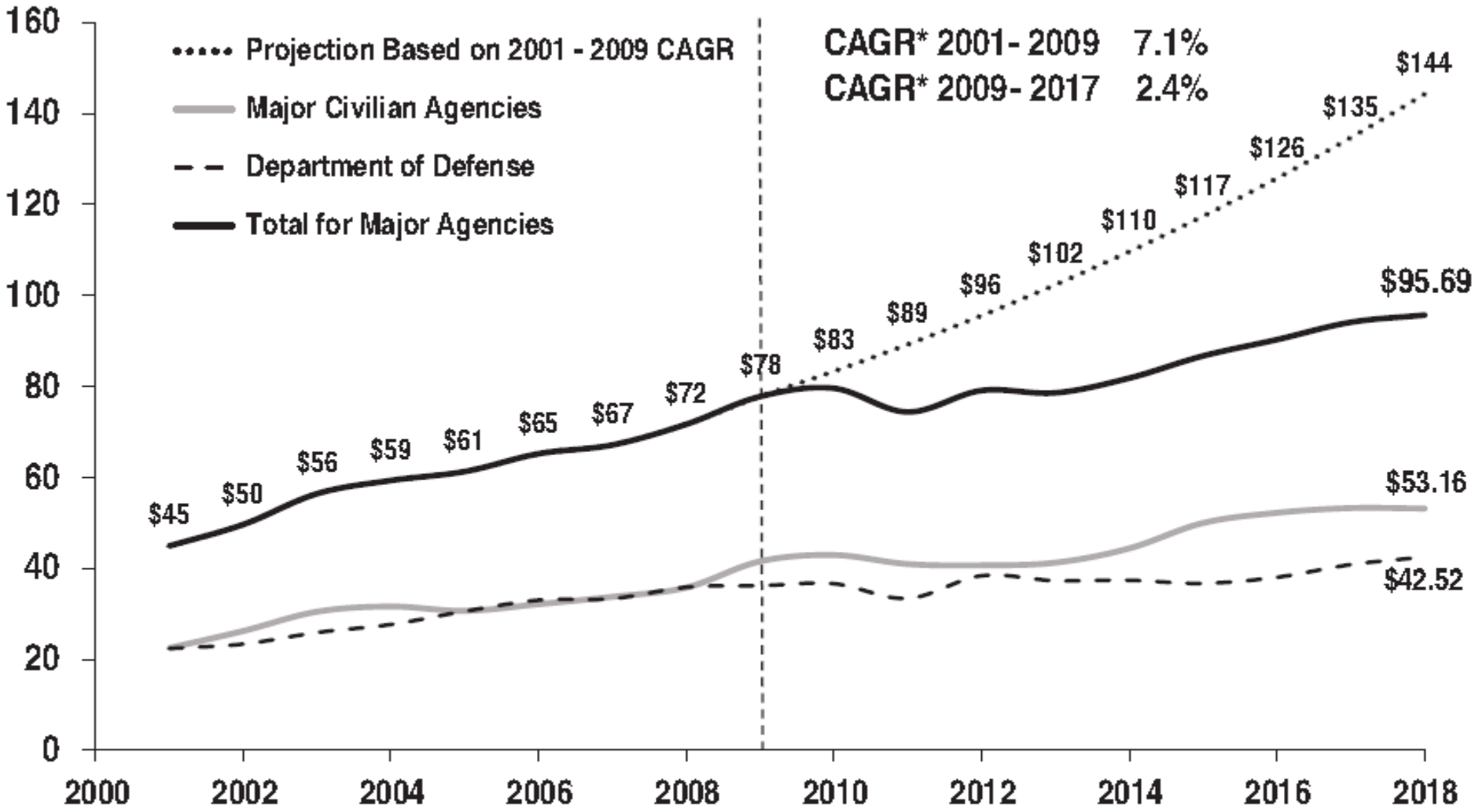
Enterprise Security Architecture

Kurt Danis, DAFC
CISSP-ISSEP
13 July 2017



14 years ago…

In a 2003 memo, Sen. Joseph Lieberman, D-Conn., said, "federal agencies should be deriving better results from the $60 billion spent annually on information technology. Much of that money is wasted on IT systems that are redundant or obsolete." Moreover, Lieberman wrote, **"The lion's share of the $60 billion spent on IT is spent on service contracts, and there is ample evidence to suggest that oversight of these contracts has been deficient."**



*Compound Annual Growth Rate.

