MulticoreWorld XI 2024

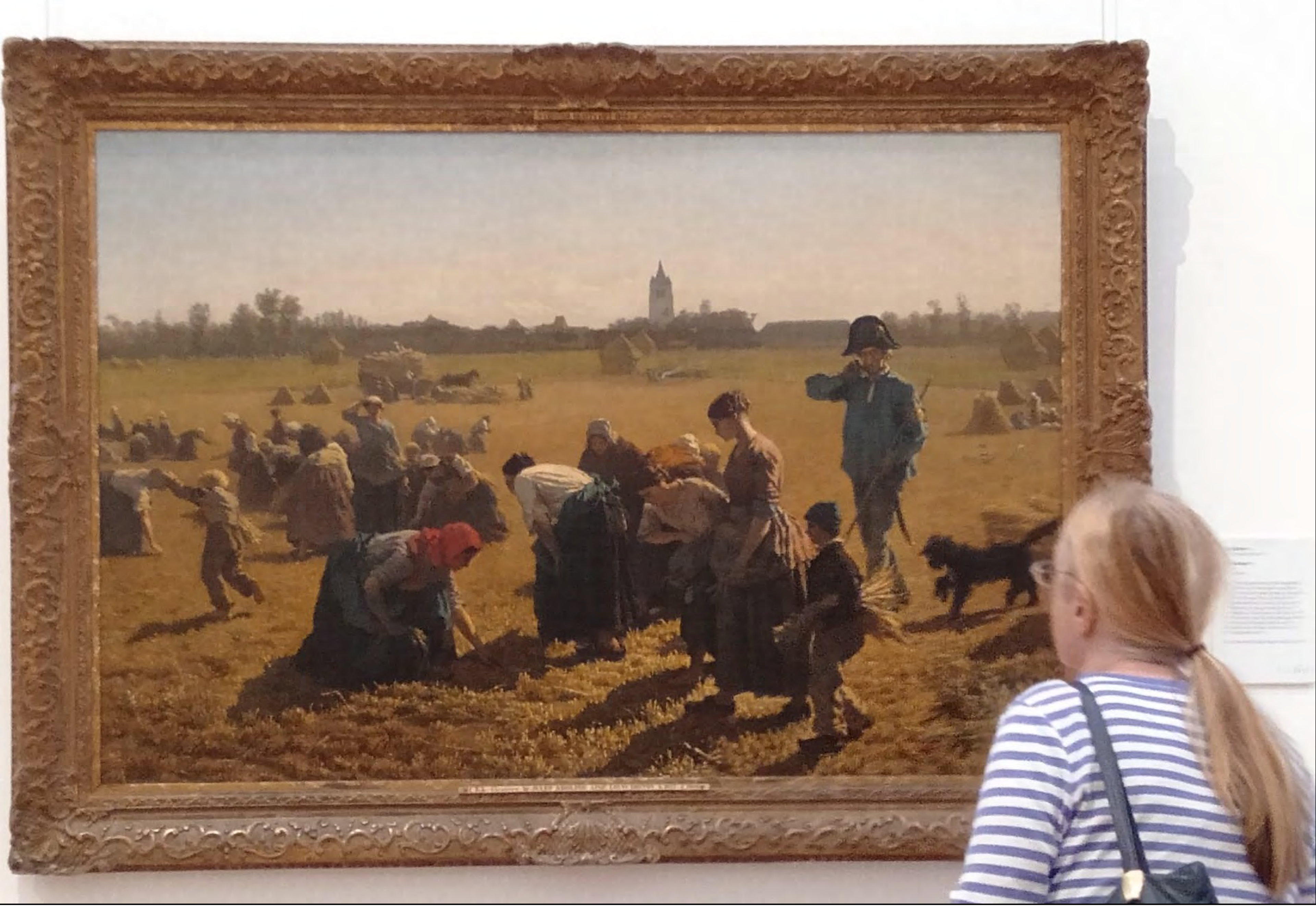
Sorting the wheat from the chaff:

Using SABSA
to prioritise
cybersecurity countermeasures
for HPC

EUR ING Duncan Hall
2024-02-15

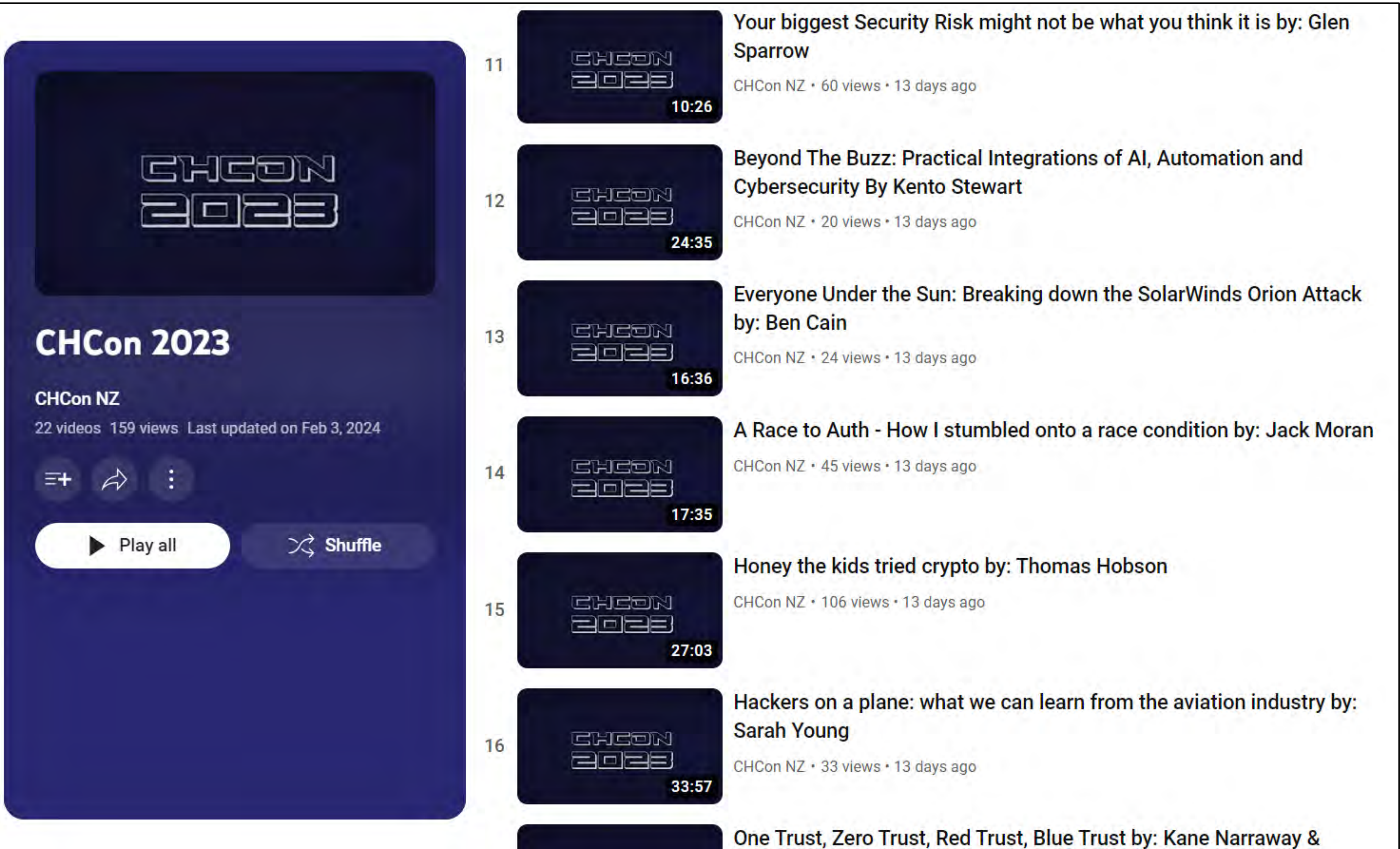
He kōrero mōku (introducing myself):

Nau mai haere mai	**Welcome everyone**
Kō Duncan Hall toku ingoa	**My name is Duncan Hall**
Kei te Whanganui-a-Tara e noho ana ahau	**I’m from Wellington**
Kō Manatū Aorere te wāhi tari	**(*I work at*) (*literally*) the Ministry of Flying Around the World ☺** **Ministry of Foreign Affairs and Trade** **≡ Department of State, FCDO, DFAT**
Kō kaihanga pūnaha matihiko tōku rōpū mahi	**(*I work in*) digital (*literally, digit – as in finger, and brain*) systems development** **≡ informatics**
Kō te mahi Kaiwetepanga Ngaio Whaimana tāku mahi	**I am a Chartered Professional Engineer** **≡ PEng (USA)**
Nō reira, kia ora tātou kātoa	**And so, greetings everyone**



Jules Breton: The Gleaners (1854), National Gallery of Ireland, 2023-10-01

FUD motivation: if you have not yet attended a "Con", I recommend you do so, at your earliest …



CHCon 2023

CHCon NZ

22 videos 159 views Last updated on Feb 3, 2024

11 Your biggest Security Risk might not be what you think it is by: Glen Sparrow
CHCon NZ • 60 views • 13 days ago
10:26

12 Beyond The Buzz: Practical Integrations of AI, Automation and Cybersecurity By Kento Stewart
CHCon NZ • 20 views • 13 days ago
24:35

13 Everyone Under the Sun: Breaking down the SolarWinds Orion Attack by: Ben Cain
CHCon NZ • 24 views • 13 days ago
16:36

14 A Race to Auth - How I stumbled onto a race condition by: Jack Moran
CHCon NZ • 45 views • 13 days ago
17:35

15 Honey the kids tried crypto by: Thomas Hobson
CHCon NZ • 106 views • 13 days ago
27:03

16 Hackers on a plane: what we can learn from the aviation industry by: Sarah Young
CHCon NZ • 33 views • 13 days ago
33:57

One Trust, Zero Trust, Red Trust, Blue Trust by: Kane Narraway &

Agenda

- SABSA
- Prioritisation
- Cybersecurity countermeasures

SABSA?

Sherwood

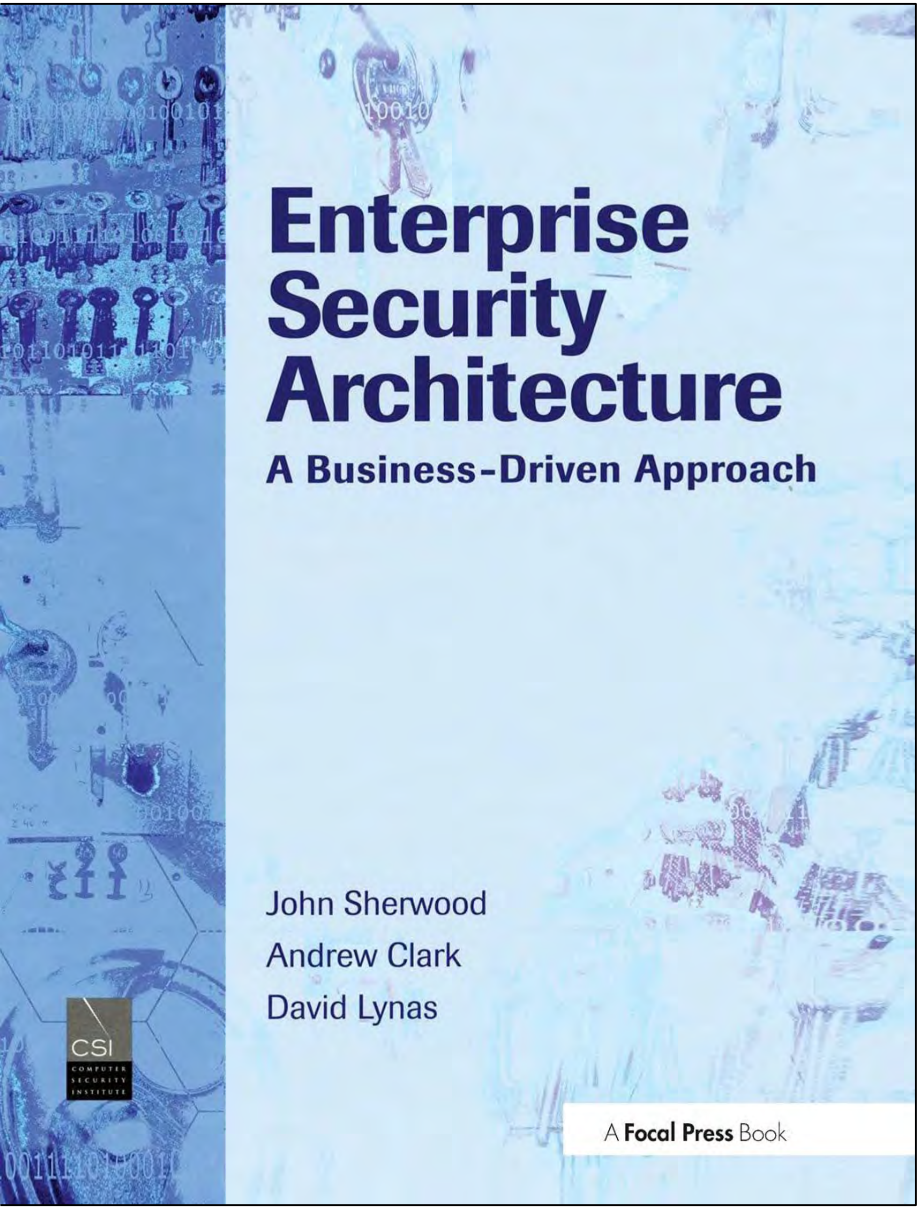
Applied

Business

Security

Architecture

The SABSA BoK, aka the "Blue Book":



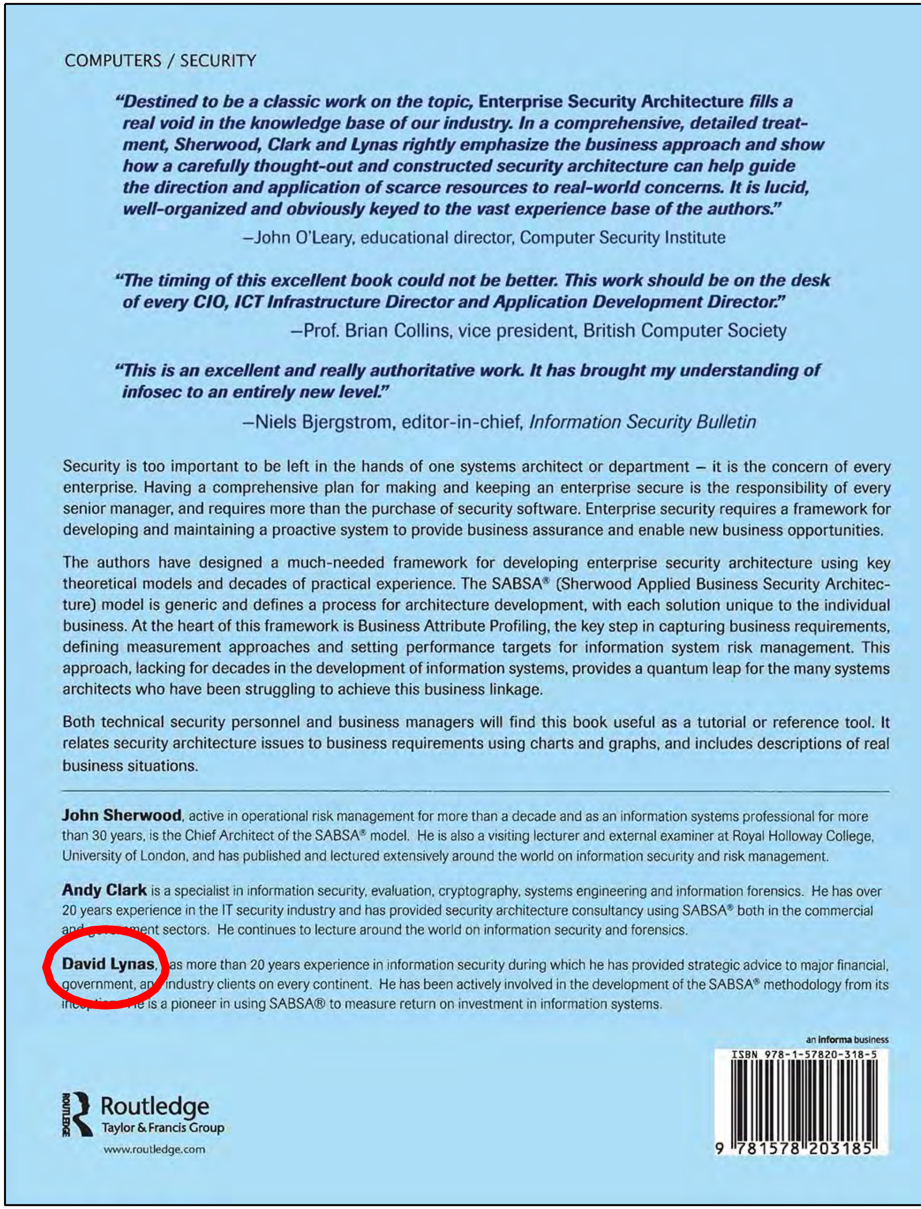
Enterprise Security Architecture

A Business-Driven Approach

John Sherwood
Andrew Clark
David Lynas

CSI COMPUTER SECURITY INSTITUTE

A Focal Press Book



COMPUTERS / SECURITY

> ***"Destined to be a classic work on the topic,* Enterprise Security Architecture *fills a real void in the knowledge base of our industry. In a comprehensive, detailed treatment, Sherwood, Clark and Lynas rightly emphasize the business approach and show how a carefully thought-out and constructed security architecture can help guide the direction and application of scarce resources to real-world concerns. It is lucid, well-organized and obviously keyed to the vast experience base of the authors."***
>
> —John O'Leary, educational director, Computer Security Institute

> ***"The timing of this excellent book could not be better. This work should be on the desk of every CIO, ICT Infrastructure Director and Application Development Director."***
>
> —Prof. Brian Collins, vice president, British Computer Society

> ***"This is an excellent and really authoritative work. It has brought my understanding of infosec to an entirely new level."***
>
> —Niels Bjergstrom, editor-in-chief, *Information Security Bulletin*

Security is too important to be left in the hands of one systems architect or department – it is the concern of every enterprise. Having a comprehensive plan for making and keeping an enterprise secure is the responsibility of every senior manager, and requires more than the purchase of security software. Enterprise security requires a framework for developing and maintaining a proactive system to provide business assurance and enable new business opportunities.

