

Identifying Security Requirements

Using SABSA Attributes Profiling



Andrew Stephen
andrew@plinth.co.nz

Agenda

The Problem

What's the Solution?

SABSA Overview

The SABSA Process

Defining the Attributes Profile

Using the Attributes Profile

The Problem

“So, what are your security requirements?”



Perceptions of Security



Perceptions of Security?

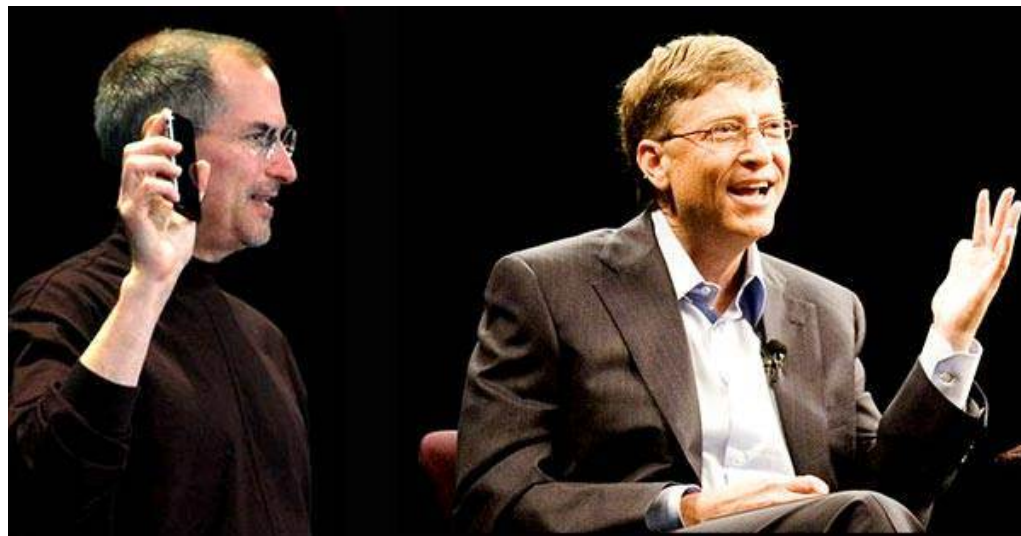


The Solution?

How do we get from this...



...To this?



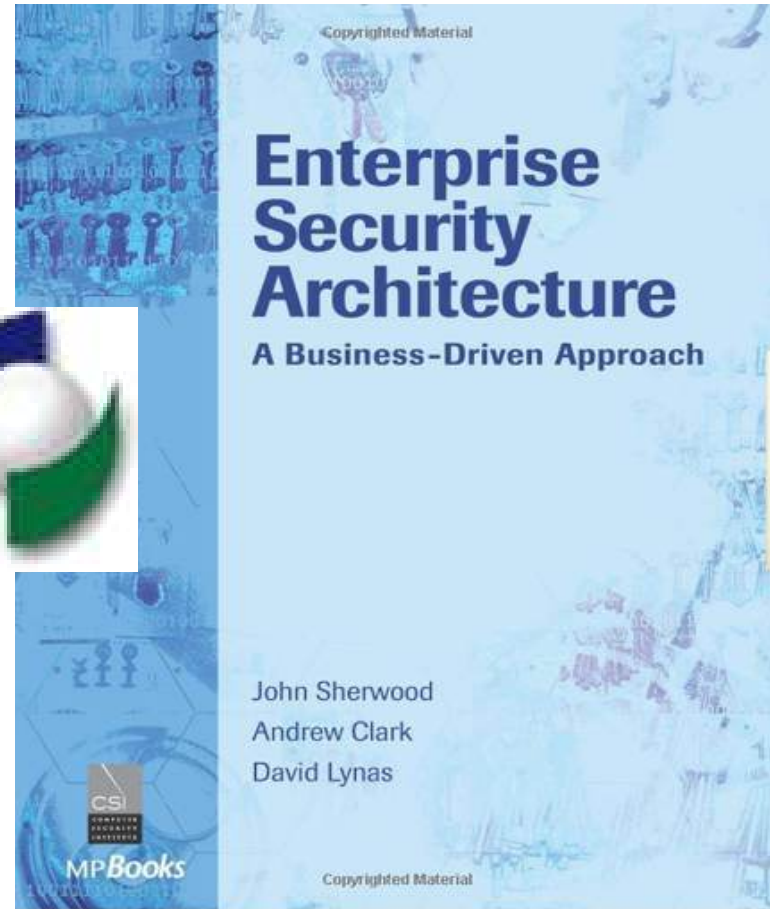
The Solution?