Source: Total IT spending for agencies reporting to the IT Dashboard. Department of Defense has provided estimates for classified IT investments not shown on the IT Dashboard. Chart reflects data available as of May 9, 2017.

NIST Cybersecurity Risk Framework

For the first time, this Budget includes discrete cyber program investments that align budget resources with the National Institute of Standards and Technology (NIST) **Cybersecurity Framework**. This will enable the alignment of budget, risk, and performance data in a **consistent way across all Federal agencies.**

Analytical Perspectives (OMB publication)
"Information Technology" chapter
Retrieved on 13Jul2017 from
https://www.whitehouse.gov/omb/budget/Analytical_Perspectives

Agenda

1. Enterprise Architecture (EA) Purpose
2. Definitions
3. Legislation
4. EA Framework examples
    a. Zachman Framework
    b. TOGAF
    c. DoDAF
5. EA for Security - SABSA

Enterprise Architecture Purpose

Orchestrating the People, Operations, and Technology

DoD CIO, Terry Halverson

- Partnering w/industry… doesn't mean selling us stuff

Director of the Navy Budget, VADM Thomas Church

- PPBE class, "Free puppy dog theory"

N-NC/J6 civilian leader IRT new continuous monitoring initiative

- "Technology is like a new baby. It's fun making babies; and then comes the responsibilities, care, planning, etc."

Security Architecture

Security Architecture – 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.

Security Architect – a person qualified to design and supervise the construction of secure business systems, usually secure business information systems.

Definitions from p.2, Enterprise Security Architecture, John Sherwood, Andrew Clark, David Lynas; published by CMP books, 2005

Rep. William Clinger, R-Pa

January 3, 1995 – January 3, 1997

Legislation

Sen. William Cohen, R-Maine

January 24, 1997 – January 20, 2001

OMB CIRCULAR NO. A–11
PREPARATION, SUBMISSION, AND EXECUTION OF THE BUDGET
Section 240—Annual Performance Planning

- "Agencies must provide required data on total IT funding... **consistent with** the overall agency budget submission, **your agency enterprise architecture (EA)**, your agency's Agency IT Portfolio Summary, and your agency's Major IT Business Case submissions."
- "**The agency must further demonstrate how the investment supports a business line or enterprise service performance goal as documented in the agency's enterprise architecture (EA)**, and annual Enterprise Roadmap submission to OMB."
- "How does the **Annual Performance Plan** relate to the agency's enterprise architecture? Once an agency's performance plan is established, agencies should ensure that the enterprise architecture planning documents are consistent with achieving the agency goals and objectives."

Legislation

"For information technology investments, be consistent with Federal and agency enterprise architectures which: integrate agency work processes and information flows with technology to achieve the agency's strategic goals, reflect the agency's technology vision, specify standards that enable information exchange and resource sharing while retaining flexibility in the choice of suppliers and in the design of local work processes, and **ensure that security is built into and funded as part of the enterprise architecture in accordance with OMB Memorandum M–00–07,** Incorporating and Funding Security in Information Systems Investments (February 28, 2000)"

-- Appendix 6, page 68, Capital Programming Guide, OMB Circular No. A–11 (2015)

