#SHAREorg

SHARE
Technology · Connections · Results

Application Security Architecture: Timing & Requirements – Getting It Right and On Time

Brian V. Cummings
brian.cummings@tcs.com
Tata Consultancy Services

Thursday, March 15, 2012
Session 10187

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

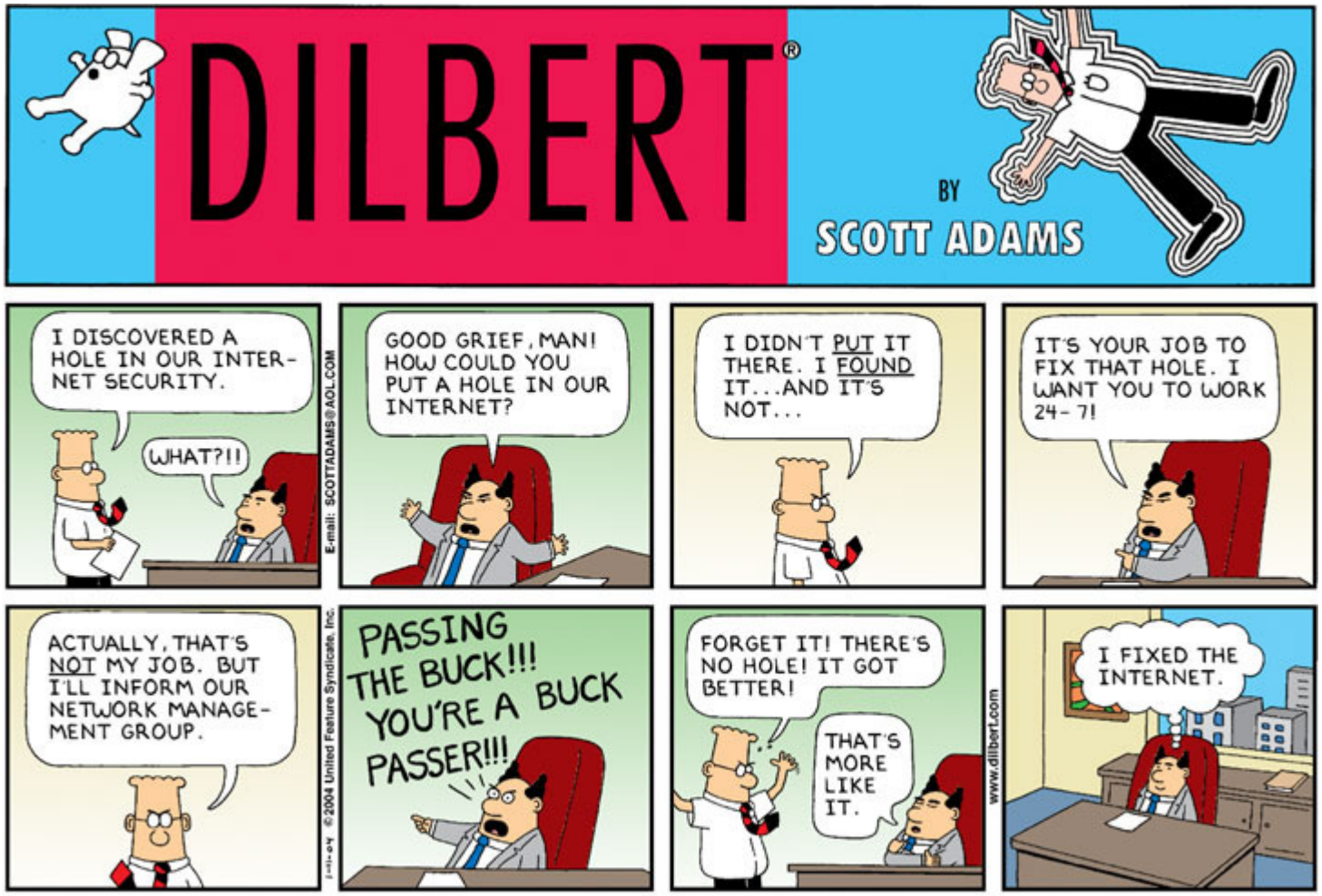
Why?

Security is to Application Development as Truth is to a Court of Law:

It is usually the last thing to come to the room, and has to be dragged in by its heels, kicking and screaming in protest!

Lawyer whose name I have long forgotten

Often a Thorny, Unresolved Issue



A recent (horror) Story

Query from a Project Lead:

Lead: "Brian, when is the best time in a development project to talk to Security?"

Brian (to self): OMG!!!
Brian (to Lead): What are you building and how far along are you.

Lead: A Procurement Web Portal for the company's vendors. We begin testing in a few weeks.

Brian (to Lead): The answer is "At the start of the project!"

The one that finally prompted this presentation

Another Recent Story

Request from a Project Lead:

Lead: "Brian, we are going live with this Web Portal in three months. We need you to help us document security and disaster recovery procedures"

Brian: What security and disaster recovery provisions have been made?

Lead: Not much, but we need the procedures!

Brian (to Lead): The answer is "At the start of the project!"

They simply don't know how much they don't know!

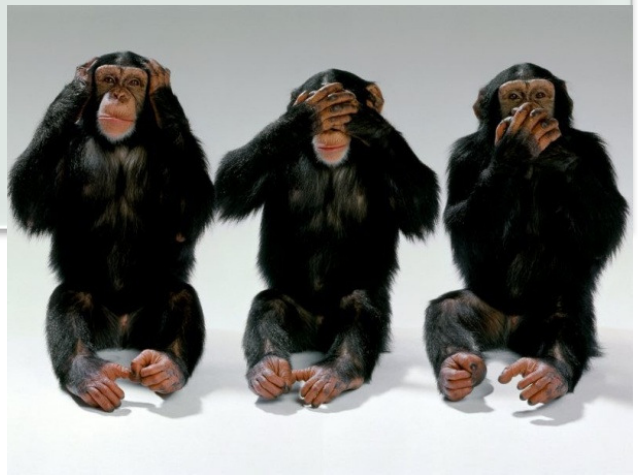
Still Another Recent Story

Dismissal from a Project Lead:

Security Architect to Lead: "What provisions are you making for security? How can I help you? We need to make sure your security architecture is consistent with our standards.

Lead to Security Architect: "We believe we can implement this Web Portal with a minimum of security. You don't need to worry about it!"

(The above in one of the world's largest financial institutions).



What? Me? Worry? Really?

Outsourcing your Application Development?

Quality Assessor to Project Lead:

Quality Guy: "Who from the client is engaged in coordinating their requirements for risk, security, compliance, and continuity?