The authors have designed a much-needed framework for developing enterprise security architecture using key theoretical models and decades of practical experience. The SABSA® (Sherwood Applied Business Security Architecture) model is generic and defines a process for architecture development, with each solution unique to the individual business. At the heart of this framework is Business Attribute Profiling, the key step in capturing business requirements, defining measurement approaches and setting performance targets for information system risk management. This approach, lacking for decades in the development of information systems, provides a quantum leap for the many systems architects who have been struggling to achieve this business linkage.

Both technical security personnel and business managers will find this book useful as a tutorial or reference tool. It relates security architecture issues to business requirements using charts and graphs, and includes descriptions of real business situations.

John Sherwood, active in operational risk management for more than a decade and as an information systems professional for more than 30 years, is the Chief Architect of the SABSA® model. He is also a visiting lecturer and external examiner at Royal Holloway College, University of London, and has published and lectured extensively around the world on information security and risk management.

Andy Clark is a specialist in information security, evaluation, cryptography, systems engineering and information forensics. He has over 20 years experience in the IT security industry and has provided security architecture consultancy using SABSA® both in the commercial and government sectors. He continues to lecture around the world on information security and forensics.

David Lynas, has more than 20 years experience in information security during which he has provided strategic advice to major financial, government, and industry clients on every continent. He has been actively involved in the development of the SABSA® methodology from its inception. He is a pioneer in using SABSA® to measure return on investment in information systems.

an informa business

ISBN 978-1-57820-318-5

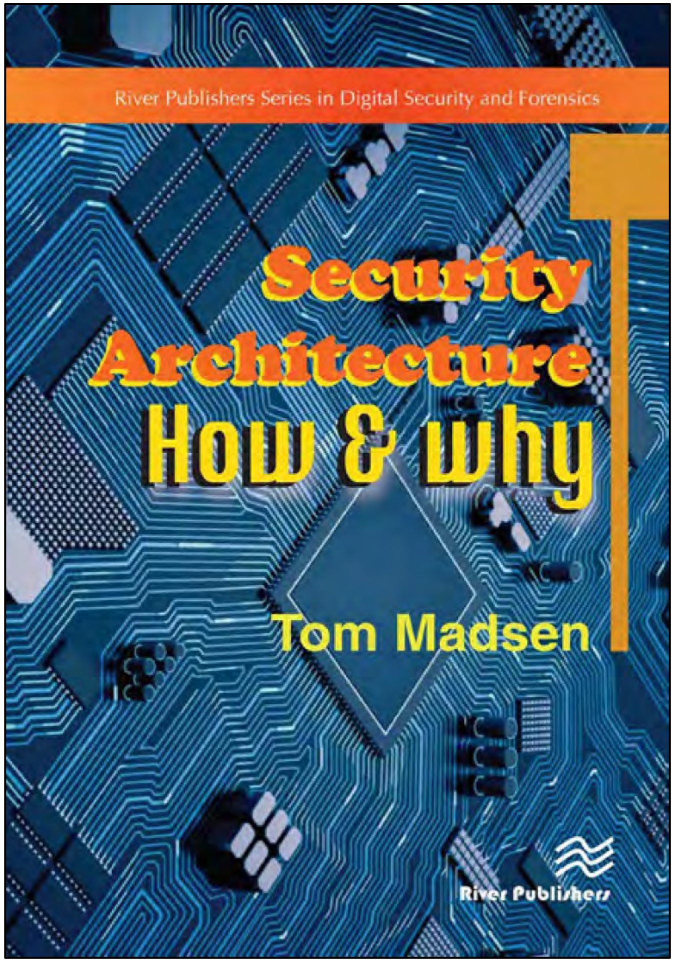
9 781578 203185

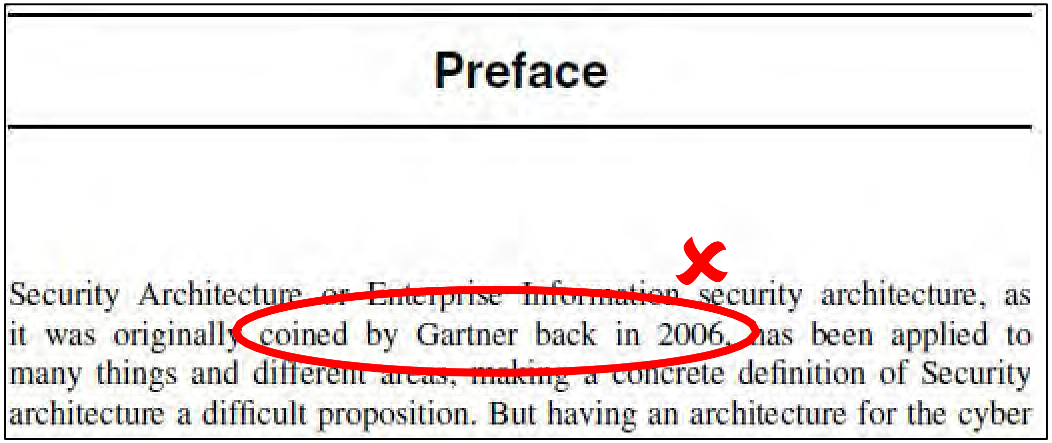
ROUTLEDGE Routledge
Taylor & Francis Group
www.routledge.com

David Lynas, DLC's CEO

Dr. Malcolm Shore, DLC's CSA

Tom Madsen’s 2022 book: recent, but some errors . . .





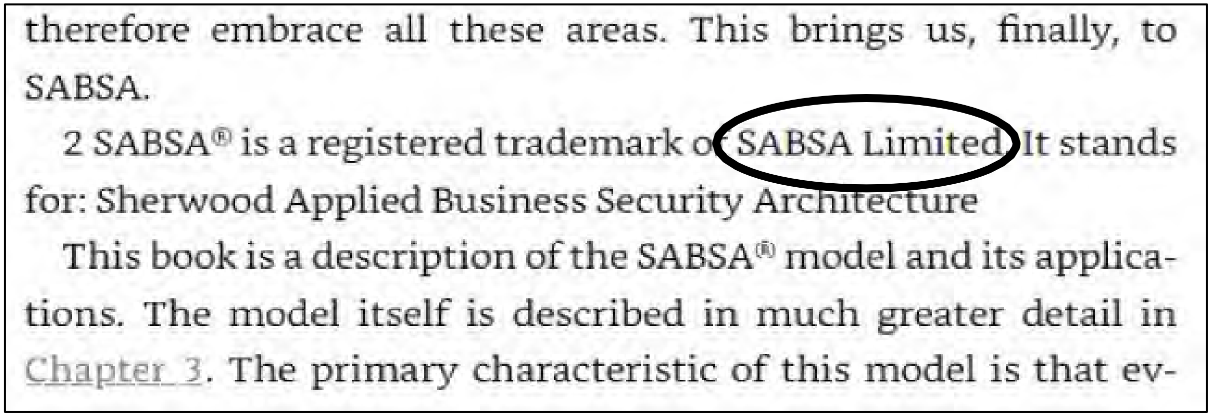
Preface

✘

Security Architecture or Enterprise Information security architecture, as it was originally coined by Gartner back in 2006, has been applied to many things and different areas, making a concrete definition of Security architecture a difficult proposition. But having an architecture for the cyber

✓ SABSA in 1995

✓ ISO7498 Part 2



therefore embrace all these areas. This brings us, finally, to SABSA.

2 SABSA® is a registered trademark of SABSA Limited. It stands for: Sherwood Applied Business Security Architecture

This book is a description of the SABSA® model and its applications. The model itself is described in much greater detail in Chapter 3. The primary characteristic of this model is that ev-

✓ SABSA Institute Community of Interest Corporation

SABSA:

An enterprise security architecture model

that takes a business-driven

risk-based approach

to developing security solutions

that are aligned with business needs

SABSA:

Starts with understanding:

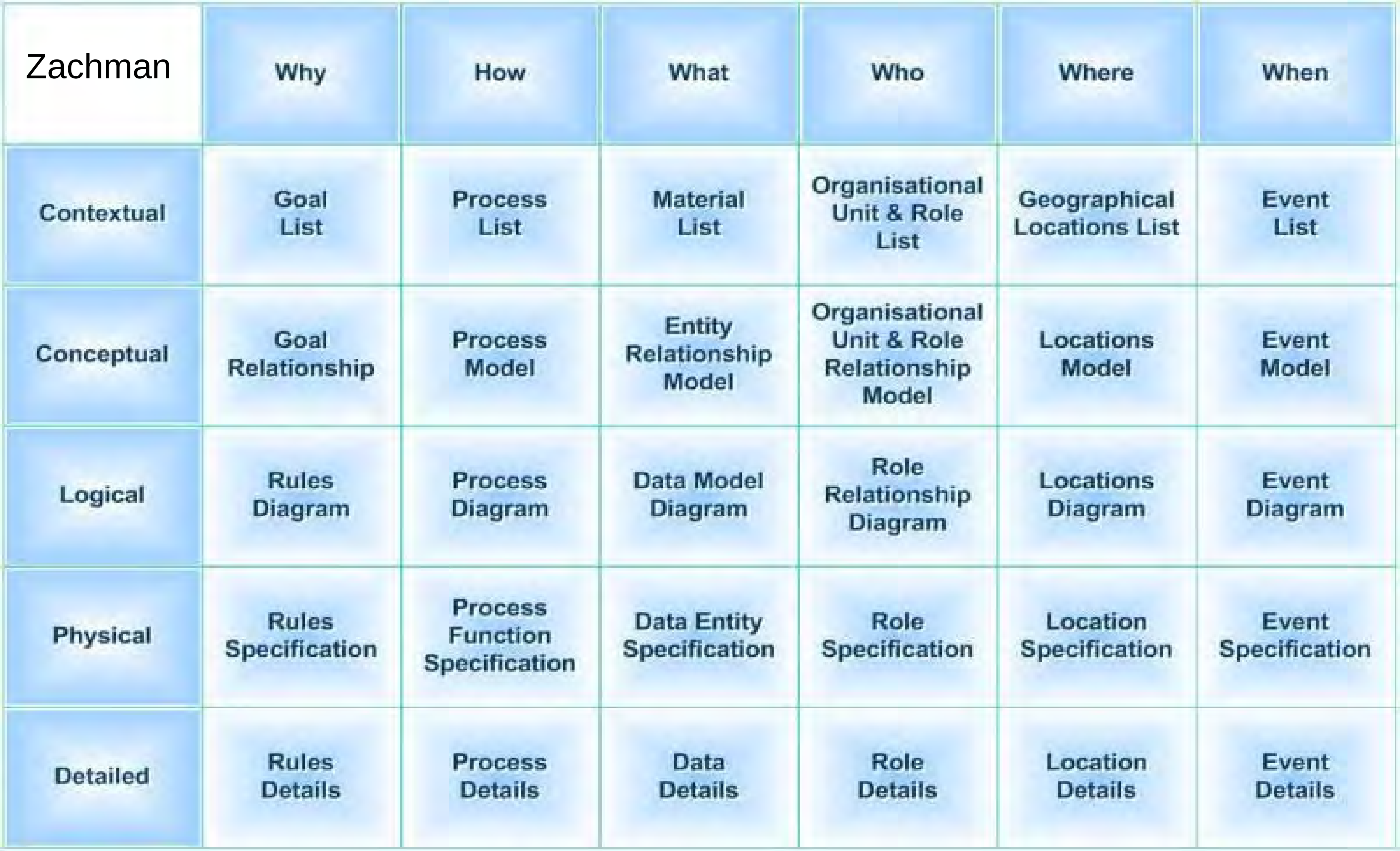
- the organisation’s drivers
- the organisation’s goals, and
- the organisation’s risk appetite

SABSA:

Specific techniques – examples only:

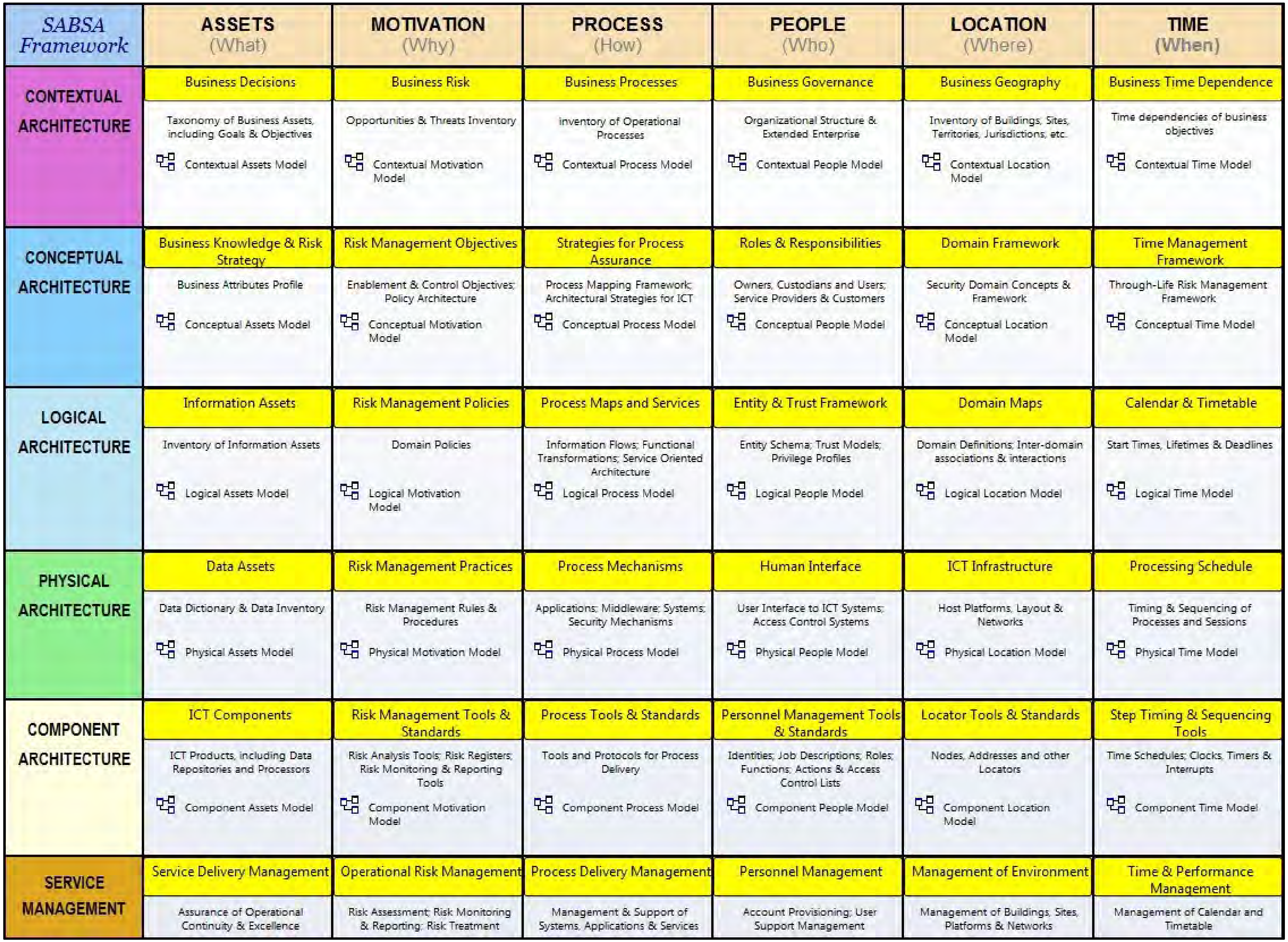
- Business attributes profiling
- Align information and digital services risk model to organisation’s risk model
- Assess control objectives and security strategies
- Taylor implementation to context
- Prioritisation