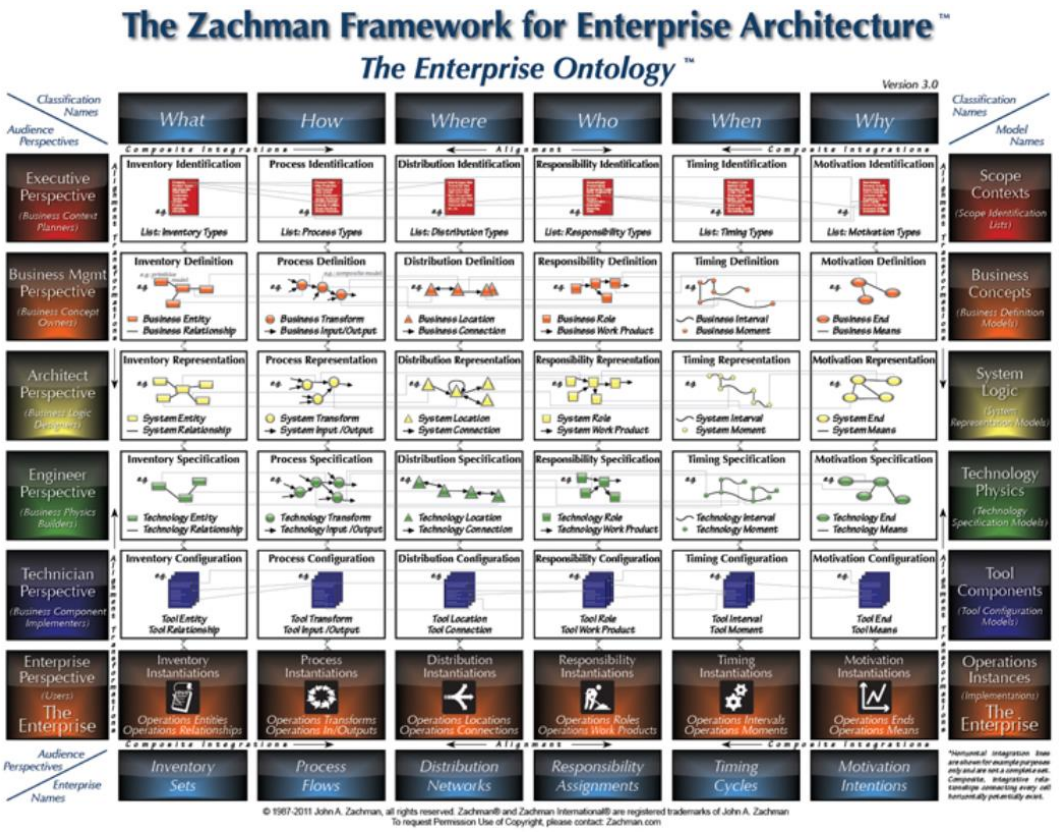
Zachman Framework

Zachman 4-Day Training Workshop - Colorado Springs:

July 18-21, 2017

Colorado Springs, CO

$3,499



TOGAF

The Open Group Architecture Framework (TOGAF):

- Approach for designing, planning, implementing, and governing an enterprise information technology architecture.
- TOGAF Architecture Development Method (ADM) based on the Technical Architecture Framework for Information Management (TAFIM), a DoD concept in the late 1980s
- Over 69,000 people with TOGAF 9 certifications (https://togaf9-cert.opengroup.org/certified-individuals)
- TOGAF defines Architecture as:
  - "formal description of a system, or a detailed plan of the system at component level to guide its implementation", or as "**the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time**."

- 24 – 28 July 2017
- Archi Tacts Inc
- TOGAF 9 Combined Level 1 and 2 ➔ **$3,000 - includes exam vouchers**
- Denver, CO

DoDAF

- C4ISR Architecture Framework v1.0 in 1996
- Developed in response to Clinger-Cohen Act
- Version 2.02, current since August 2010

Certified Enterprise Architect (CEA) Black Belt **$11,000**
Associate CEA Green Belt **$5,500**

Fees about 10% less for Government Employee

SABSA Chartered Security Architect - Foundation Certificate (SCF)

Requires a candidate **to pass 2 test modules** consisting of 40 multiple choice questions. Each test module is of 60 minutes duration.

- SABSA Security Strategy & Planning (Test Module F1)
- SABSA Security Service Management (Test Module F2)

SABSA Foundation (F1 & F2)
Dallas, TX
18 – 22 September 2017
$3,760

The SABSA Institute

SABSA is governed by The SABSA Institute. In the United Kingdom an "Institute" is not an ordinary company: it has a protected and highly-regulated status that guarantees:

- SABSA intellectual property can never be sold
- SABSA will always remain vendor-neutral
- SABSA will be free-use in perpetuity
- SABSA will have ongoing development to meet the needs of business
- SABSA's community can obtain true competency-based professional certifications that provide trust and confidence to peers and employers of an architect's capabilities

Source: http://www.sabsa.org/node/72

Sherwood Applied Business Security Architecture (SABSA)

- Methodology for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives.
- Used for **Information Assurance Architectures**, **Risk Management Frameworks**, and to align and seamlessly **integrate security and risk management into IT Architecture methods and frameworks**.