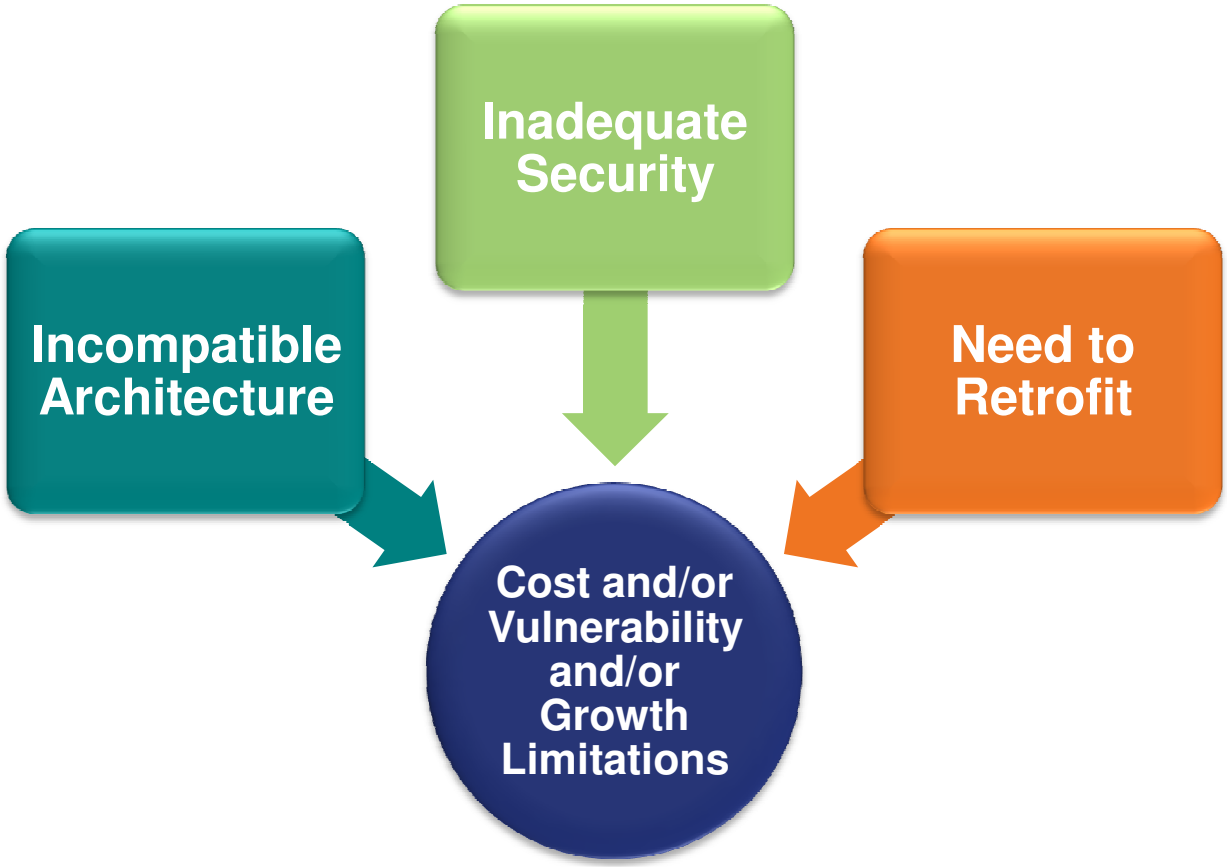
Lead to Quality Guy "Umm…they have not been involved."

Quality Guy: "Did we seek them out and they declined? Did they seek us out and we declined?"

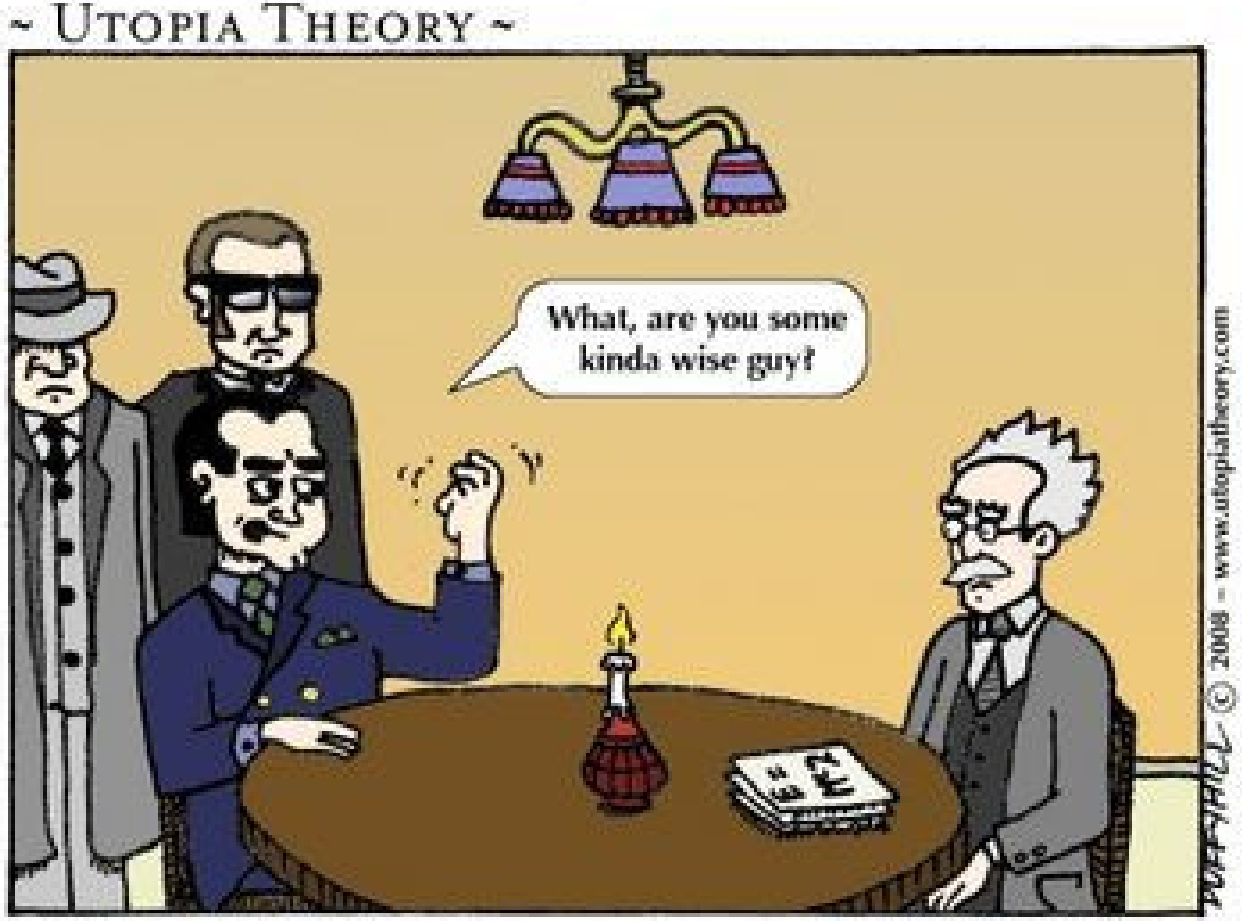
Lead: "Umm, no, neither."

What's wrong with this picture?