Many standards and frameworks

Enterprise Security Architecture

SABSA®



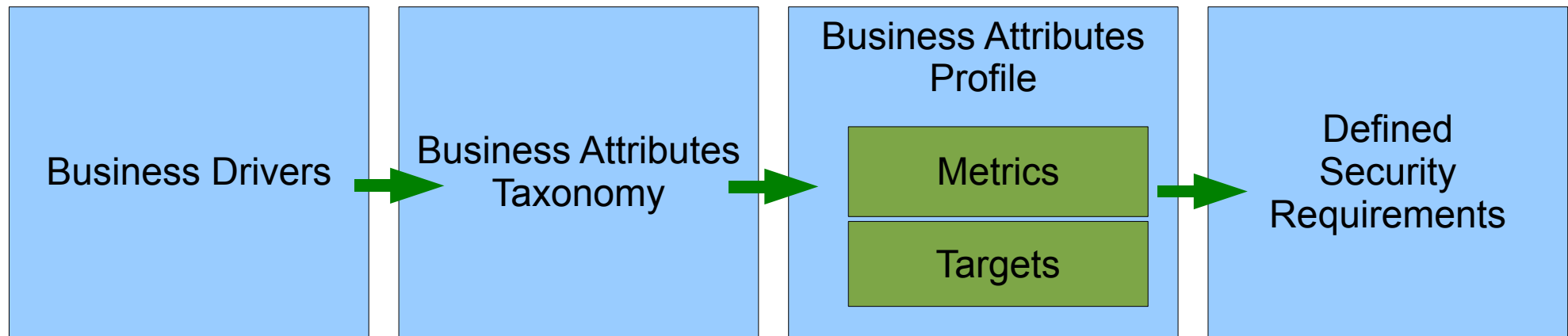
What Is The Matrix?

	Assets	Motivation	Process	People	Location	Time
	(What)	(Why)	(How)	(Who)	(Where)	(When)
Contextual (Business View)	The Business	Business Risk Model	Business Process Model	Business Organisation & Relationships	Business Geography	Business Time Dependencies
Conceptual (Architect's View)	Business Attributes Profile	Control Objectives	Security Strategies & Architectural Layering	Security Entity Model & Trust Framework	Security Domain Model	Security Related Lifetimes & Timelines
Logical (Designer's View)	Business Information Model	Security Policies	Security Services	Entity Schema & Privilege Profiles	Security Domain Definitions & Associations	Security Processing Cycle
Physical (Builder's View)	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications & User Interfaces	Platform & Network Infrastructure	Control Structure Execution
Component (Tradesman's View)	Detailed Data Structures	Security Standards	Security Products & Tools	Identities, Functions, Actions, ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing & Sequencing
Operational (Facilities Manager's View)	Assurance of Operational Continuity	Operational Risk Management	Security Service Management & Support	Application & User Management & Support	Security of Sites, Networks & Platforms	Security Operations Schedule

What Is The Matrix?

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual (Business View)	The Business	Business Risk Model	Business Process Model	Business Organisation & Relationships	Business Geography	Business Time Dependencies
Conceptual (Architect's View)	Business Attributes Profile	Control Objectives	Security Strategies & Architectural Layering	Security Entity Model & Trust Framework	Security Domain Model	Security Related Lifetimes & Timelines
Logical (Designer's View)	Business Information Model	Security Policies	Security Services	Entity Schema & Privilege Profiles	Security Domain Definitions & Associations	Security Processing Cycle
Physical (Builder's View)	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications & User Interfaces	Platform & Network Infrastructure	Control Structure Execution
Component (Tradesman's View)	Detailed Data Structures	Security Standards	Security Products & Tools	Identities, Functions, Actions, ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing & Sequencing
Operational (Facilities Manager's View)	Assurance of Operational Continuity	Operational Risk Management	Security Service Management & Support	Application & User Management & Support	Security of Sites, Networks & Platforms	Security Operations Schedule

The SABSA Process



“We rely on our reputation with customers, partners and suppliers.”

Reliable
Integrity-Assured
Private

Integrity-Assured

- Measure: Reporting of all incidents of integrity compromise
- Target: No successful compromise

Must implement integrity and validity controls.

Only one place to get these...