  [SABSA fills the gap for 'security architecture' and 'security service management' by integrating with TOGAF® and ITIL®.]

Source: http://www.sabsa.org/

EA for Security - SABSA®

Layered Architecture Views

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

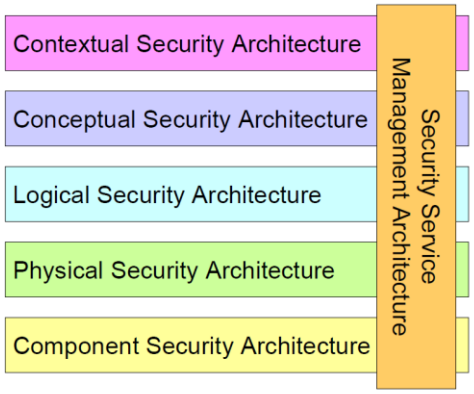


Figure 1: The SABSA Model for Security Architecture

The Business View

Owner establishes business requirements of **WHAT** must be met by the architecture.

Once the building type is defined, **the owner** must then specify more detail about its use:

- ***Why*** do you want this building? The goals that you want to achieve.
- ***How*** will it be used? The detailed functional description.
- ***Who*** will use the building, including the types of people, their physical mobility, the numbers of them expected, and so on?
- ***Where*** should it be located, and what is its geographical relationship to other buildings and to the infrastructure (such as roads, railways etc)?
- ***When*** will it be used? The times of day / week / year, and the pattern of usage over time.

Table 3: 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

References

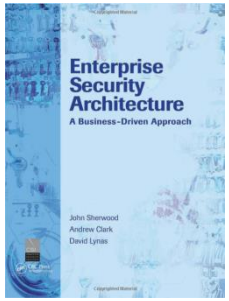
OMB Enterprise Architecture Assessment Framework
(https://www.whitehouse.gov/omb/e-gov/eaaf/)

Federal Transition Framework
(http://www.egov.gov/ftf)

Federal Enterprise Architecture Reference Models
(https://www.whitehouse.gov/omb/e-gov/fea/)

OMB Circular A-11
(http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html)

Practical Guide to Federal Enterprise Architecture
(http://www.cio.gov/archive/bpeaguide.pdf)



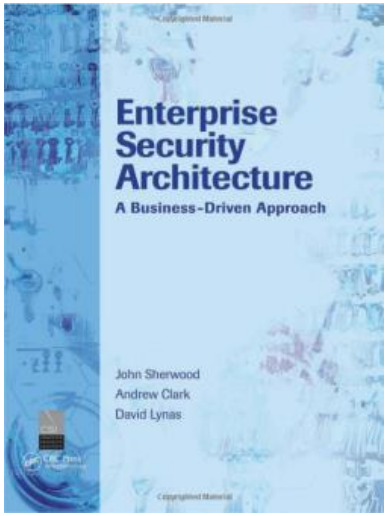
Enterprise Security Architecture: A Business-Driven Approach Hardcover – November 12, 2005

- **by John Sherwood (Author), Andrew Clark (Author), David Lynas (Author)**
- **Hardcover: 608 pages**
- **$76.80 on Amazon**

Book Review posted on (ISC)²

By Christopher P. Blake,
***** (Very Good)

- Very much aligned to the Zachman Framework
- Not for the "feint-hearted" [i.e. not easy to read for casual reader]
- Builds concepts from the ground-up: using dictionary definitions and [word] etymologies to fully explain what they mean
- As an architect: some things may have been better expressed through diagrams
- Authors appear to be 'showing-off…by utilising notations that are very academic
- Does not cover architectural styles such as Service Oriented Architecture (SOA)
- Book goes into extreme depth in certain areas where there is no practical advantage



"…some areas are perhaps too deep and too academic, with other areas arguably lacking…