SABSA is closely aligned to the Zachman framework:



Zachman	Why	How	What	Who	Where	When
Contextual	Goal List	Process List	Material List	Organisational Unit & Role List	Geographical Locations List	Event List
Conceptual	Goal Relationship	Process Model	Entity Relationship Model	Organisational Unit & Role Relationship Model	Locations Model	Event Model
Logical	Rules Diagram	Process Diagram	Data Model Diagram	Role Relationship Diagram	Locations Diagram	Event Diagram
Physical	Rules Specification	Process Function Specification	Data Entity Specification	Role Specification	Location Specification	Event Specification
Detailed	Rules Details	Process Details	Data Details	Role Details	Location Details	Event Details

The Zachman framework is closely aligned to SABSA:



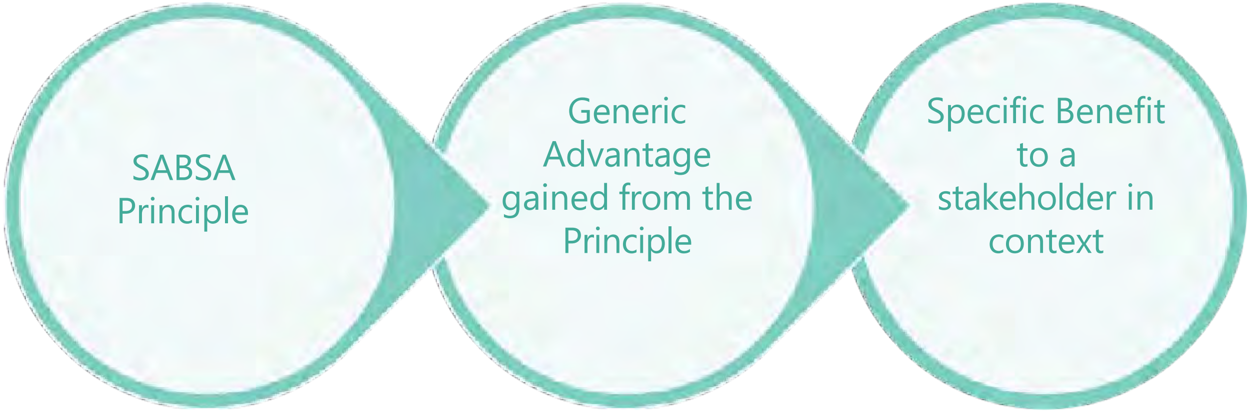
SABSA Framework	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions Taxonomy of Business Assets, including Goals & Objectives Contextual Assets Model	Business Risk Opportunities & Threats Inventory Contextual Motivation Model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

SABSA:

traceably
prioritising
security
controls

PAB: Principles → Advantages → Benefits:

The SABSA PAB transposes principles into specific adoptable benefits in a stakeholder context


SABSA Principle
Generic Advantage gained from the Principle
Specific Benefit to a stakeholder in context

SABSA Principle: The fundamental propositions to benefit business and serve solutions

SABSA Advantage: The generic improvement or success gained from the principle

SABSA Benefit: The specific improvement or success, to a particular stakeholder, in a particular context

SABSA PAB traceability examples:

Principle	Advantage	Benefit to	Benefit
Enable business	Value-assured	CIO	Enables value from digital transformation
Inspire trust	Assures stakeholder confidence	Head of Product Development	Provides assurance to our customers that our engineering processes are trustworthy and that our products can be trusted
Balance risk	Prioritised and proportional response	CTO	Technology risk is understood in the overall context of business risks and opportunities
Create certainty and clarity	Effective governance and risk ownership	CRO	Ownership, accountability, and responsibility for security-related risk is clearly defined and assigned
Establish common culture and Language	Enables collaboration, integration and adoption	CTO	The SABSA Architecture supports the goals and objectives of our Agile team, and integrates and aligns with our Agile method
Solve holistically	Systemic understanding	COO	The positive and negative effects of changes to be introduced by any plan of action are understood enterprise-wide

Prioritisation?

SABSA

and prioritisation (i.e. optimisation) for cybersecurity controls:

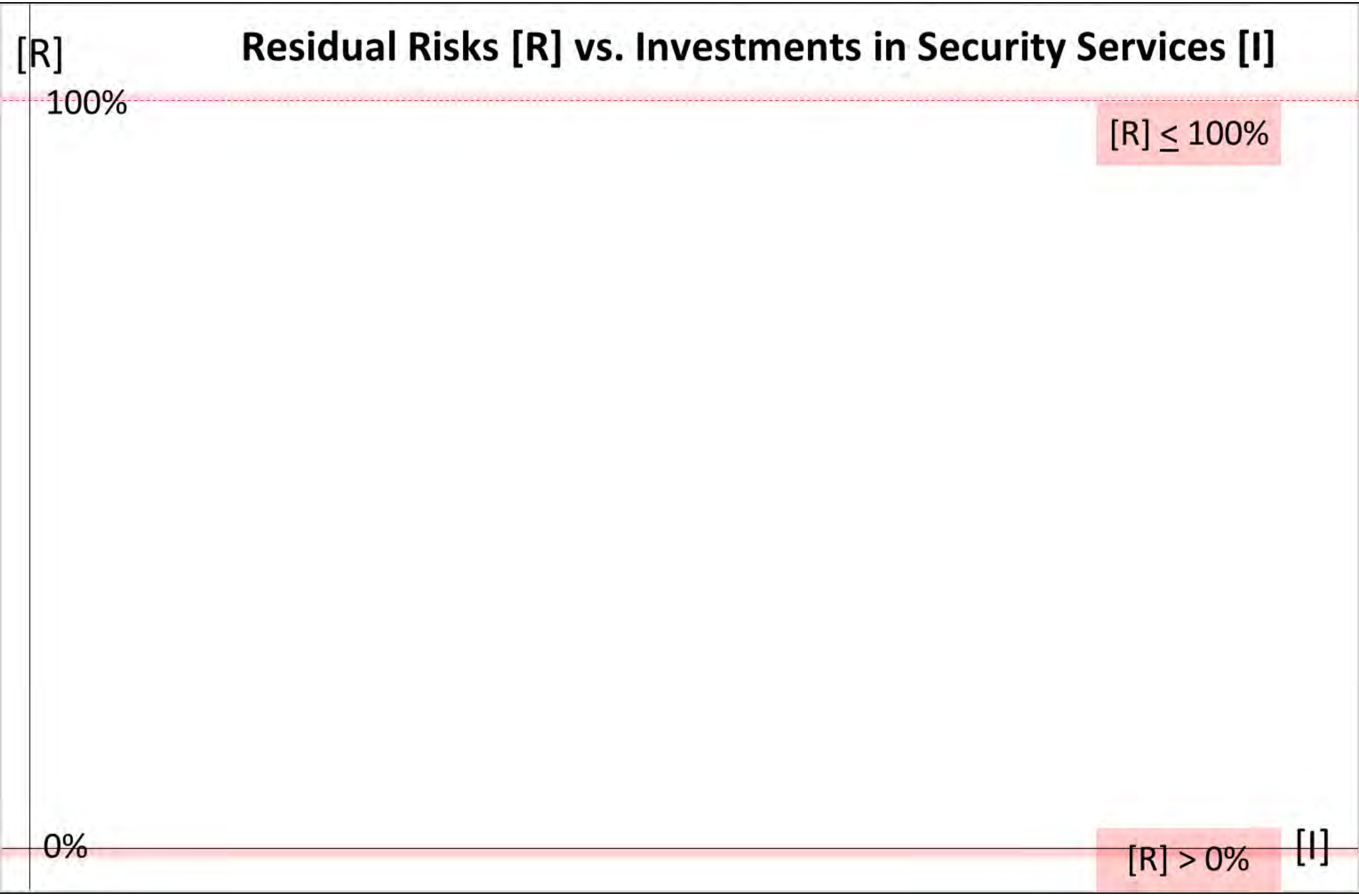
a linear programming construct

A linear programming construct to visualise SABSA in context: 1 of 7

Residual Risks [R] vs. Investments in Security Services [I]
[R]
100%
0%
[I]

Setting up a visualisation of the trade-offs between [R] and [I]

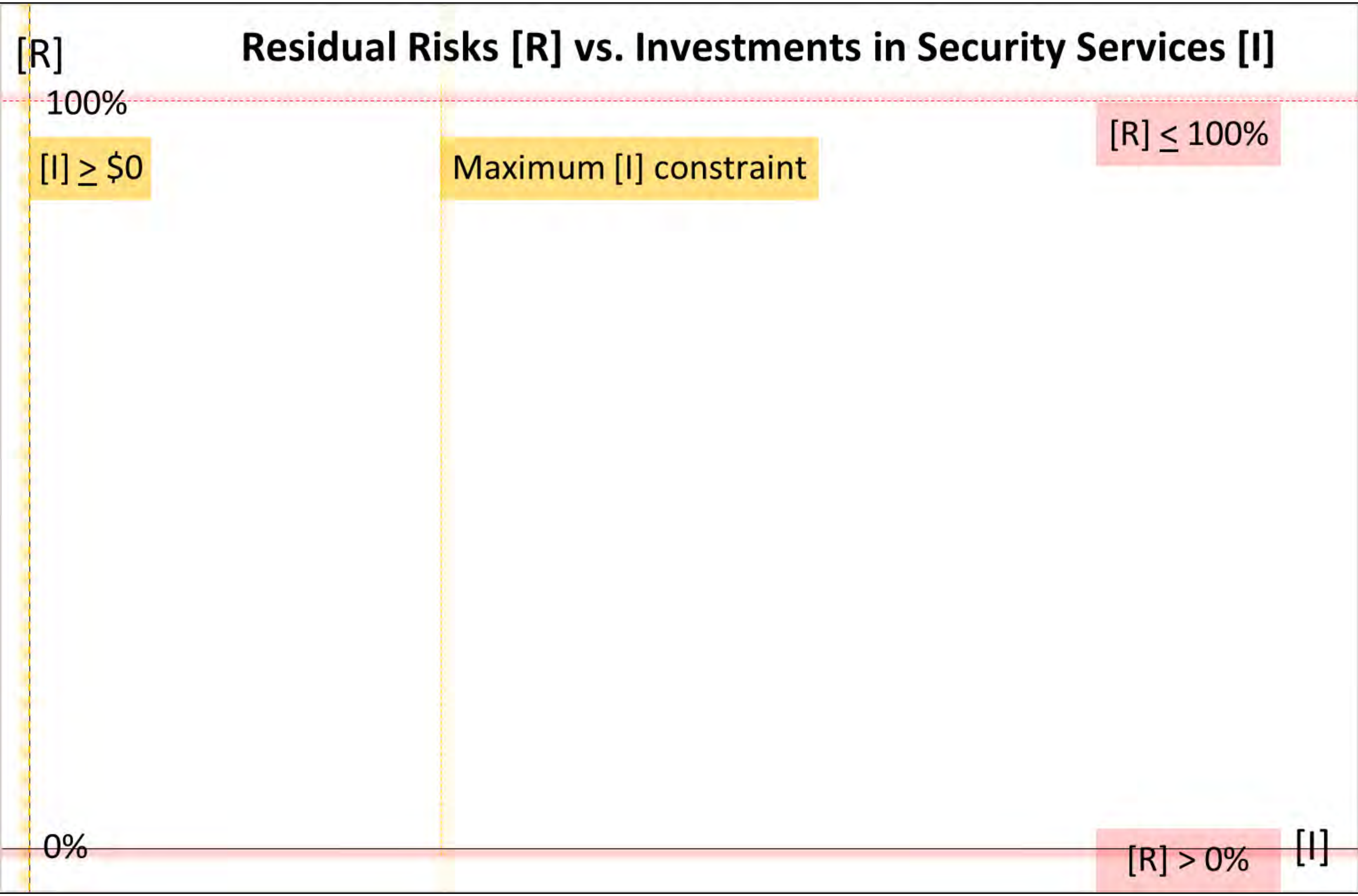
Untreated [R] set at 100%; [R] can never be negative



Residual Risks [R] vs. Investments in Security Services [I]

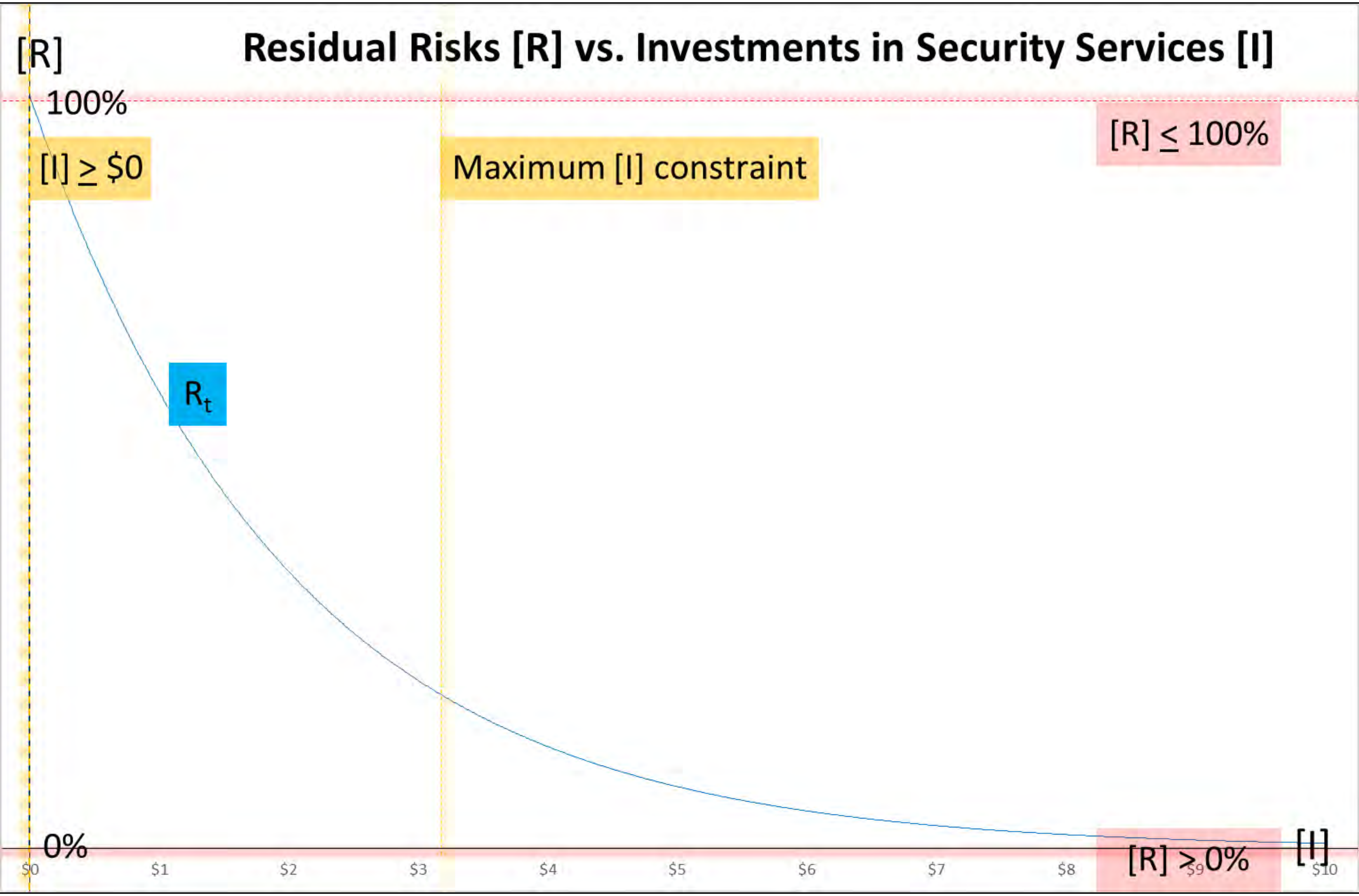
No matter what the [I], there will always be some residual risk

[I] can never be negative; there will always be a constraint on funds for [I]