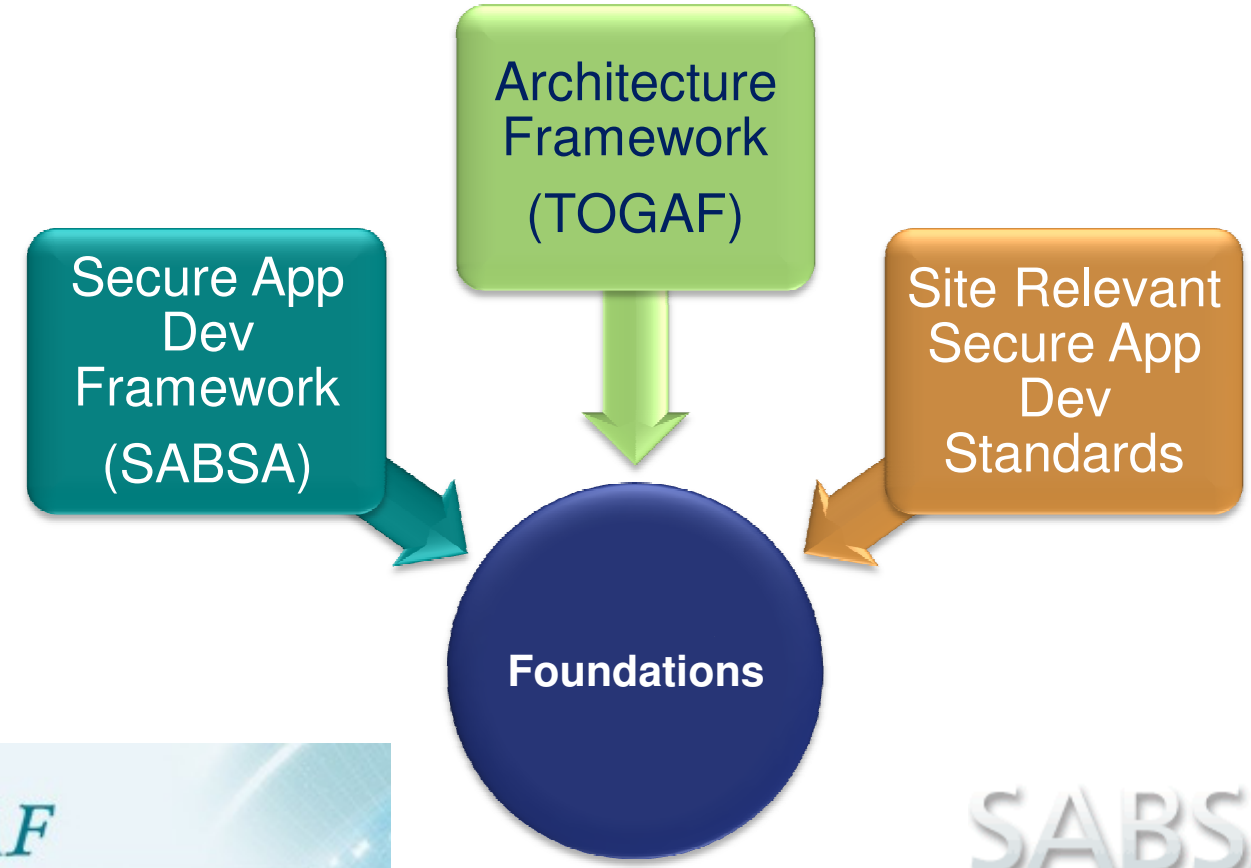
The End Result (Just Desserts)



OK, Wiseguy…What's the Answer?