NIST Special Publication 800-53 Revision 4

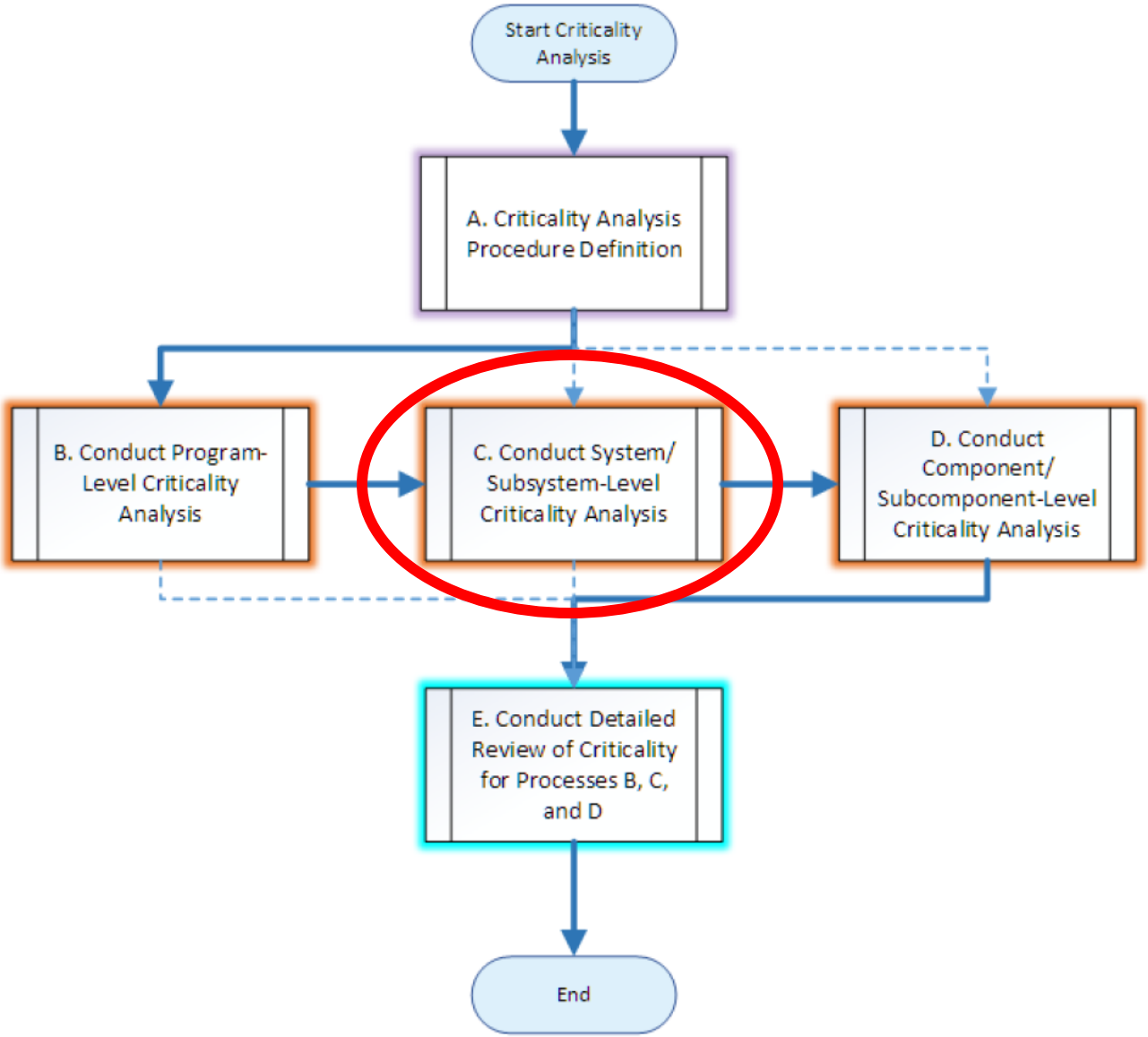
SA-14 CRITICALITY ANALYSIS

800-53 Security Control: The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined* ***information systems, information system components****, or information system services*] at [*Assignment: organization-defined* ***decision points*** *in the system development life cycle*].