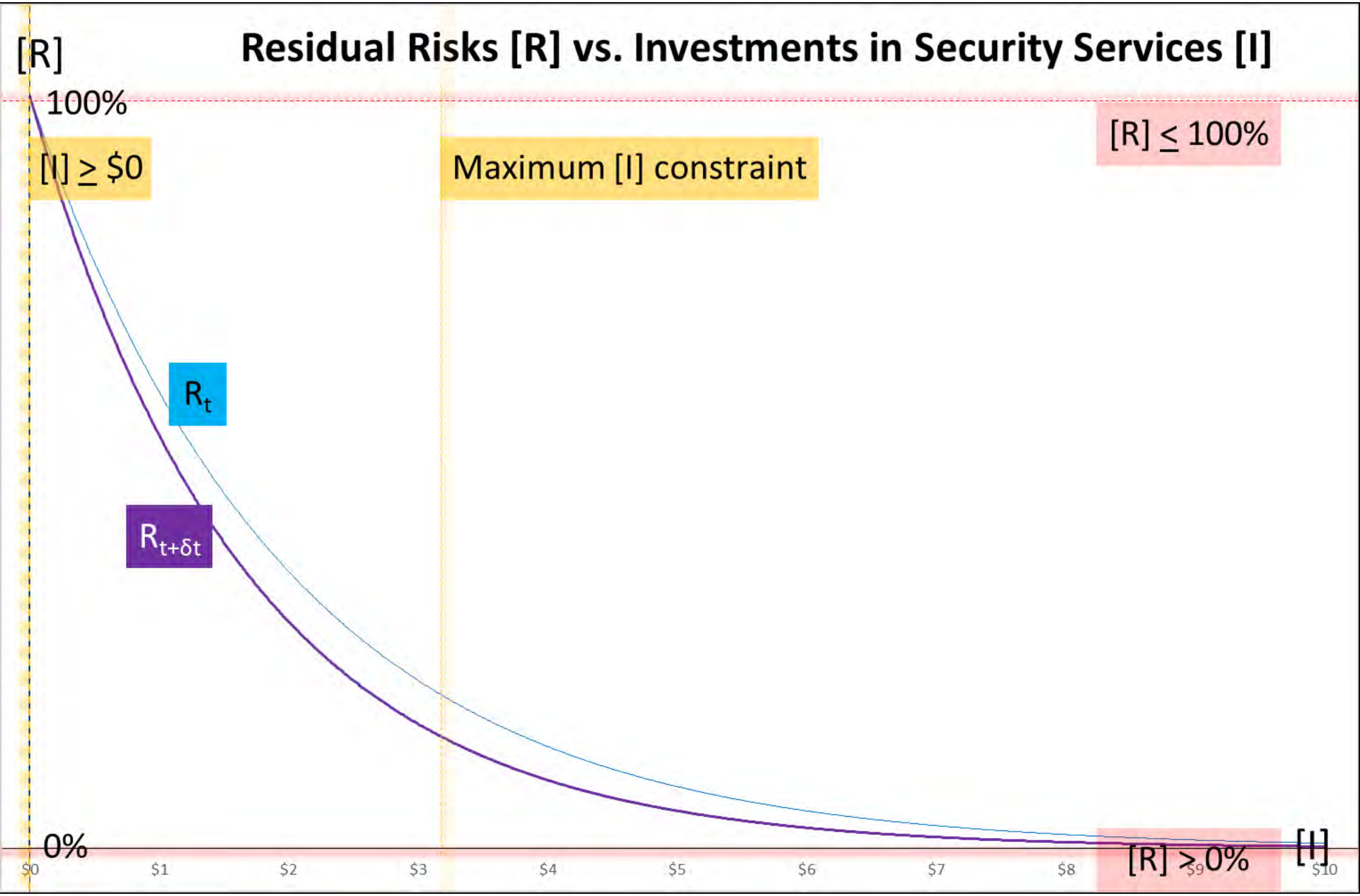
As a soft constraint, increasing Maximum [I] usually requires Cost-Benefit justification

Increased [I] usually results in an ~exponentially reducing [R]



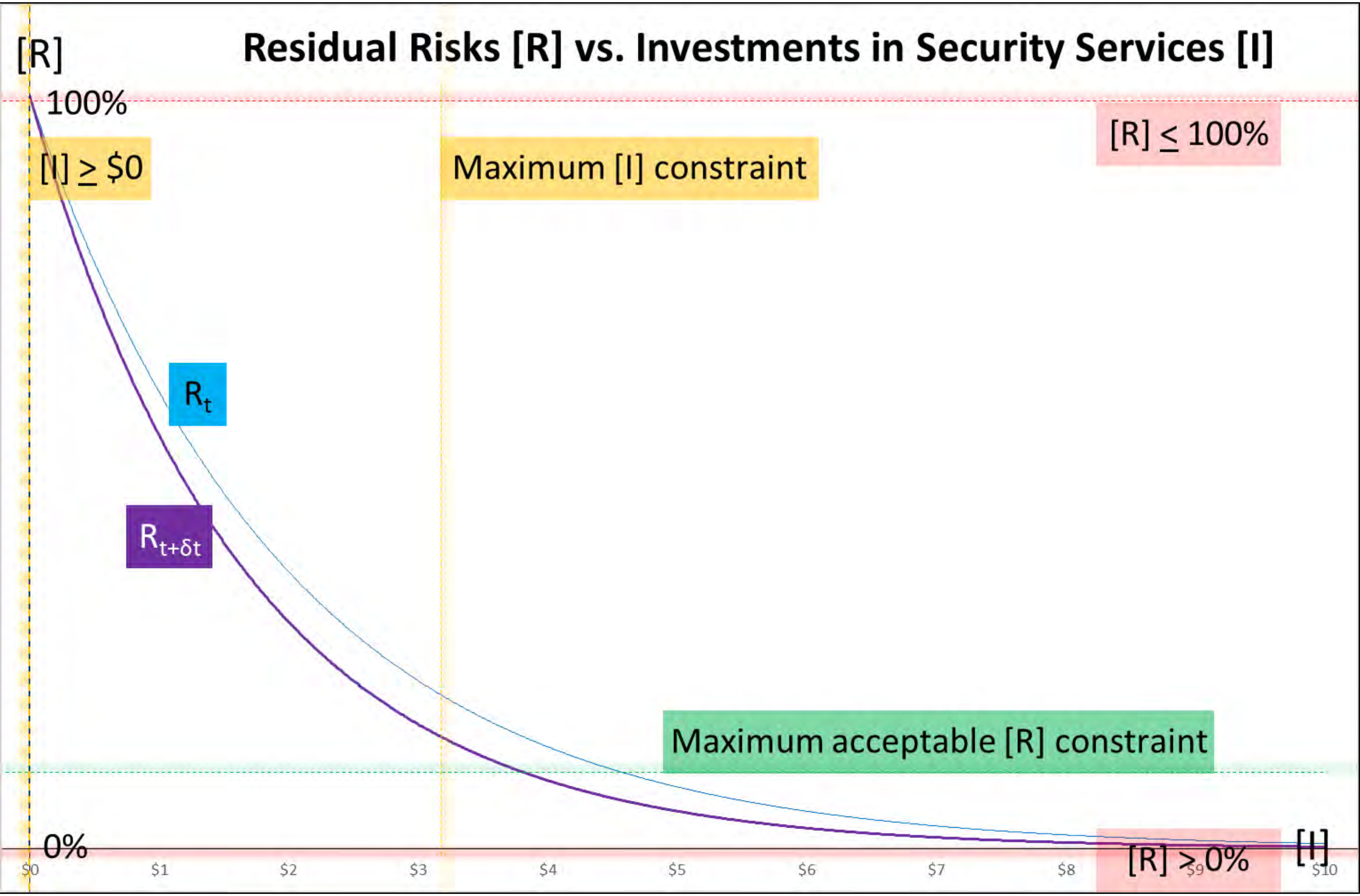
No matter what the [I], there will always be some residual risk

SABSA facilitates exploration of various Security Services to reduce [R] over time



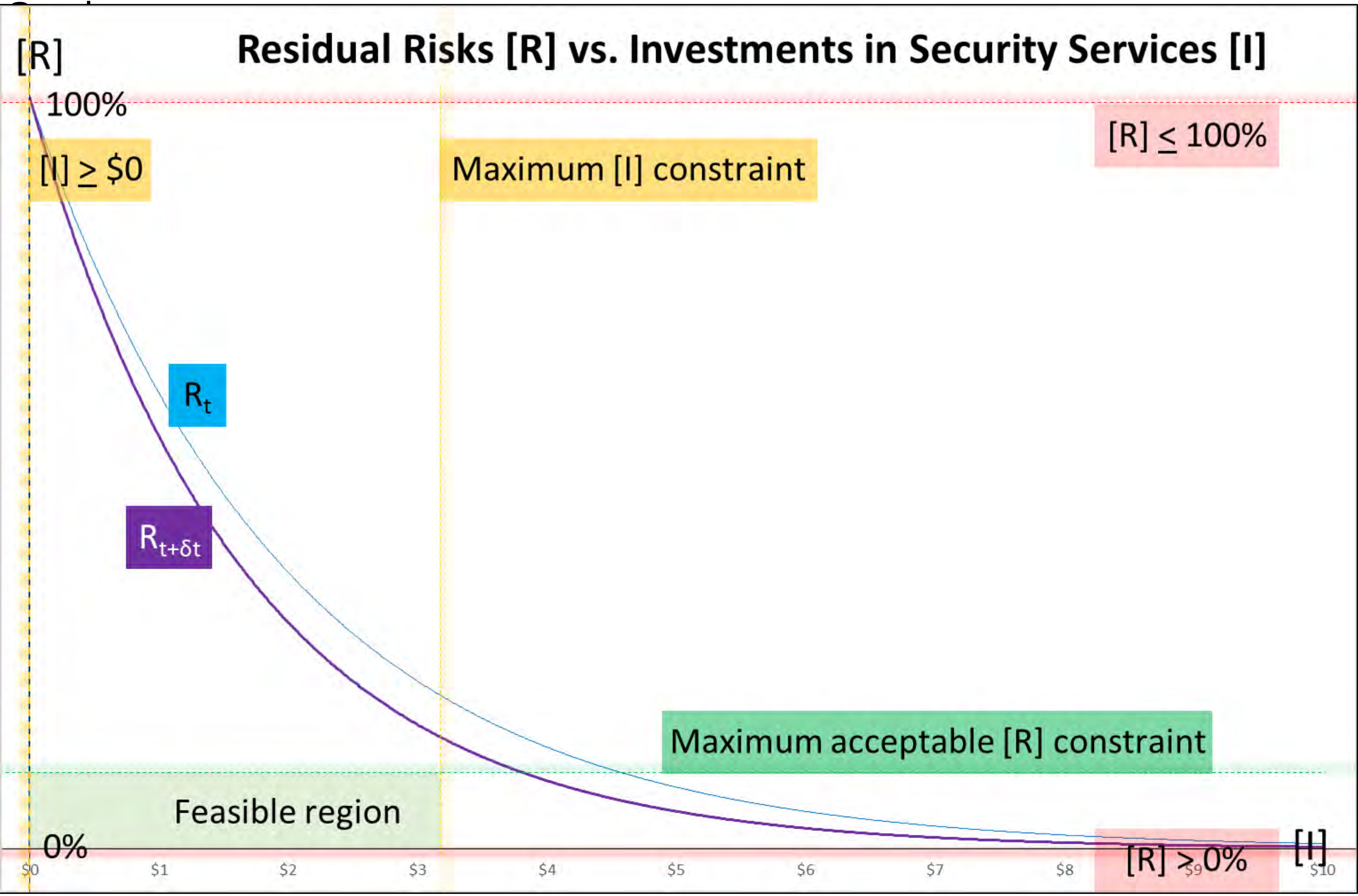
In this example, after an incremental time δt, a lower [R] results for all [I]

Key stakeholders must define their maximum acceptable [R]



Quantifying [R] can be difficult, however relative [R] is often more easily understood

Constraints define a ‘Feasible region’ as a target for prioritised [I] in Security



Requires increase in either Max[I] and/or Max[R]; or more effective Security Services

Cybersecurity countermeasures (‘controls’)?

SABSA:

5 “+1” alternative frameworks to prioritise security controls

Prioritisation of cybersecurity controls – alternatives (1A of 5):

NIST SP 800-223 – High-Performance Computing Security, *Architecture, Threat Analysis, and Security Posture*, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

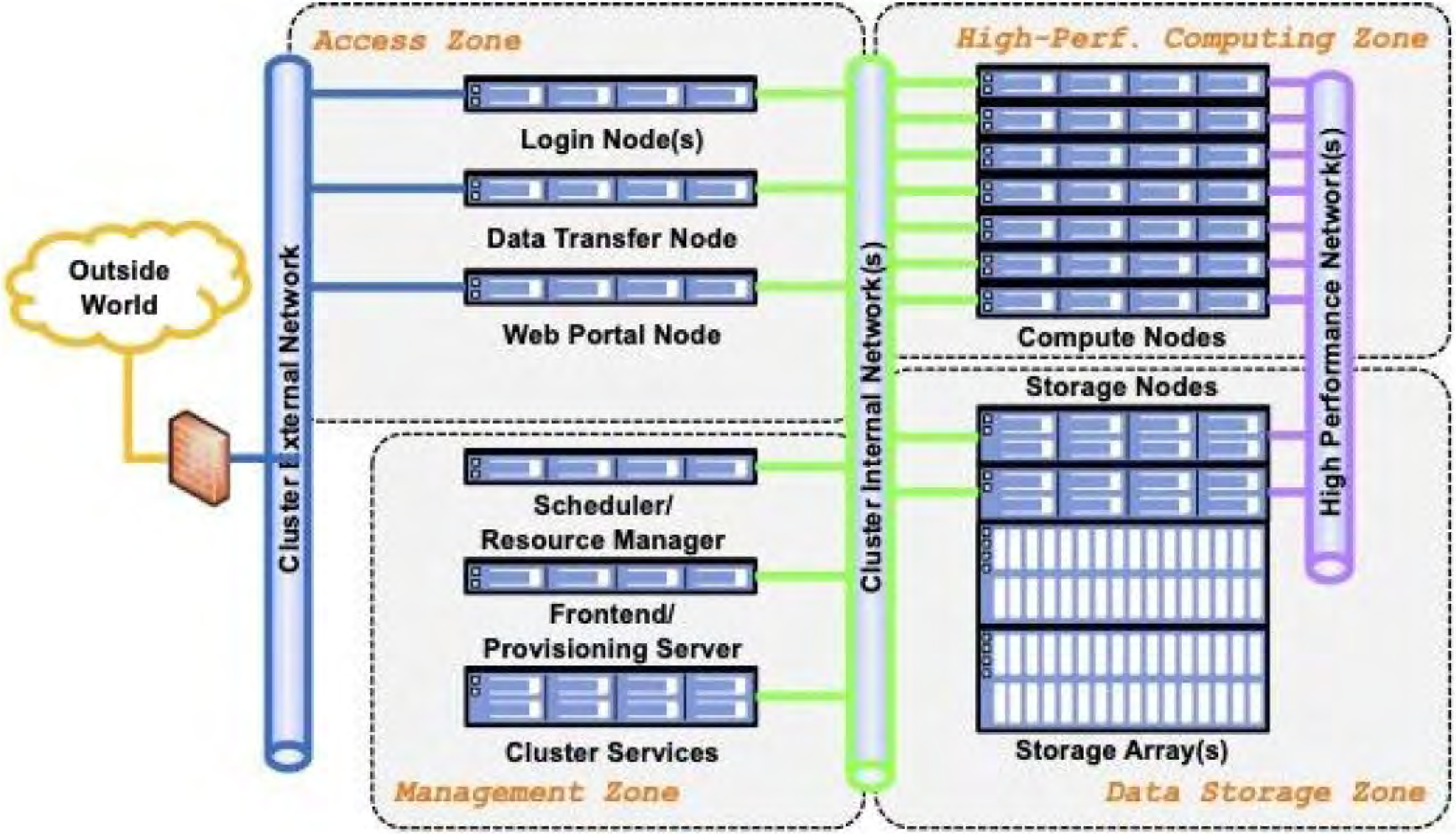


Fig. 1. HPC System Reference Architecture

Prioritisation of cybersecurity controls – alternatives (1B of 5):

NIST SP 800-55v2 ipd – Measurement Guide for Information Security,
Volume 2 – Developing an Information Security Measurement Program, 2024