1. Frameworks & Standards



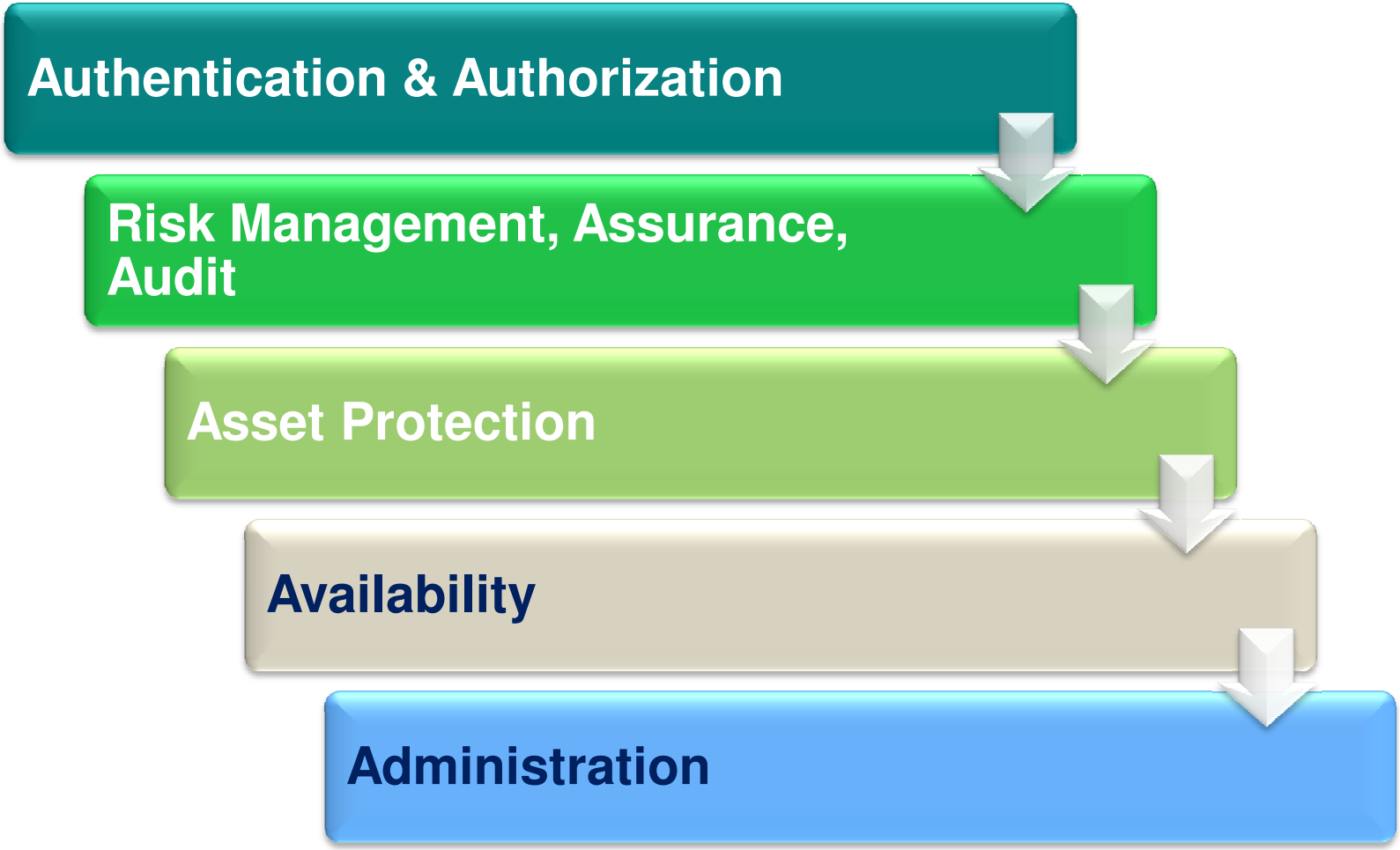
TOGAF Version 8 Enterprise Edition

http://pubs.opengroup.org/architecture/togaf8-doc/arch/

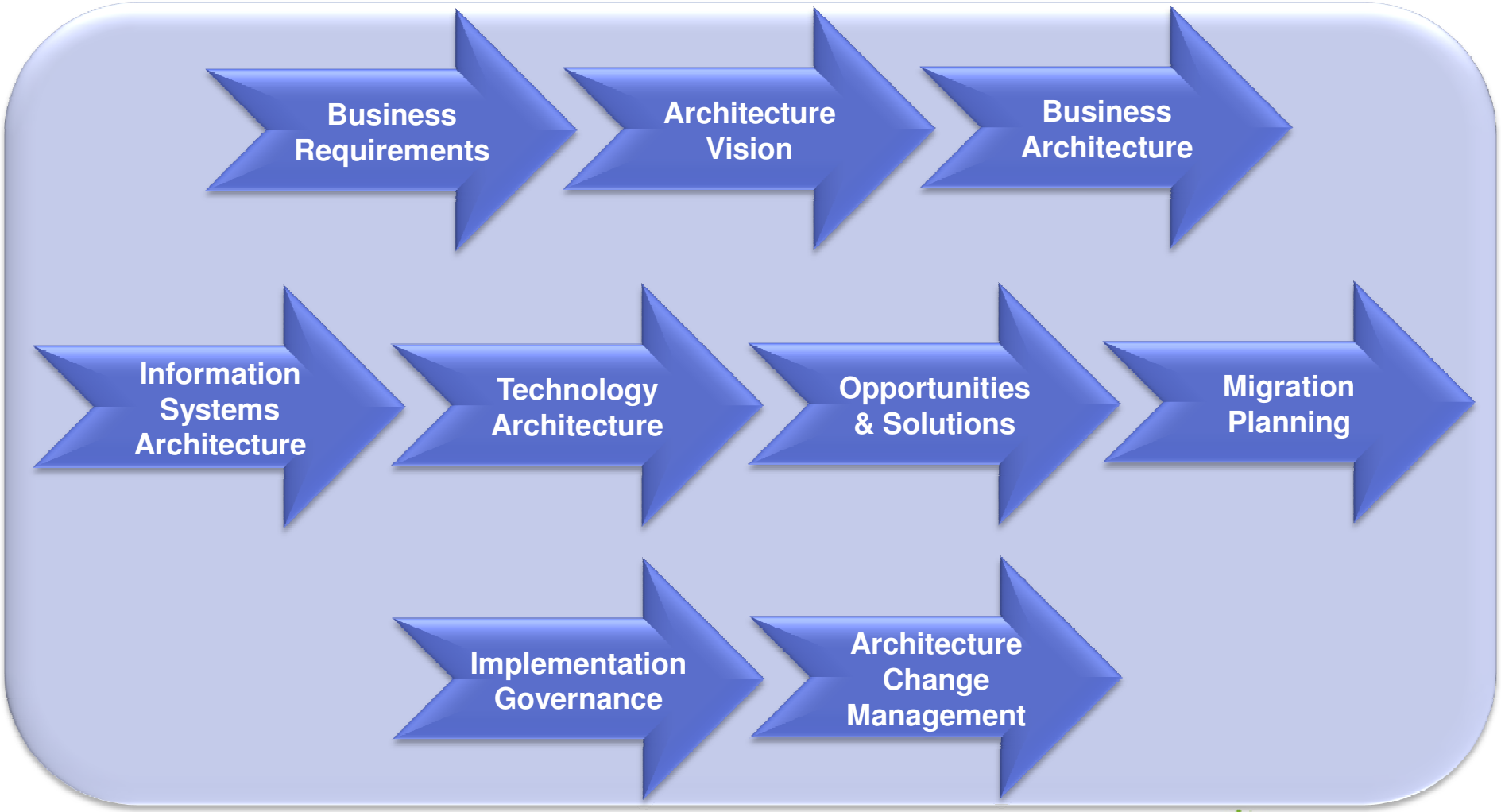
SABSA®

http://www.sabsa-institute.org/home.aspx

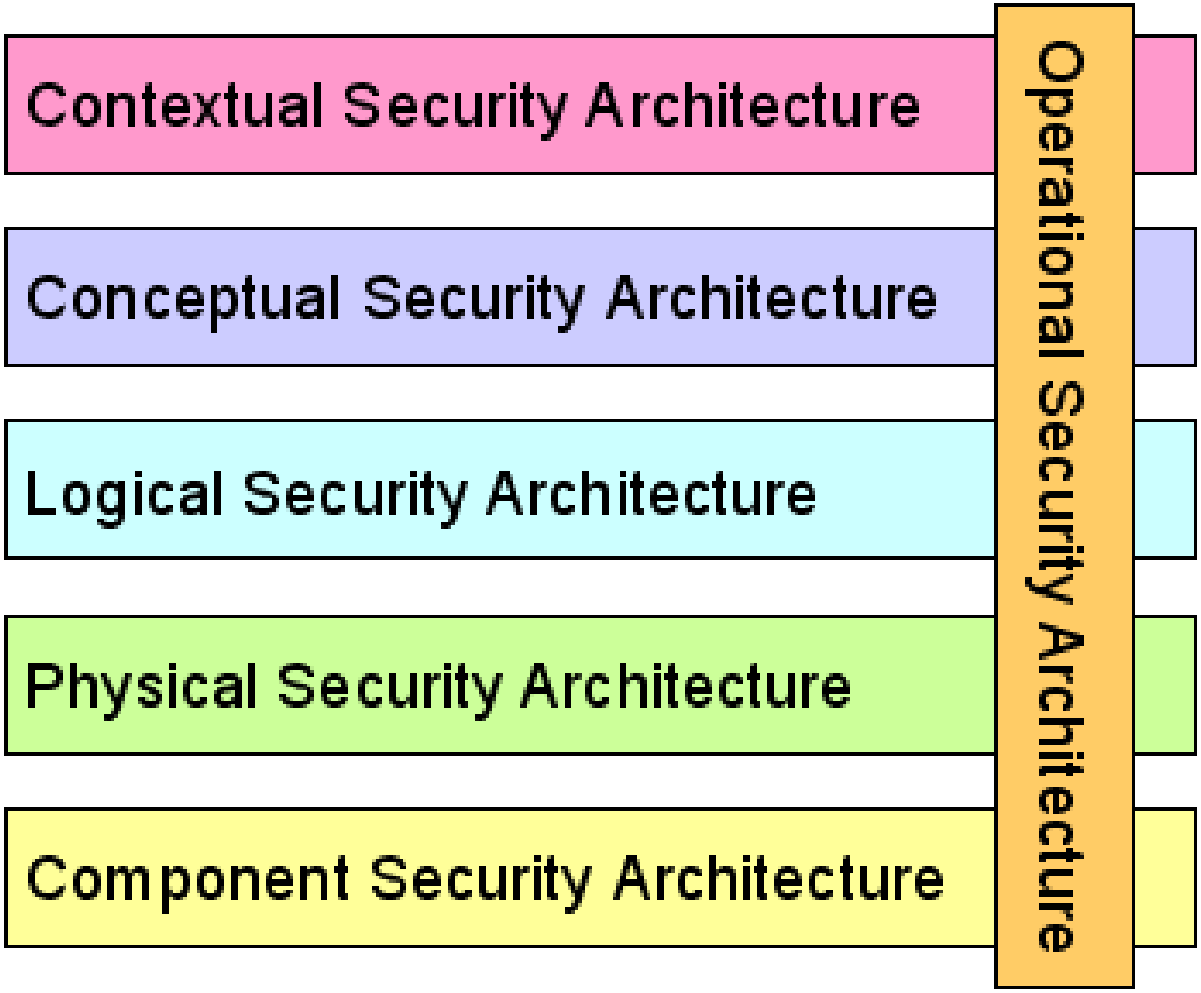
1A. TOGAF Security Architecture



1A1. TOGAF Security Architecture Phases



1B. SABSA Secure Application Development



1B1. SABSA Security 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

1C1. Site Relevant Process & Standards

SOFTWARE SECURITY ASSURANCE PROCESS HANDBOOK

Software Security Assurance Process Handbook