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

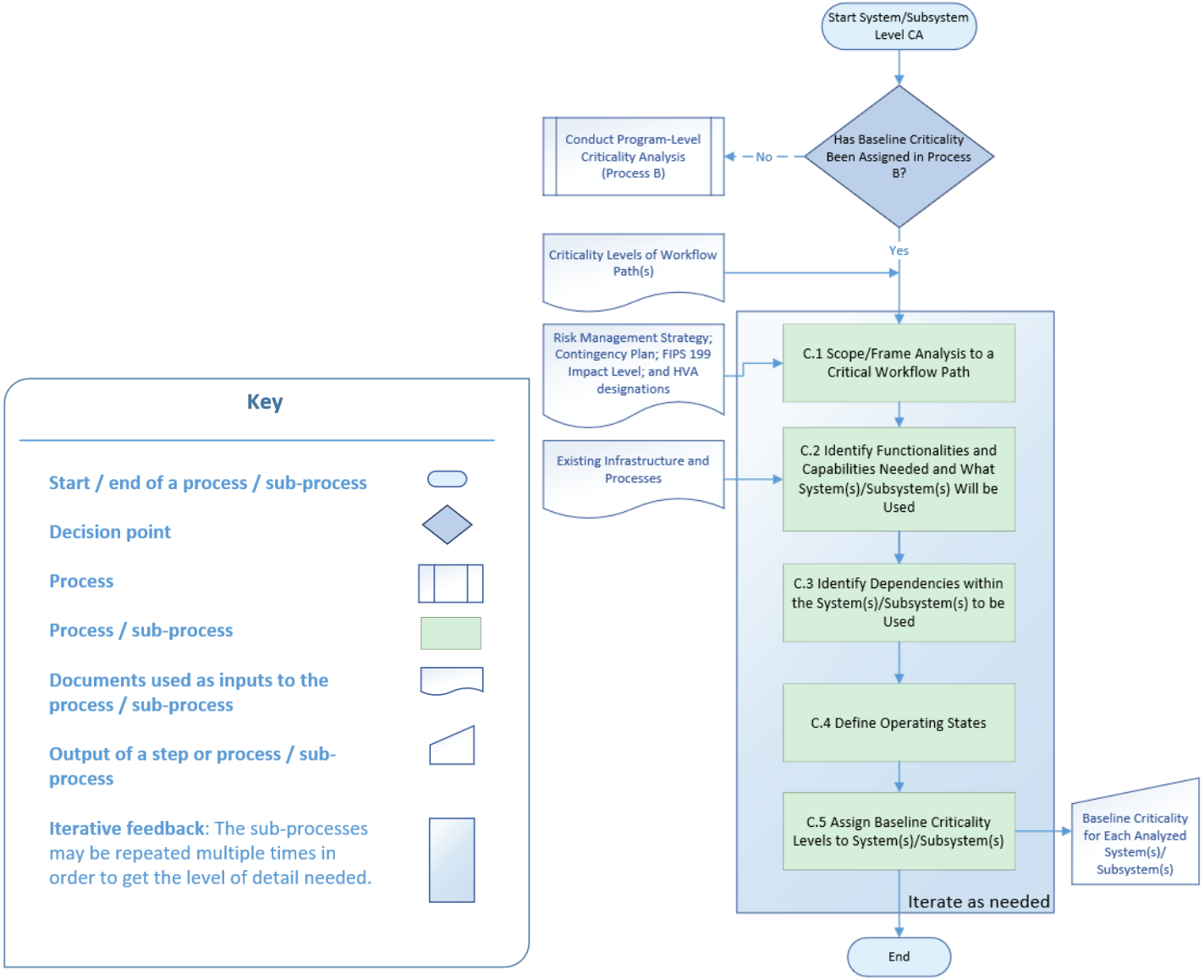
NISTIR 8179 (DRAFT)

Criticality Analysis Process Model: Prioritizing Systems And Components



NISTIR 8179 (DRAFT)

C. Conduct System/Subsystem-Level Criticality Analysis



EA Certification Resources

Zachman International®
2222 Foothill Blvd, Suite 337
La Cañada, CA 91011
866.518.4340 x102
http://www.Zachman.com

FEAC™ Institute (DoDAF & FEAF)
15954 Jackson Creek Pkwy, Ste B463
Monument, CO 80132

The Open Group (i.e. TOGAF)
8 New England Executive Park, Suite 150
Burlington MA 01803-5007
1-781-564-9200

SABSA training

David Lynas Consulting Limited
17 Ensign House
Admirals Way
Canary Wharf
London E14 9XQ
United Kingdom
T: +44 207 863 7834
F: +44 207 863 7510
training@sabsacourses.com