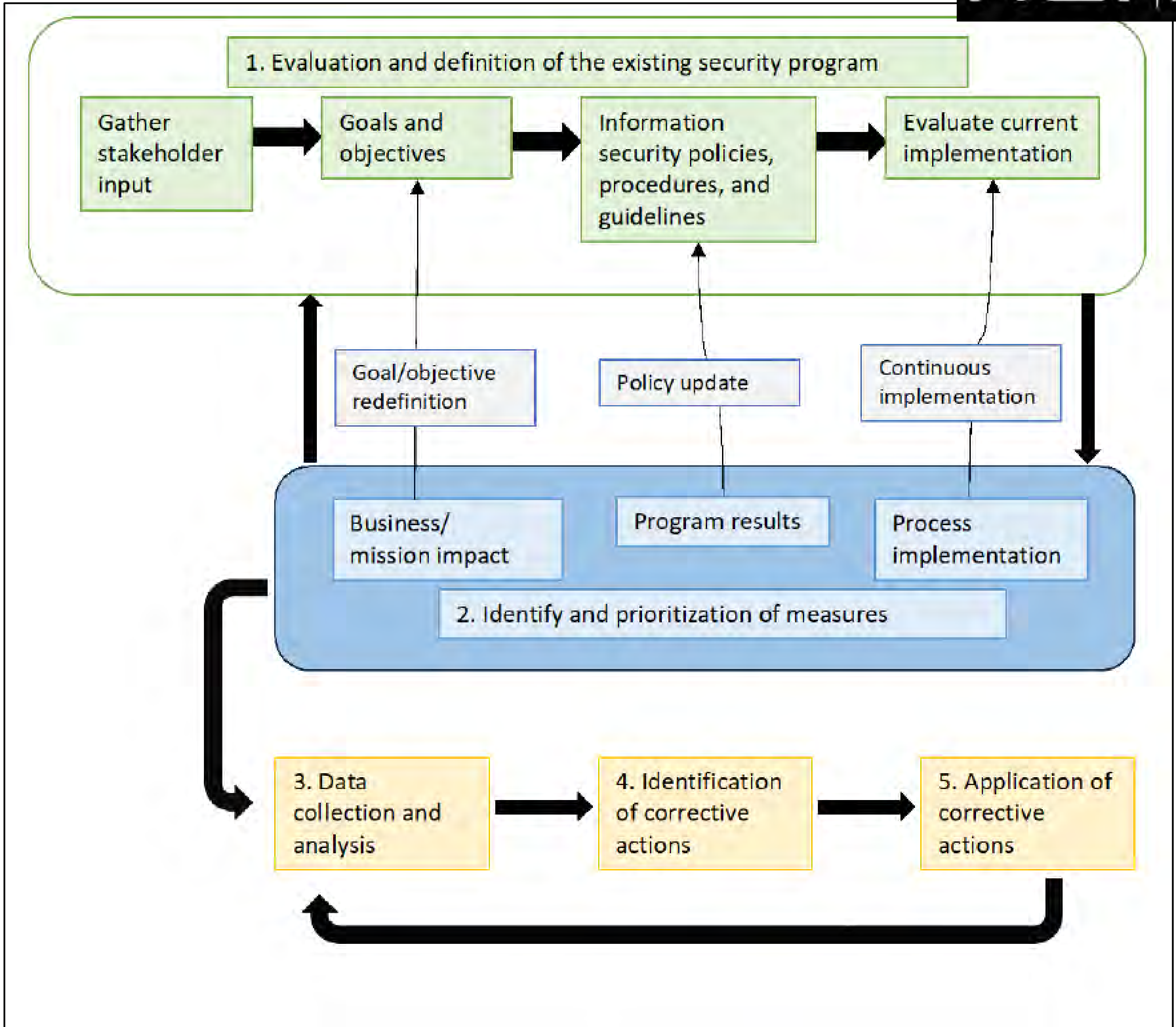
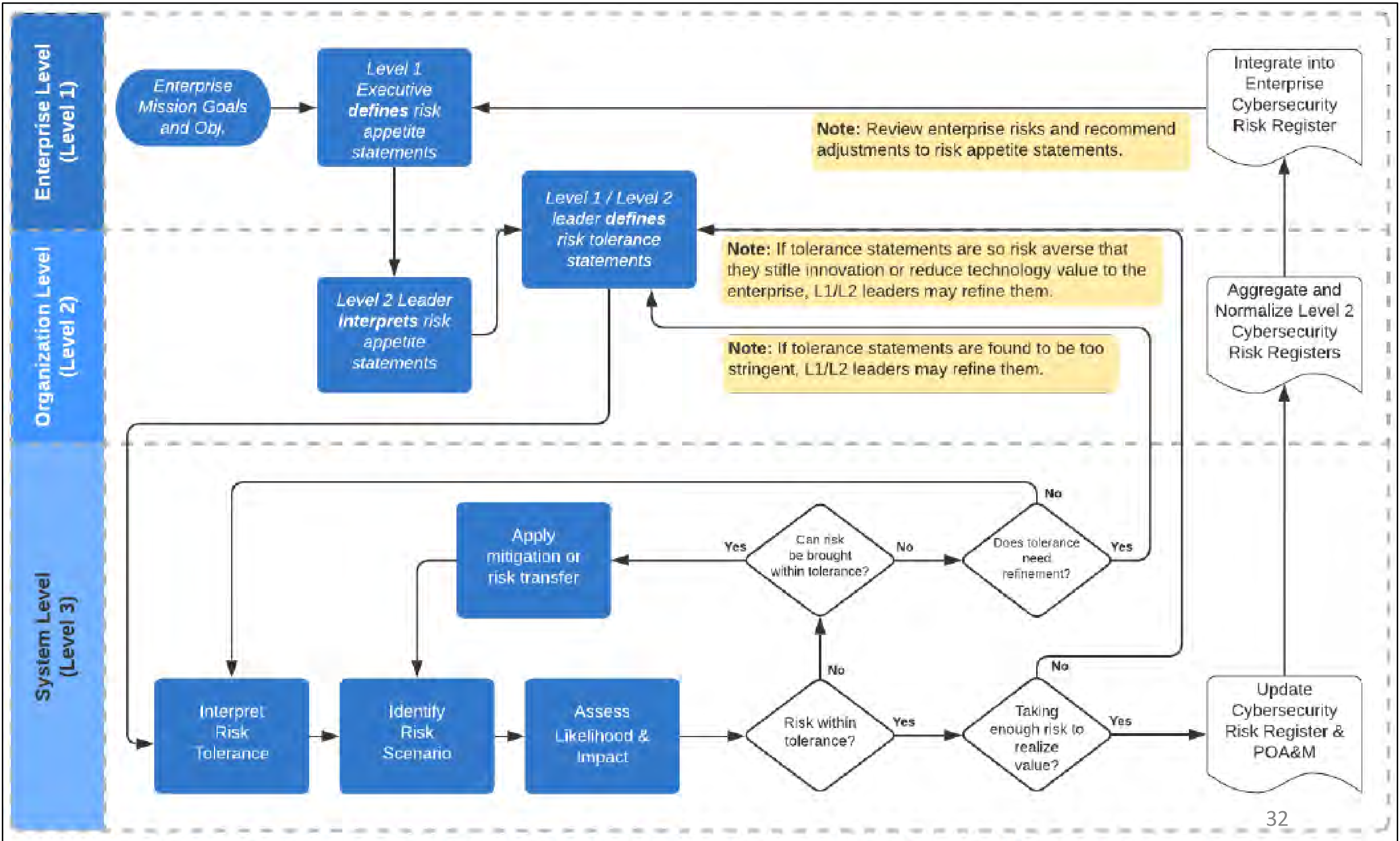

1. Evaluation and definition of the existing security program
Gather stakeholder input
Goals and objectives
Information security policies, procedures, and guidelines
Evaluate current implementation
Goal/objective redefinition
Policy update
Continuous implementation
Business/ mission impact
Program results
Process implementation
2. Identify and prioritization of measures
3. Data collection and analysis
4. Identification of corrective actions
5. Application of corrective actions

Fig. 2. Information security measurement program workflow

Prioritisation of cybersecurity controls – alternatives (1C of 5):

NIST Internal Report NIST IR 8286 (C): Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight, 2022


Enterprise Level (Level 1)
Organization Level (Level 2)
System Level (Level 3)
Enterprise Mission Goals and Obj.
Level 1 Executive defines risk appetite statements
Integrate into Enterprise Cybersecurity Risk Register
Level 1 / Level 2 leader defines risk tolerance statements
Level 2 Leader interprets risk appetite statements
Aggregate and Normalize Level 2 Cybersecurity Risk Registers
No
Apply mitigation or risk transfer
Yes
Can risk be brought within tolerance?
No
Does tolerance need refinement?
Yes
No
No
Interpret Risk Tolerance
Identify Risk Scenario
Assess Likelihood & Impact
Risk within tolerance?
Yes
Taking enough risk to realize value?
Yes
Update Cybersecurity Risk Register & POA&M

Note: Review enterprise risks and recommend adjustments to risk appetite statements.

Note: If tolerance statements are so risk averse that they stifle innovation or reduce technology value to the enterprise, L1/L2 leaders may refine them.

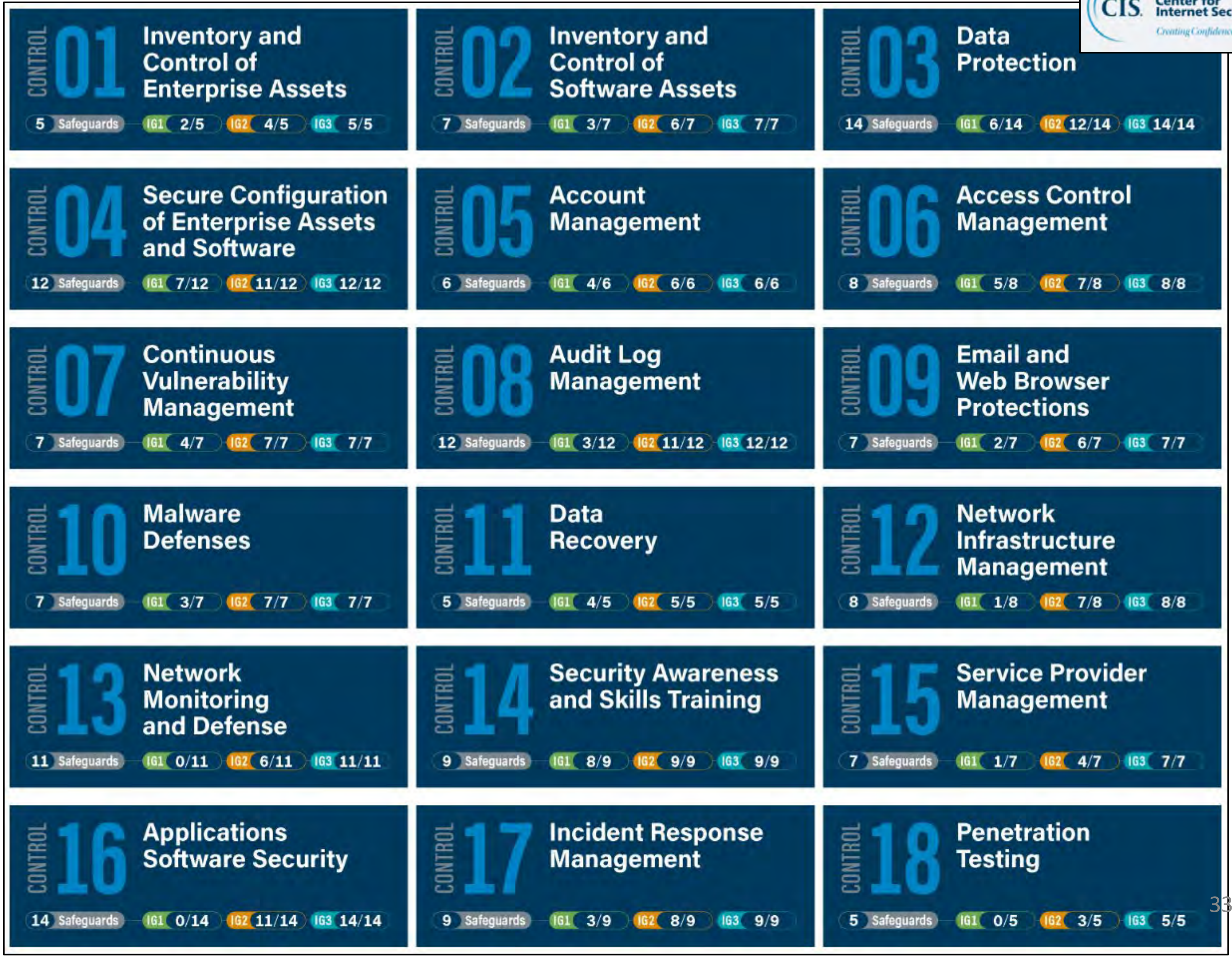
Note: If tolerance statements are found to be too stringent, L1/L2 leaders may refine them.

Figure 6: Continuous Interaction Between ERM and CSRM Using the Risk Register[12]

Prioritisation of cybersecurity controls – alternatives (2 of 5):

CIS Controls, V8, 2023

CIS. Center for Internet Security®
Creating Confidence in the Connected World.

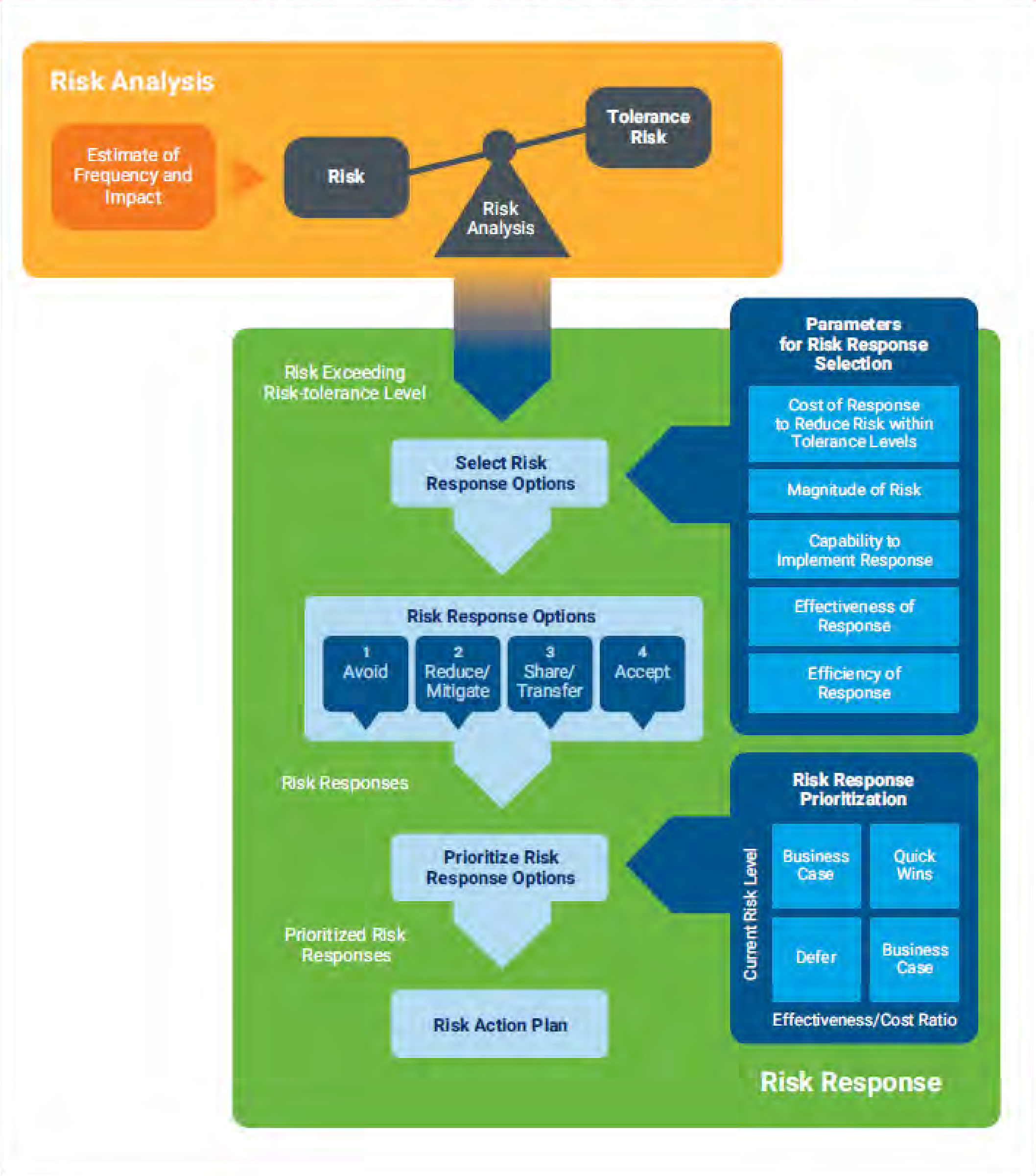


CONTROL		Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

Prioritisation of cybersecurity controls – alternatives (3 of 5):