1C2. Site Relevant Process & Standards

CHECKLIST FOR SECURITY REQUIREMENTS

Software Security Assurance Process Handbook > Checklist for Security requirements

CONTENTS [hide]

Introduction [edit]

This checklist can be used by projects to ensure that security related requirements are taken care in their projects. The projects should not limit their scope to this checklist only and should enhance/modify this checklist based on their project security requirements.

Security Requirements of Systems [edit]

Objective: To ensure that security is built into information systems.

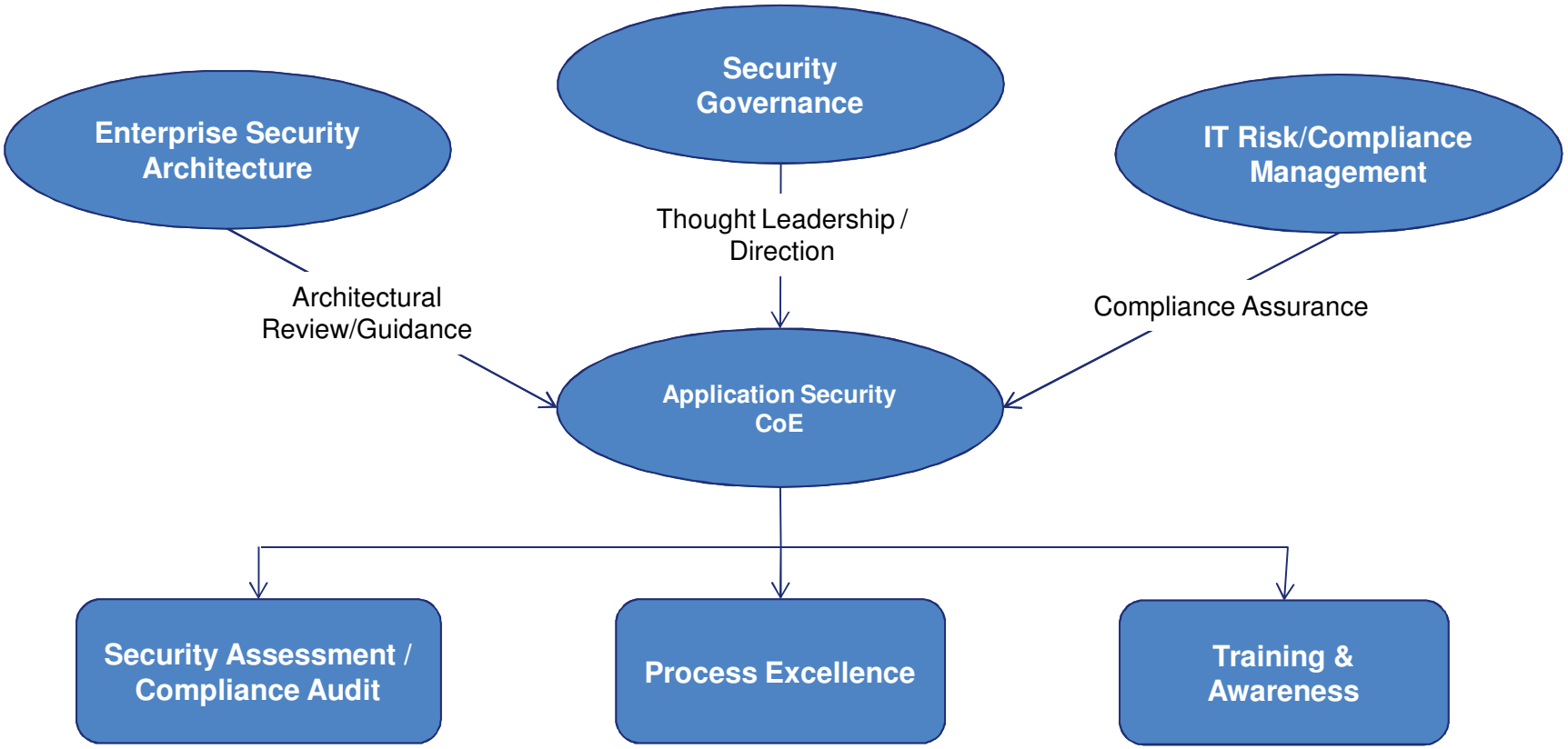
Controls:

Security requirements analysis and specification systems

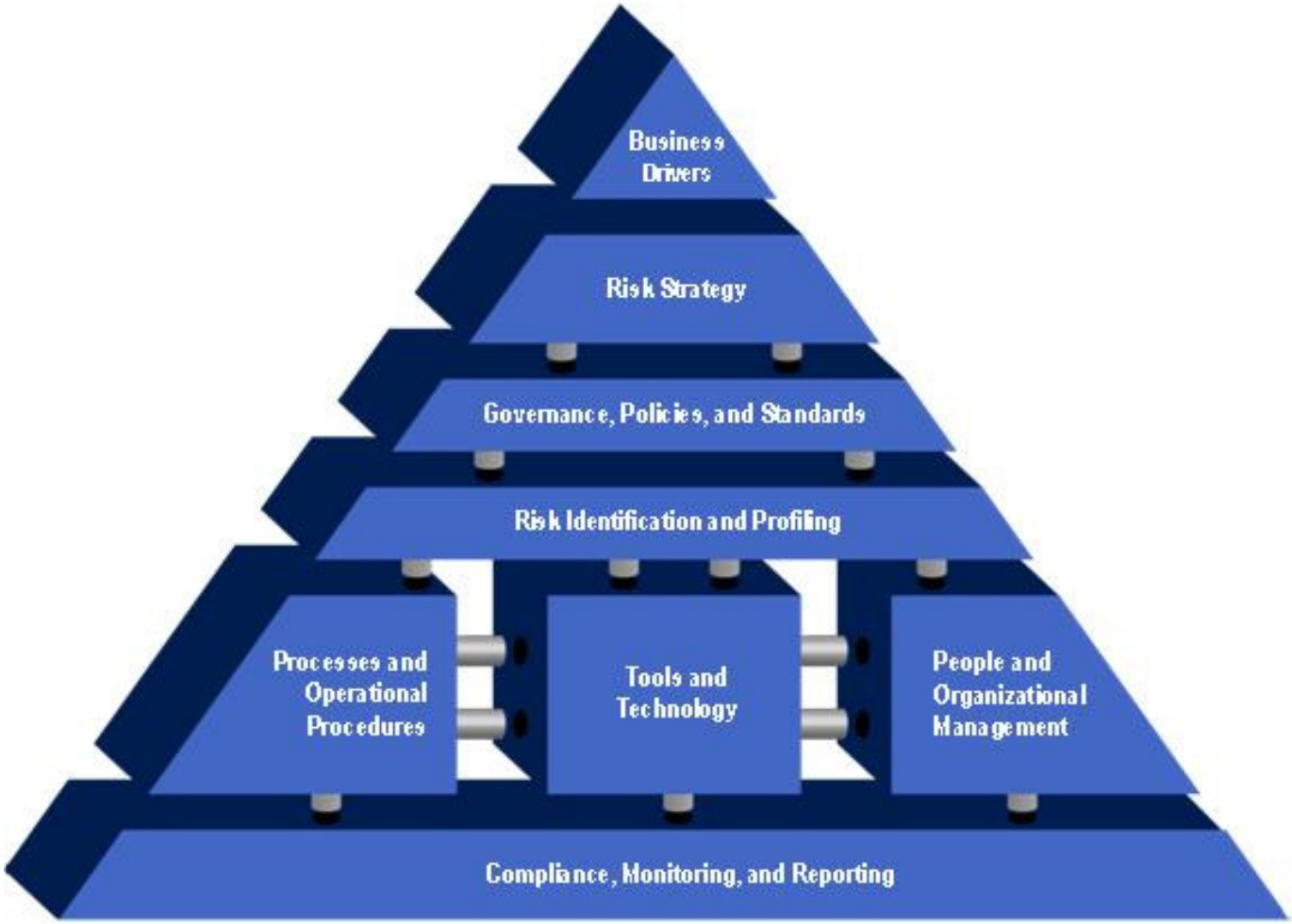
Look for:

Whether security requirements are incorporated as part of business requirement statement for new systems or for enhancement to existing systems? Security requirements and controls identified should reflect business value of information assets involved and the consequence from failure of Security