ISACA's COBIT 2019 Risk IT Framework 2nd Edition, 2020

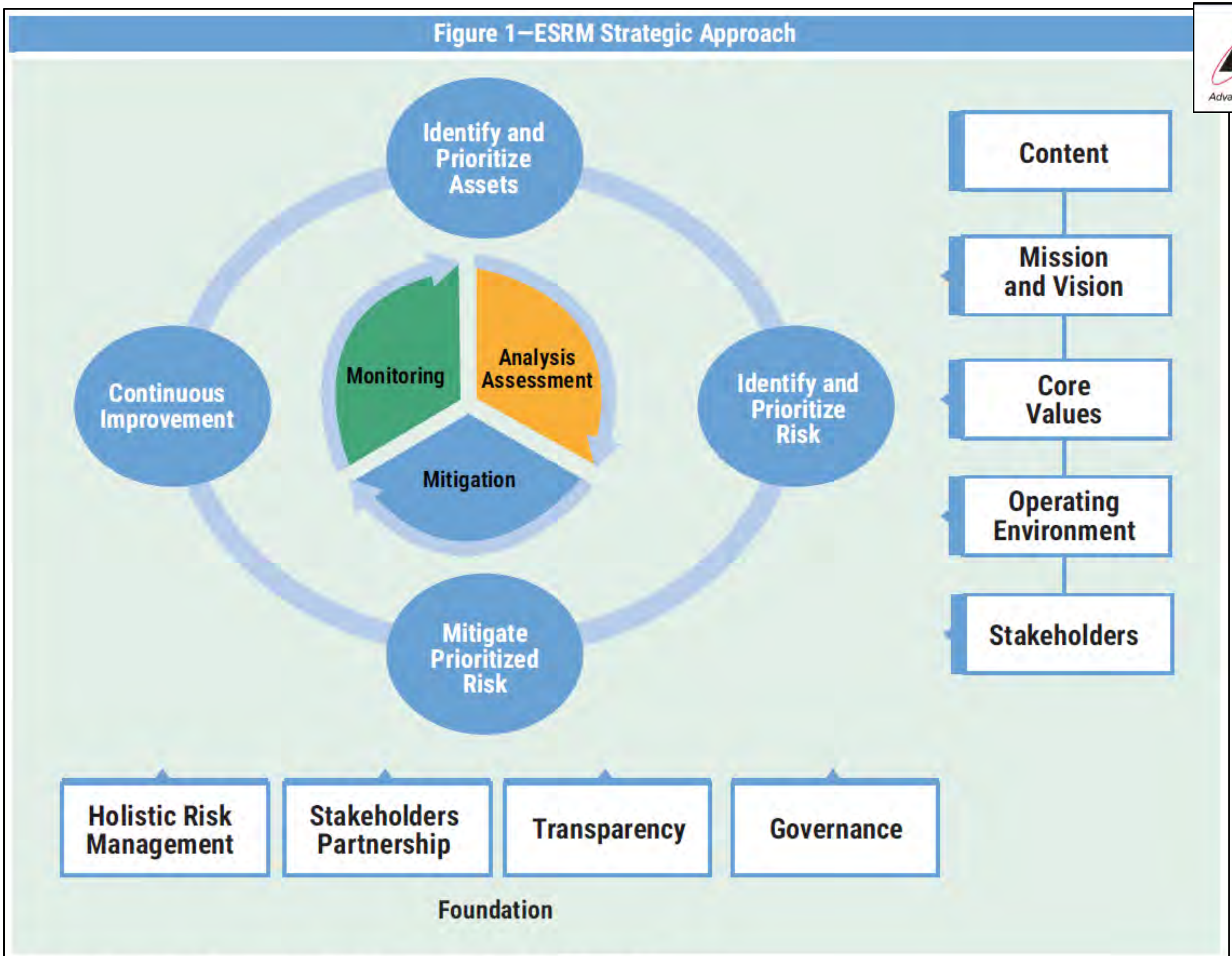
Figure 8.1—Risk Response Selection and Prioritization



Risk Analysis
Estimate of Frequency and Impact
Risk
Tolerance Risk
Risk Analysis
Risk Exceeding Risk-tolerance Level
Select Risk Response Options
Parameters for Risk Response Selection
Cost of Response to Reduce Risk within Tolerance Levels
Magnitude of Risk
Capability to Implement Response
Effectiveness of Response
Efficiency of Response
Risk Response Options
1 Avoid
2 Reduce/ Mitigate
3 Share/ Transfer
4 Accept
Risk Responses
Risk Response Prioritization
Current Risk Level
Business Case
Quick Wins
Defer
Business Case
Effectiveness/Cost Ratio
Prioritize Risk Response Options
Prioritized Risk Responses
Risk Action Plan
Risk Response

Prioritisation of cybersecurity controls – alternatives (4 of 5):

ASIS Enterprise Risk Security Management (ESRM), 2019



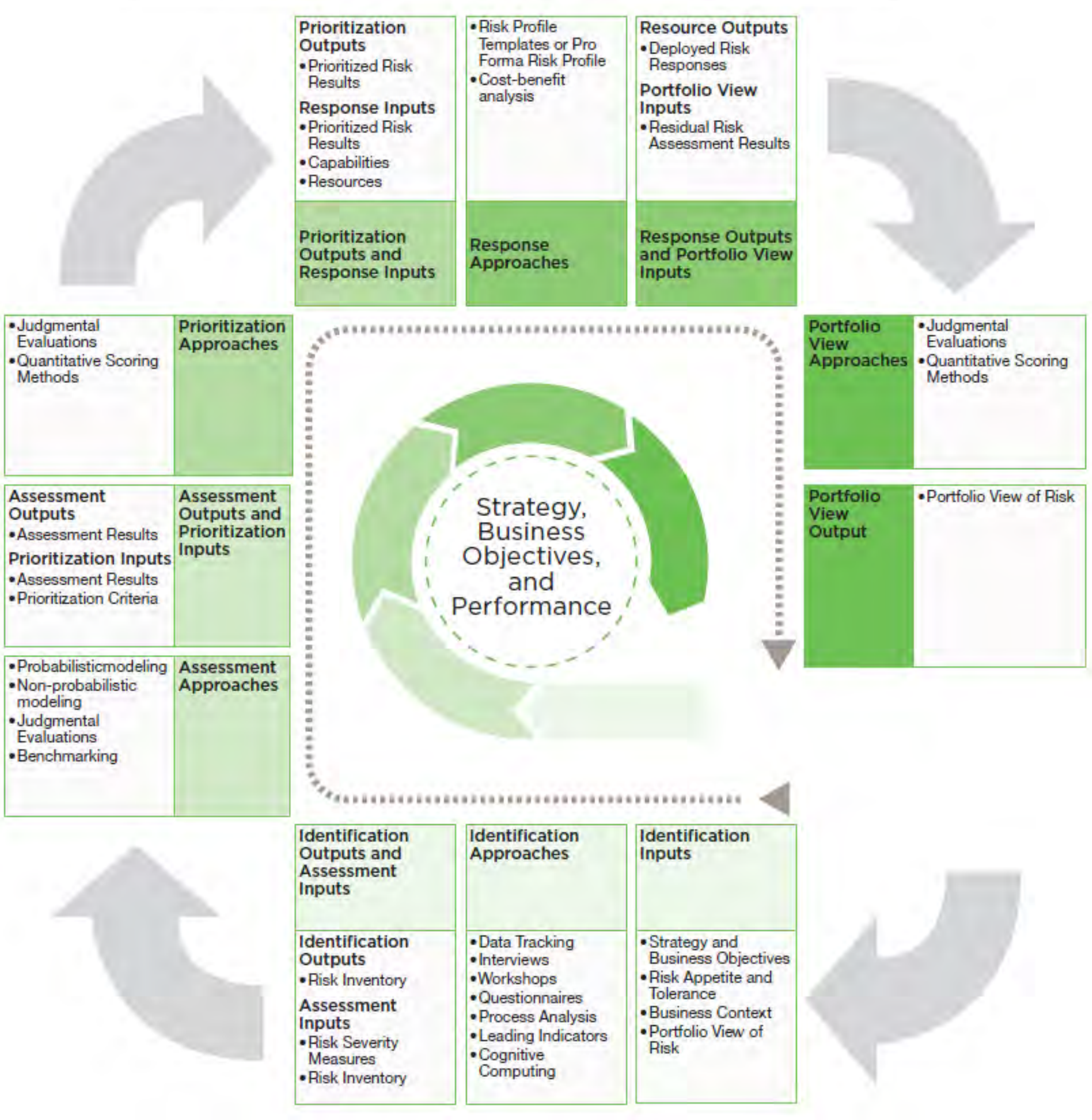
Source: ASIS International, Enterprise Security Risk Management Guideline, 2019. Used with permission.

Prioritisation of cybersecurity controls – alternatives (5 of 5):

COSO (Committee of Sponsoring Organizations of the Treadway Commission)
ERM (Enterprise Risk Management) – Integrating with Strategy and Performance – Principles Relating to Performance, 2017

COSO
COMMITTEE OF SPONSORING ORGANIZATIONS

Figure 8.1: Linking Risk Assessment Processes, Inputs, Approaches, and Outputs



Prioritization Outputs
- Prioritized Risk Results

Response Inputs
- Prioritized Risk Results
- Capabilities
- Resources

Prioritization Outputs and Response Inputs

- Risk Profile Templates or Pro Forma Risk Profile
- Cost-benefit analysis

Response Approaches

Resource Outputs
- Deployed Risk Responses

Portfolio View Inputs
- Residual Risk Assessment Results

Response Outputs and Portfolio View Inputs

Portfolio View Approaches
- Judgmental Evaluations
- Quantitative Scoring Methods

Portfolio View Output
- Portfolio View of Risk

Identification Inputs
- Strategy and Business Objectives
- Risk Appetite and Tolerance
- Business Context
- Portfolio View of Risk

Identification Approaches
- Data Tracking
- Interviews
- Workshops
- Questionnaires
- Process Analysis
- Leading Indicators
- Cognitive Computing

Identification Outputs and Assessment Inputs

Identification Outputs
- Risk Inventory

Assessment Inputs
- Risk Severity Measures
- Risk Inventory

Assessment Approaches
- Probabilisticmodeling
- Non-probabilistic modeling
- Judgmental Evaluations
- Benchmarking

Assessment Outputs and Prioritization Inputs

Assessment Outputs
- Assessment Results

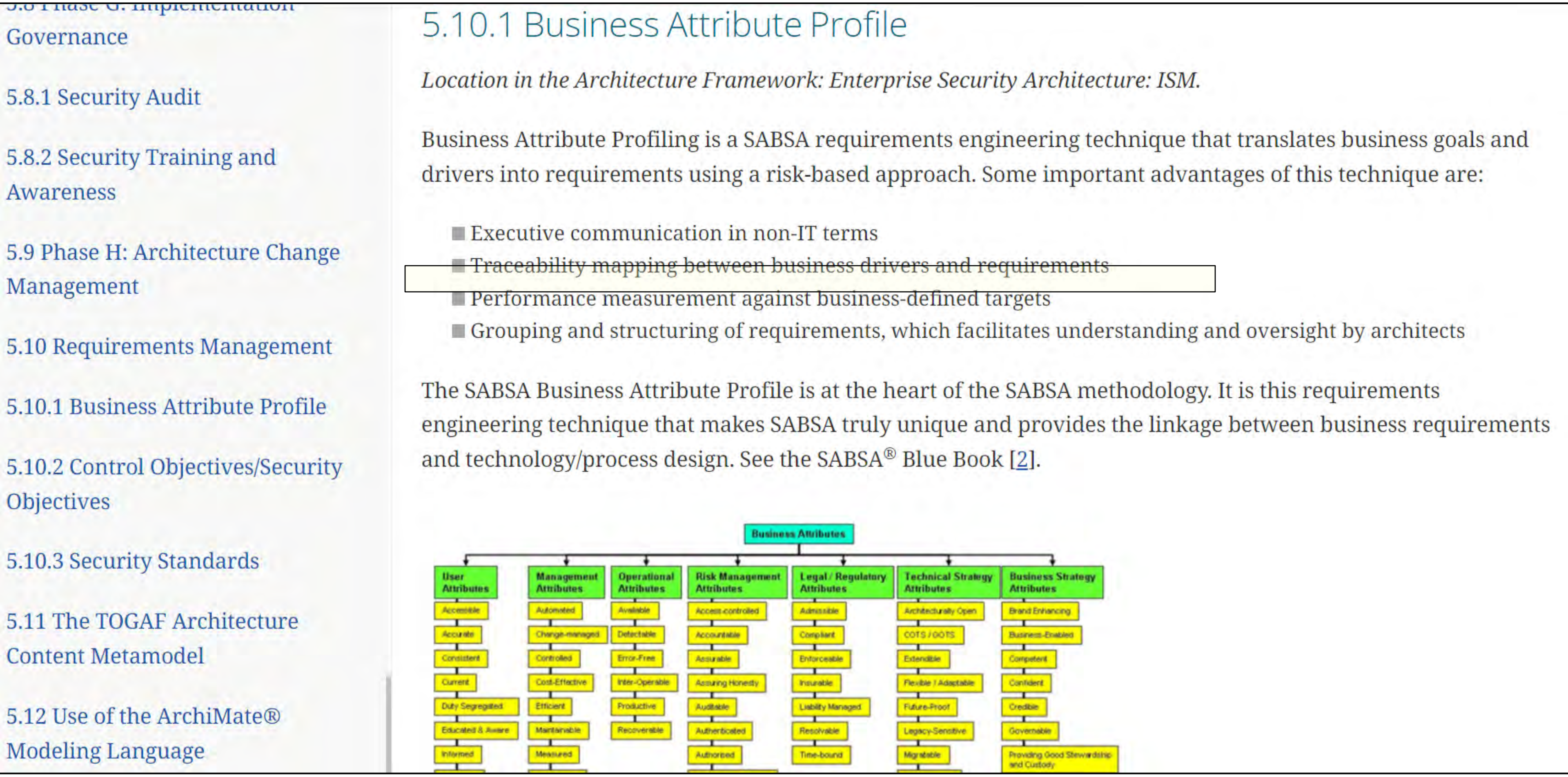
Prioritization Inputs
- Assessment Results
- Prioritization Criteria

Prioritization Approaches
- Judgmental Evaluations
- Quantitative Scoring Methods

Strategy, Business Objectives, and Performance

Prioritisation of cybersecurity controls – alternatives “+1”:

The Open Group Architecture Framework (TOGAF), 2022



5.10.1 Business Attribute Profile

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Business Attribute Profiling is a SABSA requirements engineering technique that translates business goals and drivers into requirements using a risk-based approach. Some important advantages of this technique are:

- Executive communication in non-IT terms
- Traceability mapping between business drivers and requirements
- Performance measurement against business-defined targets
- Grouping and structuring of requirements, which facilitates understanding and oversight by architects

The SABSA Business Attribute Profile is at the heart of the SABSA methodology. It is this requirements engineering technique that makes SABSA truly unique and provides the linkage between business requirements and technology/process design. See the SABSA® Blue Book [2].

Business Attributes

User Attributes	Management Attributes	Operational Attributes	Risk Management Attributes	Legal / Regulatory Attributes	Technical Strategy Attributes	Business Strategy Attributes
Accessible	Automated	Available	Access-controlled	Admissible	Architecturally Open	Brand Enhancing
Accurate	Change-managed	Detectable	Accountable	Compliant	COTS / GOTS	Business-Enabled
Consistent	Controlled	Error-Free	Assurable	Enforceable	Extendible	Competent
Current	Cost-Effective	Inter-Operable	Assuring Honesty	Insurable	Flexible / Adaptable	Confident
Duty Segregated	Efficient	Productive	Auditable	Liability Managed	Future-Proof	Credible
Educated & Aware	Maintainable	Recoverable	Authenticated	Resolvable	Legacy-Sensitive	Governable
Informed	Measured		Authorised	Time-bound	Migratable	Providing Good Stewardship and Custody

Summary,

Call to Action

SABSA: Summary

- Focus on highest priority information assets
- Focus on the most efficient portfolio of controls to reduce [R]
- Identify trade-offs for [I] vs. [R]
- Provides traceability, ∴ rationale for commitment of [I]
- Outside USA, used in many industries:
  - e.g. finance, government services, ICs, standards bodies
- Training emphasises SABSA in practice, theory also addressed
- A vibrant practitioner community exists, 2 annual conferences:
  - COSAC (COmputer Security And Controls) Ireland;
    e.g. 2023-10-02 to 2023-10-05
  - COSAC Asia-Pacific Melbourne;
    e.g. 2024-02-27 to 2024-02-29

SABSA: Call to Action

- COSAC community to reach out to NIST and HPC community ✓

- SABSA to be presented at SC23 conference ✓

- NIST and HPC folk to attend SABSA training ½

- NIST and HPC folk to participate in COSAC TBA

- NIST CSF 2.0 to recommend prioritisation ½

  TSI CSF 2.0 rec'n: **Governance – Assessment and Reporting**:

  > "A business impact analysis (BIA) identifying and prioritizing information systems and components and assessing criticality of assets and the risks to those business assets or systems in relation to identified key assets of the organization has been completed to guide the required protections."

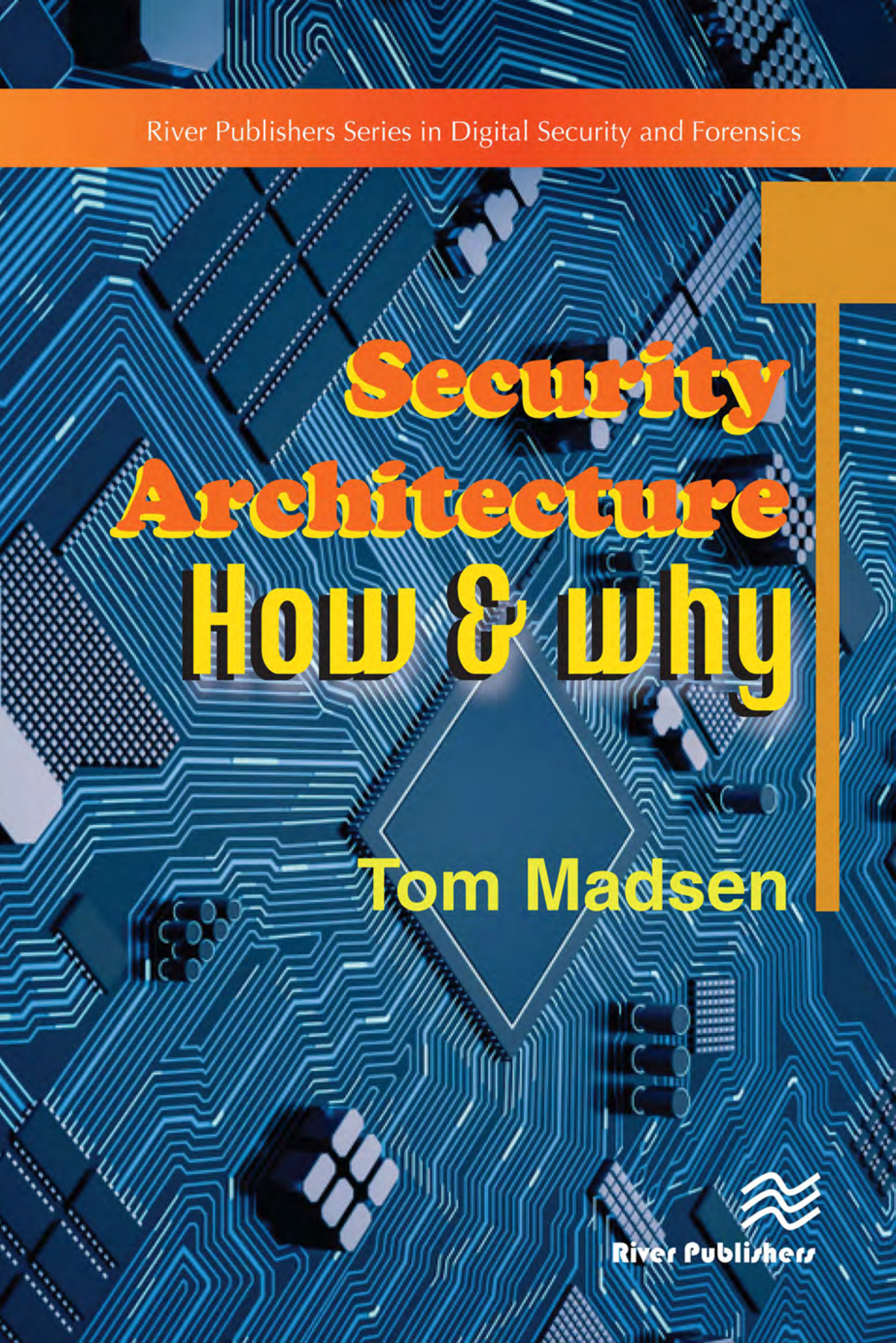
Questions,

Discussion

Appendix

Madsen: Security Architecture

River Publishers Series in Digital Security and Forensics



Security Architecture

How & why

Tom Madsen

River Publishers

Security Architecture – How & Why

RIVER PUBLISHERS SERIES IN DIGITAL SECURITY AND FORENSICS

The “River Publishers Series in Security and Digital Forensics” is a series of comprehensive academic and professional books which focus on the theory and applications of Cyber Security, including Data Security, Mobile and Network Security, Cryptography and Digital Forensics. Topics in Prevention and Threat Management are also included in the scope of the book series, as are general business Standards in this domain.

Books published in the series include research monographs, edited volumes, handbooks and textbooks. The books provide professionals, researchers, educators, and advanced students in the field with an invaluable insight into the latest research and developments.

Topics covered in the series include-

- Blockchain for secure transactions
- Cryptography
- Cyber Security
- Data and App Security
- Digital Forensics
- Hardware Security
- IoT Security
- Mobile Security
- Network Security
- Privacy
- Software Security
- Standardization
- Threat Management

For a list of other books in this series, visit www.riverpublishers.com

Security Architecture – How & Why

Tom Madsen

NNIT, Denmark

River Publishers

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Published 2022 by River Publishers
River Publishers
Alsbjergvej 10, 9260 Gistrup, Denmark
www.riverpublishers.com

Distributed exclusively by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
605 Third Avenue, New York, NY 10017, USA

Security Architecture – How & Why / by Tom Madsen.

Routledge is an imprint of the Taylor & Francis Group, an informa business

ISBN 978-87-7022-584-7 (print)
ISBN 978-10-0079-429-8 (online)
ISBN 978-1-003-33938-0 (ebook master)

While every effort is made to provide dependable information, the publisher, authors, and editors cannot be held responsible for any errors or omissions.

Contents

Preface

Security Architecture or Enterprise Information security architecture, as it was originally coined by Gartner back in 2006, has been applied to many things and different areas, making a concrete definition of Security architecture a difficult proposition. But having an architecture for the cyber security needs of an organization is important for many reasons, not least because having an architecture makes working with cyber security a much easier job since we can now build on a, hopefully, solid foundation. Developing security architecture is a daunting job, for almost anyone and in a company that has not had a cyber security program implemented before, the job becomes even harder. The benefits of having a concrete cyber security architecture in place cannot be overstated! The challenge here is that security architecture is not something that can stand alone, it absolutely must be aligned with the business in which is being implemented.

In this book, I hope to bring across to you the importance of and the benefits of, having security architecture in place. The book will be aligned with most of the sub frameworks in the general framework called SABSA or Sherwood Applied Business Security Architecture. SABSA is comprised of several individual frameworks and there are several certifications that you can take in SABSA, something I highly recommend if Security Architecture is something you would like to pursue as a career path. Aside from getting validation of your skills, SABSA as a framework is focusing on aligning the Security Architecture with the business and the business strategy. An important task in developing a security strategy! Each of the chapters in this book will be aligned with one or more of the components in SABSA, the components will be described as with the introduction to each of the chapters in this introduction.

I will be using examples throughout this book, to get my points across. These examples are based on technology from Microsoft and Cisco. This does not mean that I am recommending those vendors for your own architectures! These are just the vendors that I have chosen to specialize in, so that is the technology I am using with my own clients when consulting for clients in

Denmark. Denmark is a huge Microsoft and Cisco country; hence they are the vendors I am specializing in. Now, the chapter descriptions:

Chapter 1 – Why Security?
This chapter will help you make the argument to your business or organization, as to why having a security architecture in place is important as well as describe the benefits to the business, an important argument to make!

Chapter 2 – Why Architecture?
Here I will try to describe what architecture in this context is all about, especially how a formal architecture makes integration between systems and infrastructure-less complex and thus easier to secure in the architecture.

Chapter 3 – Security Architecture Model
This is the first chapter, where we dig into SABSA. Specifically, this chapter will detail the six sub frameworks that SABSA consists of and prepare you for the more detailed treatment in later chapters, of these subunits of SABSA.

Chapter 4 – Contextual Architecture
One of the core reasons for the effectiveness of SABSA is the business-oriented approach to security that is applied in this framework. This chapter will focus on how to align security architecture with the business needs and any regulations/compliance that needs to be considered as part of the architecture.

Chapter 5 – Conceptual Architecture
This is where we as security architects begin to add real value to an organization. Here we will begin the work of conceptualizing the solutions that will serve the business needs and make changes and adaptions later in the process much easier.

Chapter 6 – Logical Architecture
The logical part of the security architecture will follow naturally from the conceptual steps we did in the previous chapter. Now we will be looking into the functional and requirements and how these will fit into physical architecture steps in the next chapter.

Chapter 7 – Physical Architecture
Until now we have been looking at the more theoretical parts of SABSA, now the rubber meets the road with actual boxes of hardware and software. This is also the layer where we as architects look into the various data structures in use and the physical security requirements surrounding our architecture.

Chapter 8 – Component Architecture

This is the layer in the SABSA framework where the more specialized tools and components are located. This is also the chapter we I will be using examples from Microsoft and Cisco, to help you try and operationalize some of the more theoretical parts of this book.

Chapter 9 – Security Policy

Any security service, in security architecture, will need to be managed. How you go about this will contribute to the effectiveness of the service in the architecture as well as the overall effectiveness of the entire security architecture. Unfortunately, this is the step that is often overlooked or not taken seriously when implementing security architecture. In this chapter, I will give you some pointers and suggestions you can use in your own project.

Chapter 10 – Applied Security architecture with SABSA

This is where the rubber meets the road. In this chapter, I will walk you through some architecture examples using Cisco and Microsoft Azure. The examples will be based on a technology refresh of the entire networking infrastructure and migration of servers and applications to Microsoft Azure.

List of Figures

List of Tables

1

Why Security?

To understand ‘Security Architecture’ we must first make sure that you fully understand the meaning of security. It is a term that is used many times in many contexts and frequently with different meanings depending on the context.

In this chapter will provide you with a foundational understanding of security and how it fits in with Security Architecture.

1.1 Business Prevention

Cybersecurity has a bad reputation. If you, like me, have worked as an information system security professional in a business environment you know this only too well. When you walk into the room everyone groans. They say: ‘Here come the security guys again! They are going to give us even more passwords to remember, more rules to enforce and they will create even more difficulties in our lives that will prevent us from getting on with real business. Why don’t they just leave us alone’ ?

I have even heard someone refer to the IT security organization as the ‘business prevention’ department! It is not an entirely unfair reputation. Are we being misjudged and slandered by our colleagues? Well, if we are honest with ourselves, as a profession we probably deserve some of it. But the profession has certainly got that reputation because we collectively behaved like that and did not understand the business environment that our recommendations and mandates had to fit inside.

How did we get this reputation? What did we do wrong? As I see it, we did not necessarily do anything directly wrong at the time this reputation developed. But as mentioned before, cybersecurity fits into a larger whole, inside the organization or business, that we are working within and understanding this environment requires that the security individual understand this environment. Many cybersecurity professionals come from a technical background, without any business experience, something i am happy to see is slowly changing and business understanding is a core part of most of the educational efforts the schools and universities are offering on their cybersecurity programs.

1.2 Measuring and Prioritizing Business Risk

Security is used to protect assets with a value. If assets are in some way damaged or destroyed, then you will experience a business impact. The potential event by which you can suffer the damage or destruction is a threat, to prevent threats from crystallizing into a loss event that has a business impact, you use a protection or mitigation, measure to keep the threats away from your assets. If the assets are poorly protected, then you have a vulnerability to the threat. To improve the protection and reduce the vulnerability you introduce security controls, which can be either technical or procedural.

The process of identifying business assets, recognizing the threats, assessing the level of business impact that would be suffered if the threats were to materialize and analyzing the vulnerabilities, is known as a risk assessment and a risk assessment is not a one of exercise. Mature companies are conducting these kinds of assessments on a continuing basis and applying suitable controls to gain a balance between security, usability, cost and other business requirements as a part of their normal operations.

Risk assessment and risk mitigation jointly comprise what is often called operational risk management. Later chapters in this book examine operational risk management in much greater detail.

The main thing that you need to understand at this stage is that risk management is all about identifying and prioritizing the risks through the process and applying appropriate levels of control in line with those priorities.

Not all risks are worth the effort of implementing additional security and controls, either because the potential losses are not significant enough or because the costs of implementing the controls are higher than the value of the asset that is to be protected. What you get from a risk assessment is a set of business requirements for security, ranked in order of priority. These are most often expressed as a series of security and control objectives – abstract descriptions of business requirements for controls or mitigations. These in turn are used to drive the selection of risk mitigation approaches broad security and control strategies, logical security services, physical security mechanisms and finally the security products, tools and technology platforms with which you construct the Security Architecture.

Risk analysis comes in two forms, qualitative, where the risk assessments deliver a more subjective value of the various risks identified. A quantitative risk assessment delivers more concrete data values, that can be used by a company for prioritizing the efforts of protecting the various assets. These two forms are often used in conjunction with one another. The qualitative risk assessment provides the assessor with information on which risks might require a deeper analysis using quantitative methods, this is because using quantitative methods for all risks can be a massive investment in both time and money.

1.3 Security as a Business Enabler

The reputation that we, as information security professionals would like to have is quite different from the one that we have in many organizations. Although that is quickly changing, with the number of ransom ware attacks and data loss incidents we are seeing increases in frequency these years. Slowly but surely, this is changing to: Here come the security guys. They are going to help us to meet our business objectives and keep our data safe. Not the business prevention department, but the 'business enabling' department. But if we do our job properly and with due concern for the organization and the business environment that we are navigating within, we can make this happen. That is what our goal should be.

We must sell these information security ideas to our business colleagues and then make them come true. If we do not offer this sort of value to our business, then why are we there? There are several key technologies that are changing the way that business will be done in the future.

These include:

1. The Cloud
2. 5G mobile networking
3. Software-defined networking.
4. High bandwidth internet connections for the end-users
5. Wireless networking

The major change that we will see because of the deployment of these technologies is the continued migration of both the point of sale and the point of delivery right into the premises of the customer popularly known as the B2C (business-to-consumer) model.

People who want to buy something no longer need to make a physical visit to the vendor. They can use some of their communications technology to reach out from their home. They can browse through virtual shops, looking at virtual products on the virtual shelves. The products themselves may be picked automatically in the electronic warehouse, packed and sent to the customer with minimal human intervention. This same scenario applies to cases where business organizations. This is known as the B2B model. 'Supply chain management' and 'eProcurement' are among the most popular phrases used to describe the goals of business organizations when applying this model.

However, the number of threats, impacts and vulnerabilities that arise within all of these extremely complex systems is not to be trifled with. The major obstacle to the development of electronic business on such a huge scale is the low level of confidence that is inspired in the customer. Especially with the number of successful attacks we see increase these years.

Think of the business risks:

1. Disclosure of private, personal information,
2. Fraudulent buyers
3. Theft of credit card data
4. Errors and mistakes in such complex systems

So here is our opportunity to show how good we are. We have the whole world pleading for the security of information systems to enable them to do business and protect customer data. You have the technology to provide the solutions. What you must also demonstrate is that you have the associated skills to apply that technology to solve the problems facing the business.

You need much more than pure technology. You also need:

1. Good understanding of the business needs
2. Strategic architectures
3. Project management
4. Systems integration
5. Security management policies and practices
6. Enterprise-wide security culture and infrastructure

1.4 Empowering the Customers

We have looked at examples from the retail world of electronic commerce. In these cases, we see that electronic information systems are the means to empower the customer to gain greater benefits. These information systems, therefore, become important competitive factors for the suppliers, because the customers will use their power to select those suppliers who can meet the challenge of providing these benefits fastest and to the best price.

Information security is a critical component here, without it will be difficult for vendors to meet this customer service challenge. Customers will evaluate suppliers not only on the products themselves but also on how those products are marketed, sold and supported. Add to this the recent GDPR legislation from the EU, with this the customers are justifiably expecting us to protect their data as well. Losing customer data is a surefire way of ending up on the front pages of the newspapers and customers that see their data lost to the Internet are less likely to repeat business with us, making such losses life-threatening to a company!

Where online information systems are involved, that means that the quality, reliability, integrity and availability of those information services will be key factors in determining which suppliers succeed and which do not. Add to this confidentiality of the data we store on customers. To maintain that quality of service, one of the major tools you will need is an effective, risk-based information security program and a structured information systems security architecture, the very reason for this book!

1.5 Protecting Relationships

There is another security-related dimension to business relationships that we have not yet explored: the concept of trust. We shall return to this in detail later on in the book, but for now, let us take a quick glance at the subject.

When you do business with someone, at whatever level (personal or corporate), you are establishing some level of trust in the other party. You usually evaluate a number of signals that you receive, perhaps over some time, to determine how much you trust this person. How do they present themselves (Dress, Act, Personality?) Have they done business before? How did it go? How long has the company been established? Can you get a reference from someone else you know and trust (a trusted third party) – someone that already knows this person and can vouch for him or her? You know the drill!