2. Security Architecture Governance



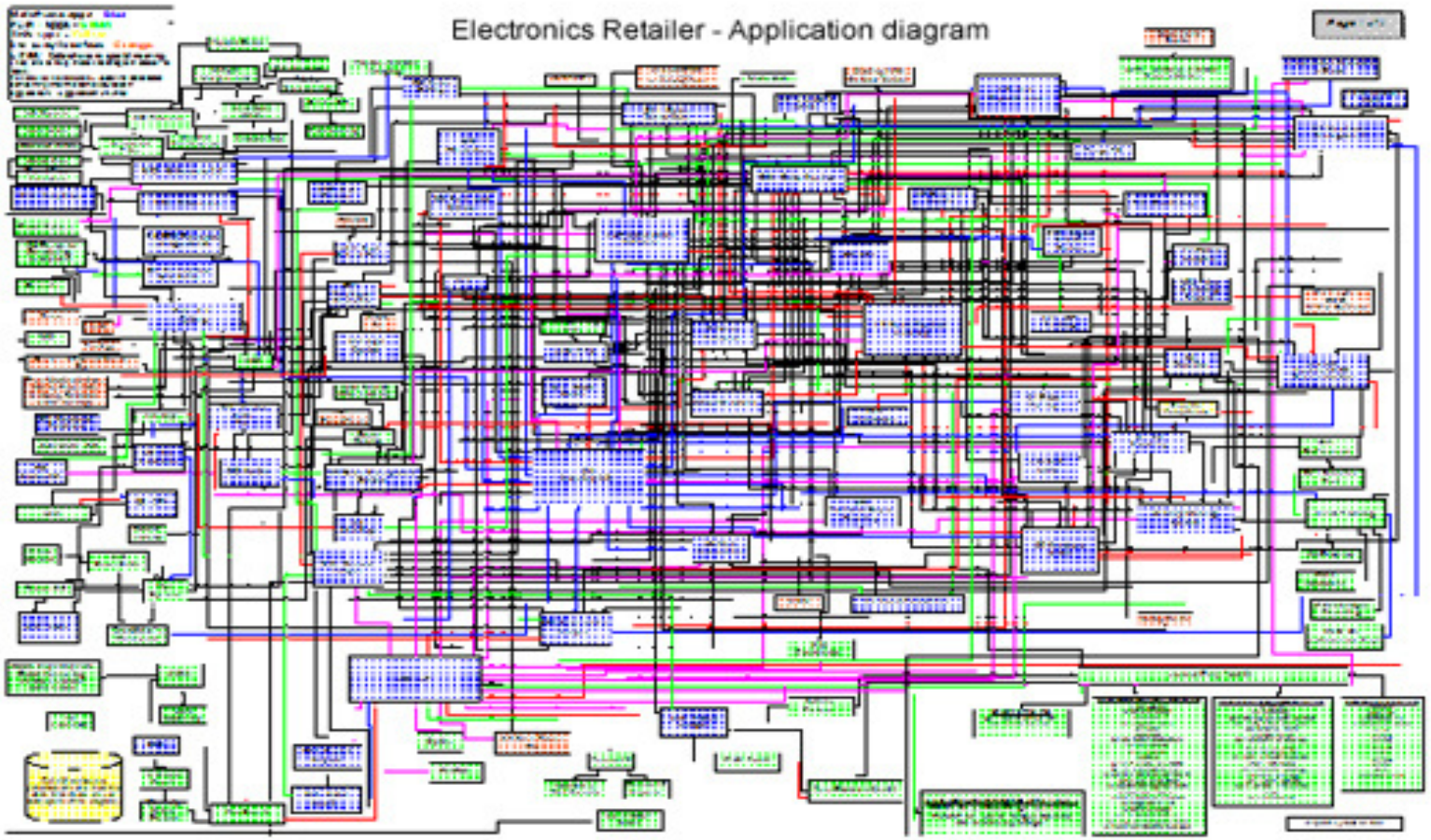
3. Application Security Risk Management



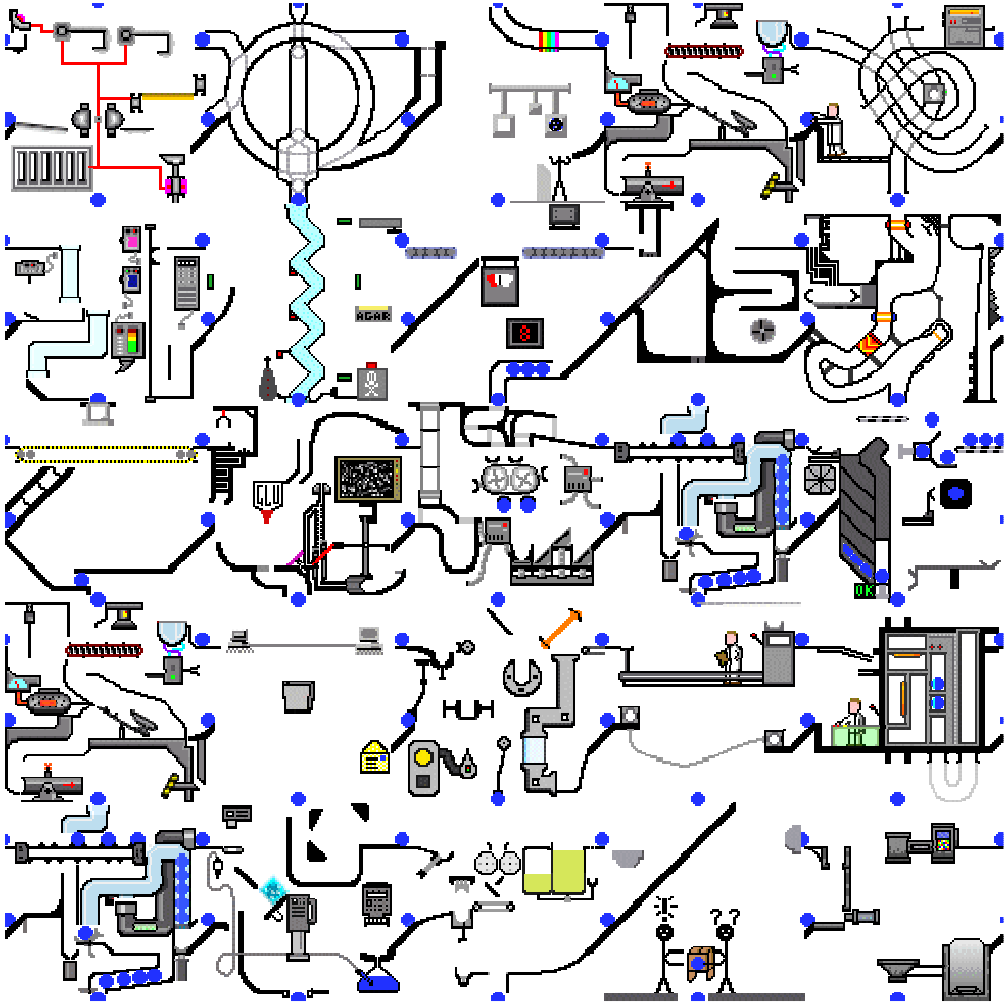
3a. Application Security Risk Management

Risk Tier	Applicability	Security
Extreme Risk	Internet facing transactional applications, especially of a financial nature.	Strongest identification, authentication, access control, PKI encryption vs SSL, storage encryption. Continuous vulnerability testing.
High Risk	Applications that handle financial data; privacy regulated data; intellectual property; company sensitive or restricted data. Internet facing or not.	Strong identity authentication, access control, SSL, storage encryption, and standard vulnerability testing.
Moderate Risk	Other core business applications; non-transactional Internet facing apps	Baseline security controls
Low Risk	All others	Baseline security controls

4. Application Project Security Architects



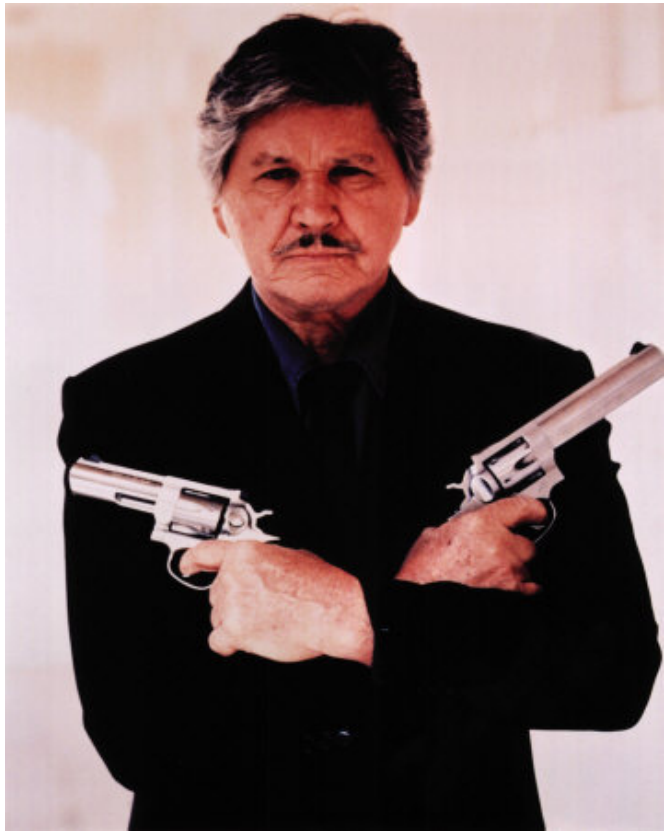
4a. A More Whimsical Diagram



5. Security Architect as a Consultant

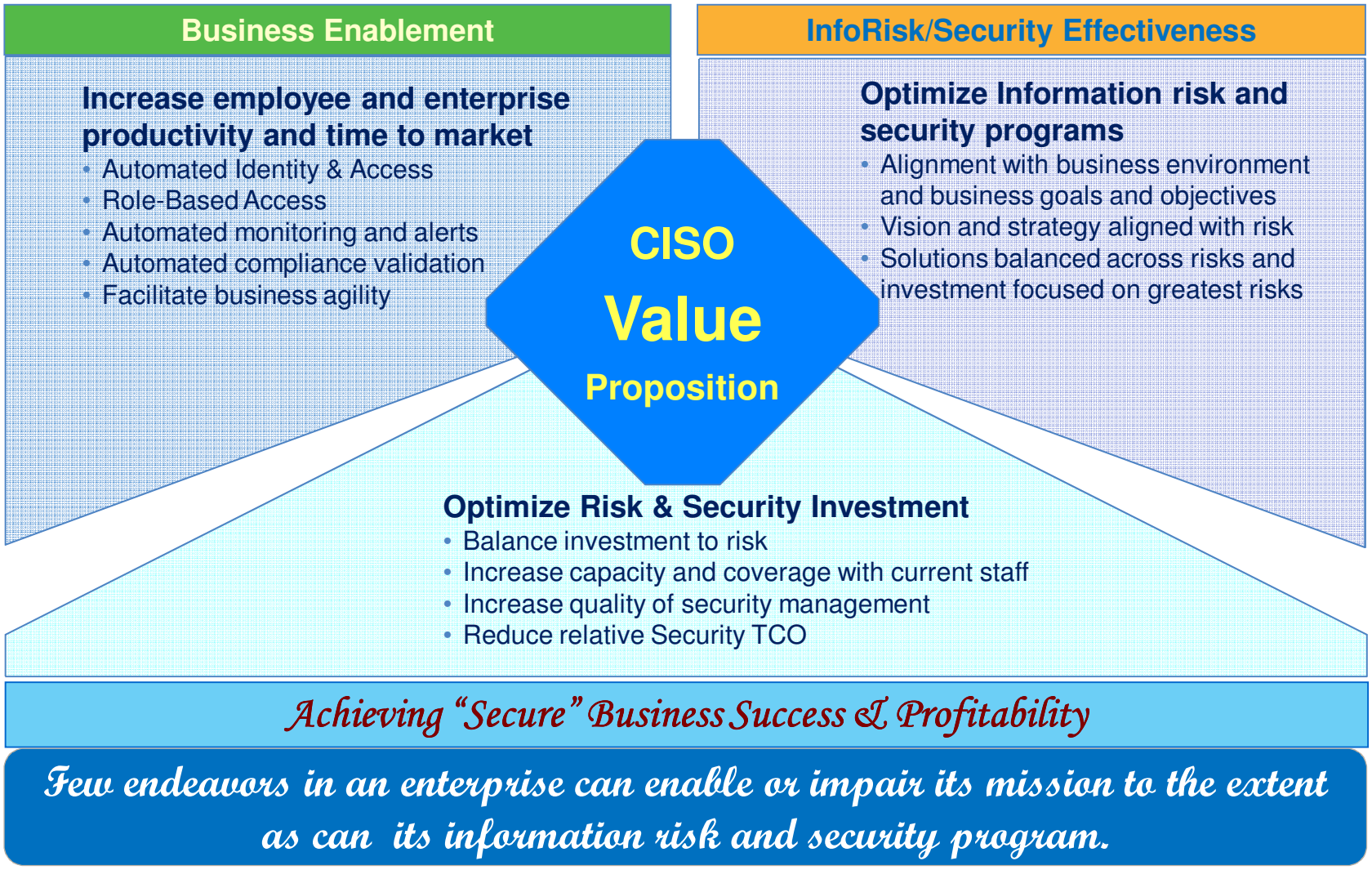
Do This!