Trust is an essential pre-requisite to doing business and trust is entirely a relationship thing. Trust is not created through IT systems but through some mutual knowledge between the parties. However, technical systems are used to protect the trust in the relationship that already exists. These technical services are no substitute for trust. They do not create trust. They merely protect the trust that already exists. However, indirect trust, through a third party (sometimes called transitive trust), is an important part of setting up digital business networks. It is obviously an advantage for both customers and suppliers to be empowered to do business with one another even though they have no previous knowledge of one another. This is where the third-party referee comes into the picture. The third-party needs to be trusted by both parties. This trusted third party is then able to play the role of 'introducer' by vouching for each of the two business parties to the other. This is usually achieved by the trusted third party issuing each entity with some certified credentials. This is called a digital certificate and is certified by a digital signature of a trusted third party. This is what we have been using for many years in the online space with digital certificates for the customer to be sure that the vendor they are interacting with is actually who they say they are.

It's like the situation where you go to a party at someone's house – someone who is an old friend of yours and with whom you have a long-standing trust relationship, built up through decades of experience and mutual interaction. At the party, another guest, someone who you have not met before, nor heard of, approaches you. It's quite different from meeting this person in a bar or on the street, where you might be very cautious and even suspicious of being approached by a stranger. The first thing you each ask one another is your name and how you know the host of the party. This establishes the credentials – 'Oh, I'm an old friend from college days' or 'I'm a work colleague'. It gives a new friendship a kick-start because you have established that you are both trusted by the host, who in this case acts as a trusted introducer for you both, giving both of you some confidence that it is alright to proceed with a friendship. You can begin to interact with a level of trust that would not be possible in the downtown bar. This is what a trusted third party is doing in the case of digital certificates. The third party is guaranteeing that the certificate can be trusted so we as consumers can trust the vendor exhibiting the certificate.

Many business deals are founded upon a personal introduction by a mutually trusted third party or by belonging to some business community that is in some way regulated by a trusted overseer.

So, when we build information systems, these technical systems can leverage the trust that already exists, whether directly or indirectly via the certificates, and they can protect those trusted business relationships in the course of doing business through this new information system-based medium.

1.6 To Summarize

Security is all about protecting business goals and assets. It means providing a set of controls that are matched to business needs and risk profiles, which in turn are derived from an assessment and analysis of business risks. The objective of risk assessment is to prioritize risks to focus on those that require mitigation.

Risk is a complex concept, and for any given course of action, there is a risk associated with doing that thing and risk associated with not doing it. Thus, one must take care not to mitigate a specific risk while unintentionally increasing the overall risk to the wider range of business goals and objectives. Something that is becoming increasingly more complex to do in an increasingly regulated world and the ever-increasing risk of a cyber-attack.

In its best possible light, security should be seen as enabling business by reducing risks to an acceptable level, thus allowing the business to make use of new technologies for greater commercial and information security advantage. Security can also be the means to add value to the core product by enabling information services that are essential to the enhancement of the product itself or to the operational support of the product out in the world, something I predict will become a business differentiator in the coming years.

Secure information services can empower the customers, enabling them to do business more easily and providing them with enhanced services that will have competitive value while ensuring that they trust in our efforts to protect them from harmful leaks of their data. Security in business information systems also protects and leverages the trust that exists between business partners, allowing them to establish relationships and to do business in new ways using new technologies. Technologies that might even open up new avenues of business for our organizations!

2
Why Architecture

This chapter explores what I mean by architecture. In particular, I will examine the differences between 'architecture' and, for lack of a better word, plumbing. Both of these areas provide great value to cybersecurity, but they are not the same thing. In the world of IT, people sometimes mix up which is which. In this chapter I will try to convey:

1. The concept of architecture is to integrate complex solutions to a diverse range of complex needs and to manage that complexity.
2. The layered approaches to architecture and the use of architectural reference models and frameworks.
3. The benefits of taking a strategic architectural approach as opposed to just applying solutions individually.

2.1 Origins of Architecture

Architecture originated in the building of towns and cities and everyone understands this meaning of the word, so it makes sense to me, to begin by examining the meaning of 'architecture' in this more traditional context. Architecture is a set of rules and conventions by which we create buildings that serve the purposes which they are intended for. An office building will look different from a residential home for instance. Our concept of architecture is one that supports ours needs to live, to work, to do business, to travel, to socialize and to pursue leisure activities. Architecture is founded upon understanding the needs that it must accommodate. These needs are expressed in terms of function, aesthetics, culture, government policies and regulations.

This all boils down to two major factors that determine what architecture we will create. These factors are:

1. The Purpose
2. Technological capabilities

2.2 Managing Complexity

One of the key functions of architecture as a product developed by the architect is to provide a framework and design within which complexity can be managed successfully. Small, isolated, individual projects do not need architecture, because their level of complexity is limited and the chief designer can manage the overall design. As the size and complexity of a project grow, however it becomes clear that more designers are needed, all working to create something that has the appearance of being designed by a single design authority. Also, if a project is not isolated in nature, but rather is intended to fit within a much larger and complex set of other projects, then architecture is needed to act as a road map which all these projects can be brought together into a more complete whole. The result must be as if they were all intended to be part of a single, large, project. This applies whether the various projects are designed and implemented simultaneously or if they are designed and implemented independently over an extended period. As complexity mented simultaneously or if they are designed and implemented independently over an extended period. As complexity increases, then a framework is needed and will benefit the overall project program, within which each designer can work, contributing to the overall design.

2.3 Information Systems Architecture

The whole idea behind architecture in buildings has been adapted to areas other than the building of towns and cities. In more recent times the idea has been adopted in the context of designing and building computer systems and so the concept of information systems architecture was been born. Just like conventional architecture defines the rules and standards for the design of buildings, information systems architecture addresses the same issues for the design and construction of computers, communications networks and the distributed business systems that are implemented using the various technologies available to us. As with the conventional architecture of buildings and cities, information systems architecture must therefore consider the goals that are to be achieved with the systems we are designing. The technical skills of the people to construct and operate the systems and their individual sub-systems.

If we accept this foundation, then we are already well on our way to recognizing that information systems architecture is concerned with much more than just technical factors. It is concerned with what the enterprise wants to achieve and the business environment that these systems will have to fit within. Technical factors are often the main ones that influence the architecture, how often have you heard the argument that we know Microsoft or Oracle, hence these technologies must be used, and under these conditions, the architecture can fail to deliver business expectations. This book is mainly concerned with the security of the business information systems, although I will be touching on other areas around this core subject. Hence the focus is on an enterprise security architecture, to emphasize that it is the enterprise and its activities that are to be secured and that the security of the underlying infrastructure is only part of this overall goal.

2.4 Architectures

Security Architecture encompasses much different architecture and is touched by much different architecture within the modern enterprise. Below I will be touching on a few of these architectures, but keep in mind that there is a plethora of literature that is covering these areas in much more detail! This literature should be on your to-do list for a firmer foundation in enterprise architecture.

2.4.1 Business Architecture

The business architecture describes an enterprise-wide perspective on how the business itself is structured into an organizational model and a set of processes, functions governance and the like. This is the primary architecture for all the below architecture types. The other sub-architectures are all created to support this one single overriding framework of how the business works.

2.4.2 Information Architecture

Any business around the world is represented by information. Every business relationship, every business process, every business transaction, everything about the business, is represented by information. Information is the more abstract representation of something real and tangible, like the product that a business might produce. So, information is important to a business, because the information is the business! The information is represented and stored in information systems and applications. The information architecture describes how the information is created, organized, processed, stored, retrieved and communicated. Information architecture describes information types and the relationships and organization, information behavior, information management processes and physical locations and repositories for information. It identifies and describes the major categories of information that are needed to support the business.

2.4.3 Applications Architecture

The applications are the, in our day and age, a vast amount of computer applications that are assisting the modern organization by carrying out actions on business information on behalf of the business. The applications architecture describes how applications are designed, how they integrate with one another and how they are supported within the business infrastructure environment (hardware, software and communications networks). The applications must relate to the business processes that they support and the information resources that they create, maintain and the process by adhering to the information architecture above. Characteristics of modern applications architecture are likely to be: Cloud-based, Web API's, micro services and reusable, generic modules and hence quickly adaptable to new business needs; Built on a strategic ERP system or the like, offering distributed processing via the cloud. The main objective of applications architecture is to enable and automate business processes.

2.4.4 Infrastructure Architecture

The applications are running on both virtual and physical infrastructure. Infrastructure has been the area of focus for many years, regarding cyber security and it is an integral part of the Security Architecture as well. We will be returning to this in later chapters, but for now, it is defined as including: The computer platforms (hardware and operating systems); The computer networks (cables, lines, switches, routers, etc.); The layer of software that bridges between infrastructures that have different physical characteristics. This is commonly known as middleware and is becoming increasingly important with the steady increase in cloud deployments.

2.4.5 Risk Management Architecture

Risk Management Architecture is a concept that is crossing all the previous kinds of architecture. The model represented here is more a business model and not quite a systems model, although systems are a core ingredient in any kind of risk architecture. It is essential to see risk management as an activity that happens within all the layers and again, the risk is an excellent tool for communication with the business! This risk management architecture is close to the concept of Security Architecture, but it is not quite the same. I will return to the concept of risk management in several of the later chapters.

2.4.6 Governance Architecture

Surrounding all other components just mentioned is the all-important piece labeled Management and Governance Architecture. Governance is one of the things that I, personally, think will only become more important in the coming years. Good governance, whether it is IT governance or corporate governance, will become a differentiator for companies to show responsibility to both governments and customers, with all of the corporate scandals we have seen in recent years. The representation of this as an all-encompassing component of security architecture is important. It is through this framework that the senior management controls the business, manages risk and governs how the business uses information, applications and infrastructure. The management and governance architecture describes the decision-making processes and levels of authority that are assigned to decision-making entities (individuals or committees).

2.5 Enterprise Security Architecture

It is the common experience of many organizations that information security solutions are often designed, acquired and installed on a tactical basis without further thought to how this solution will fit within the already existing infrastructure and business environment. A requirement is identified, a use case is written and a solution is sought to meet the identified need. In this process, there is no opportunity to consider a more strategic dimension and the result is that the organization builds up a mix of various technical solutions on an ad hoc basis without integration between the components or the costs involved in operating a disparate set of security solutions.

2.5 Enterprise Security Architecture

It is the common experience of many organizations that information security solutions are often designed, acquired and installed on a tactical basis without further thought to how this solution will fit within the already existing infrastructure and business environment. A requirement is identified, a use case is written and a solution is sought to meet the identified need. In this process, there is no opportunity to consider a more strategic dimension and the result is that the organization builds up a mix of various technical solutions on an ad hoc basis without integration between the components or the costs involved in operating a disparate set of security solutions.

Those enterprises that suffer these problems are often aware of these issues, but struggle to find an approach that will make things better. Good architecture never happens by accident and so the enterprise must find skills, methods and tools that help it to succeed with a more strategic architectural approach. One approach that avoids these problems is the development of an enterprise security architecture that is business-driven and describes a structured relationship between the technical and procedural solutions that supports the long-term needs of the business or organization. If the architecture is to be successful, then it must provide a framework within which decisions can be made on the selection of security solutions. These decision criteria absolutely must be derived from a thorough understanding of the business requirements, including the need for cost reduction, modularity, scalability, ease of re-use, operability, usability, inter-operability both internally and externally and integration with the enterprise ICT architecture and its legacy systems. Note the cost reduction part of the previous sentence, there is money to be saved here! Maybe not on the immediate implementation, but the long-term costs of the security solutions will be vastly decreased.

Furthermore, information system security is only a small part of information security, which in turn is just one part of a larger topic: business assurance. Business assurance consists of three major areas: information security; business continuity; physical and environmental security. Only through an integrated approach to these aspects of business assurance will it be possible for the enterprise to make the most cost-effective and beneficial decisions regarding the management of the various risks that any business or organization is facing daily. The enterprise security architecture and the security management process must therefore embrace all these areas. This brings us, finally, to SABSA.

2 SABSA® is a registered trademark of SABSA Limited. It stands for: Sherwood Applied Business Security Architecture

This book is a description of the SABSA® model and its applications. The model itself is described in much greater detail in Chapter 3. The primary characteristic of this model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities might be developed and exploited. The model is layered, an enabling function through which new business opportunities might be developed and exploited. The model is layered, with the top layer being the business requirements definition stage. At each of the lower layers, a new level of abstraction is developed, going through the definition of the conceptual architecture, logical architecture, physical architecture and finally at the lowest layer, the selection of technologies and products – or the shopping list.

The model itself is generic and can be the starting point for any kind of organization or business, by going through the process of analysis and decision-making implied by its structure, the output becomes specific to the enterprise and is at the end of the process customized to a unique business model. The output from applying the model becomes the enterprise security architecture and is central to the success of a strategic program of information security management within the organization.

2.6 Being a Successful Security Architect

Unless the security architecture can address a wide range of operational requirements and provide real business support and business enablement, rather than just focusing upon security, then it is likely that it will fail to deliver what the business expects and needs.

This type of failure is a common enough case throughout the information systems industry, not just within information systems security. In this book, I will put an enormous amount of emphasis on the need to avoid this mistake by keeping in mind the real needs of the business. It is not enough to compile a set of business requirements, document them and put them on the shelf, and then proceed to design a security architecture based on whatever technology the business is most familiar with. Being a successful security architect means thinking in business terms, even when you get down to the real detail and nuts and bolts of the construction. You always need to have in mind the questions:

1. Why are we doing this?
2. What are we trying to achieve in business terms here?

It will also be difficult to battle against the numerous other people around you who do not understand strategic architecture and who think that it is all to do with technology. These people will constantly challenge you, attack you and ridicule you. You must be ready to deal with this.

You have to realize that being a successful architect is also about being a successful communicator/negotiator who can sell the ideas and the benefits to others in the enterprise that need to be educated about these issues. One of the most important factors for success is to have buy-in and sponsorship from senior management within the enterprise. Enterprise architecture cannot be achieved unless the most senior decision-makers are on your side.

Creating this environment of acceptance and support is probably one of the most difficult tasks that you will face in the early stages of your work.

2.7 Security Architecture Needs a Holistic Approach

Many people make the mistake of believing that building security into information systems is simply a matter of referring to a checklist of technical and procedural controls and applying the appropriate security measures said list. However, security has an important property that most people know about, but few pay any attention to. The security consists of many layers, or links in a chain, the chain is only as strong as the weakest link and an attacker will always go for this weakest link.

The checklist approach also fails because many people focus on checking that the links in the chain exist but do not necessarily that the links fit together to form a secure chain. The chain is a reasonably good analogy, but the problem is much worse. Imagine a checklist that has the following items: engine block, pistons, piston rings, piston rods, bearings, valves, camshaft, wheels, chassis, body, seats, steering wheel, gearbox, etc. Suppose that this list comprehensively itemizes every single component that would be needed to build a car or motorcycle. If you go through the checklist and make sure that you have all these components, does it mean that you have a car? Not even close!

Some of the key questions not addressed by the checklist approach to car construction are:

1. Can you be sure that all the parts have been designed to work together as one smoothly running system?
2. Do you have any assurance that the car has been properly assembled?
3. Has the engine been tuned?
4. Is the system running smoothly at this moment?

Checklists are never the entire answer. Security architecture, as with all other forms of architecture, needs a holistic approach, I know, another buzzword, but stay whit me:

1. Do you understand the requirements?
2. Do you have all the components?
3. Do these components work together?
4. Do they form an integrated system?

Security Architecture
How & why

Tom Madsen

Security Architecture, or Enterprise Information security architecture, as it was originally coined by Gartner back in 2006, has been applied to many things and different areas, making a concrete definition of security architecture a difficult proposition. But having an architecture for the cyber security needs of an organization is important for many reasons, not least because having an architecture makes working with cyber security a much easier job, since we can now build on a, hopefully, solid foundation. Developing a security architecture is a daunting job for almost anyone, and in a company that has not had a cyber security program implemented before, the job becomes even harder. The benefits of having a concrete cyber security architecture in place cannot be overstated! The challenge here is that a security architecture is not something that can stand alone, it absolutely must be aligned with the business in which it is being implemented.

This book emphasizes the importance, and the benefits, of having a security architecture in place. The book will be aligned with most of the sub-frameworks in the general framework called SABSA, or Sherwood Applied Business Security Architecture. SABSA is comprised of several individual frameworks and there are several certifications that you can take in SABSA. Aside from getting a validation of your skills, SABSA as a framework focuses on aligning the Security Architecture with the business and its strategy. Each of the chapters in this book will be aligned with one or more of the components in SABSA, the components will be described along with the introduction to each of the chapters.

Exclusively Distributed by

Routledge
Taylor & Francis Group
www.routledge.com
an informa business

River Publishers

ISBN 978 87 7022-584-7

9 788770 225847