Not This!



The CISO's Challenge

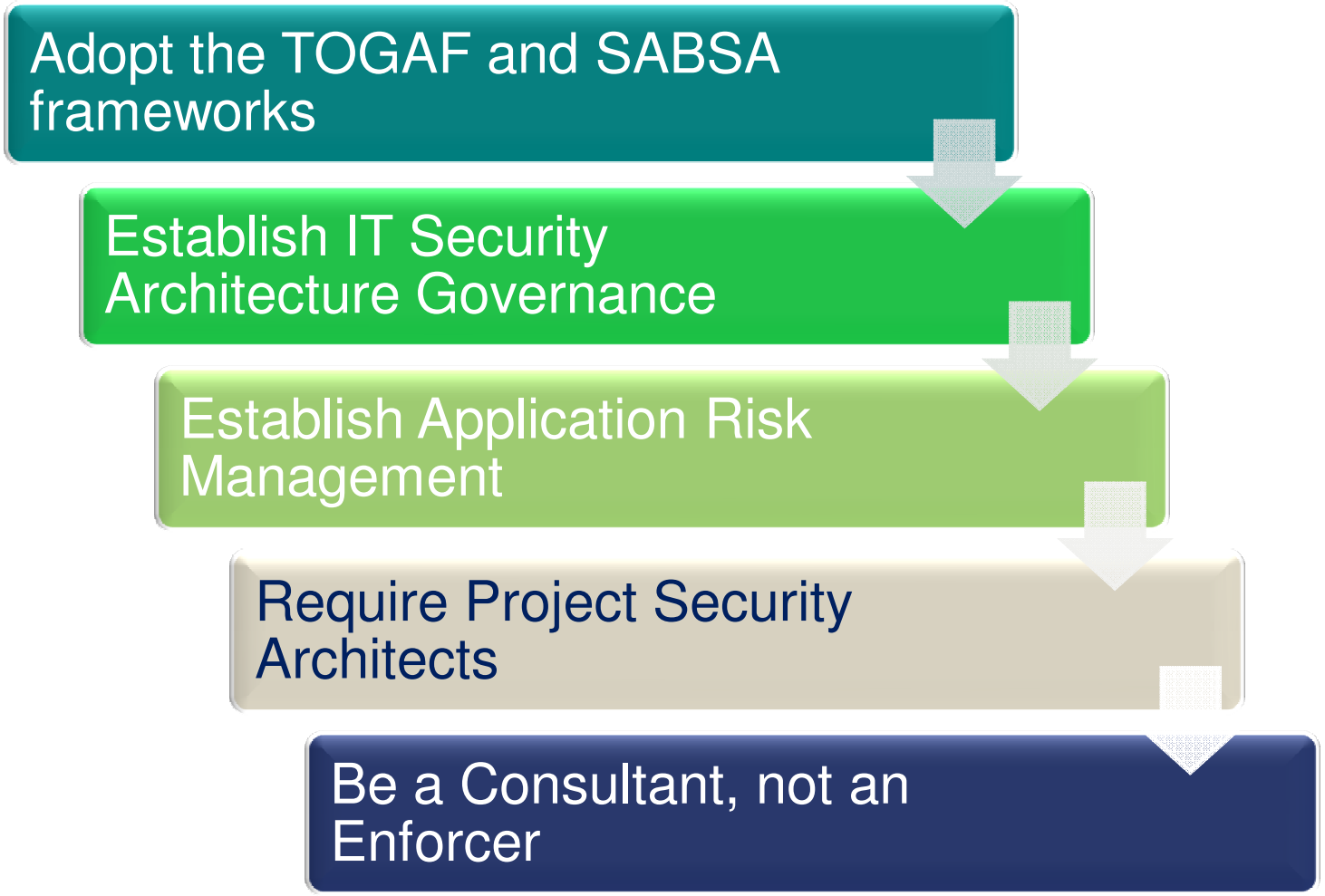
Balancing Protection, Compliance, Enablement, Productivity, Profitability



Achieving "Secure" Business Success & Profitability

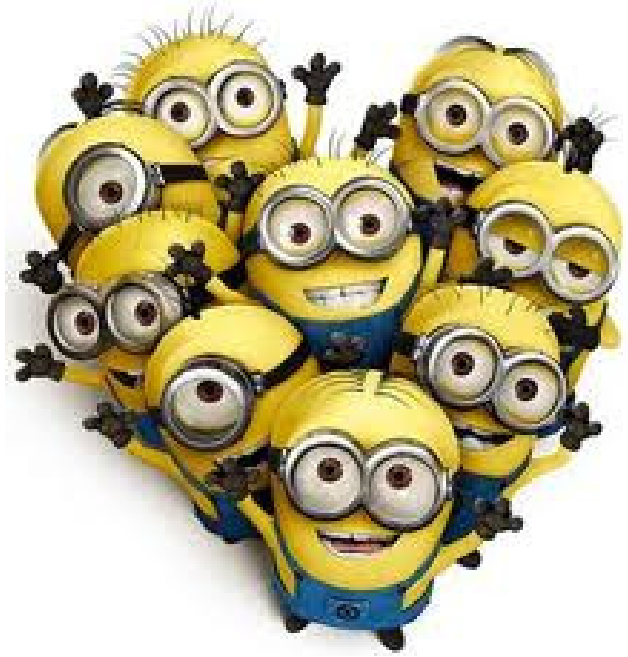
Few endeavors in an enterprise can enable or impair its mission to the extent as can its information risk and security program.

Summary of Better Practices for Application Security Architecture



The End! Thank you!

Questions?



The Minions of Despicable Me