Business Attributes Taxonomy

User	Management	Operational	Risk Management	Legal/ Regulatory	Technical Strategy	Business Strategy
Accessible	Automated	Available	Access-controlled	Admissible	Architecturally Open	Brand Enhancing
Accurate	Change Managed	Detectable	Accountable	Compliant	COTS / GOTS	Business Enabled
Anonymous	Controlled	Error-Free	Assurable	Enforceable	Extendible	Competent
Consistent	Cost-Effective	Interoperable	Assuring Honesty	Insurable	Flexible / Adaptable	Confident
Current	Efficient	Productive	Auditable	Liability Managed	Future-Proof	Credible
Duty Segregated	Maintainable	Recoverable	Authenticated	Resolvable	Legacy Sensitive	Governable
Educated and Aware	Measured		Authorised	Legal	Migratable	Providing Good Stewardship and Custody
Informed	Supportable		Capturing New Risks	Regulated	Multi-sourced	Providing Investment Re-use
Motivated	Continuous		Confidential	Time-Bound	Scalable	Reputable
Protected	Monitored		Crime-Free		Simple	Culture Sensitive



User	Management	Operational
-------------	-------------------	--------------------

Risk Management	Legal/Regulatory	Technical Strategy	Business Strategy
------------------------	-------------------------	---------------------------	--------------------------

User Attributes	Description
Accessible	Information to which the user is entitled to gain access should be easily found and accessed by that user.
Accurate	The information provided to users should be accurate within a range that has been pre-agreed as being applicable to the service being delivered.
Anonymous	For certain specialised types of service the anonymity of the user should be protected.
Consistent	The way in which login, navigation and target services are presented to the user should be consistent across different times, locations and channels of access.
...	...
Usable	The system should provide easy to use interfaces that can be navigated intuitively by a user of average intelligence and training level (for a particular system). The user's experience of these interactions should be at best interesting and at worst neutral.

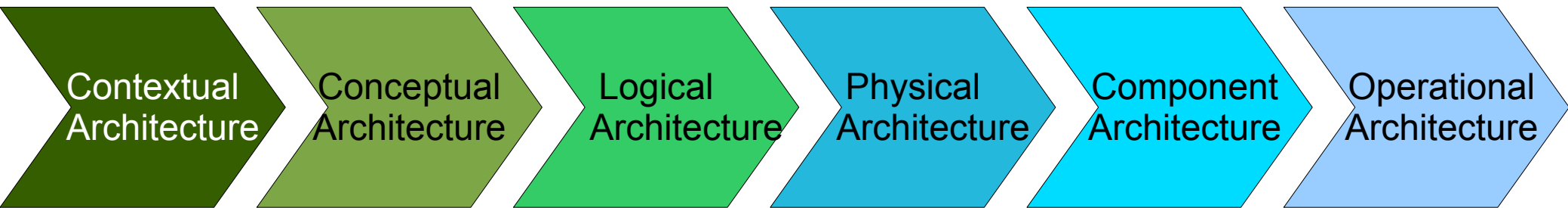
Measures & Targets Defined

User Attributes	Description	Metric type	Measurement
Accessible	Information to which the user is entitled to gain access should be easily found and accessed by that user.	Soft	Search tree depth necessary to find information Target: < 3
Accurate	The information provided to users should be accurate within a range that has been pre-agreed as being applicable to the service being delivered.	Hard	Acceptance testing on key data to demonstrate compliance with design rules. Target: No exceptions

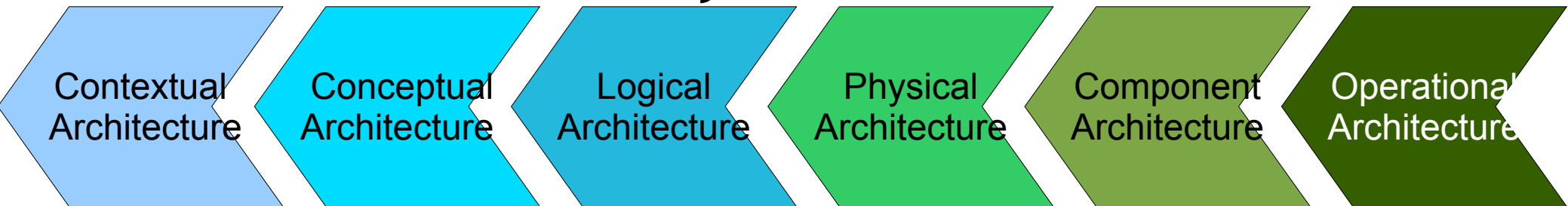
This is now a Business Attributes Profile

Practical Use: Traceability

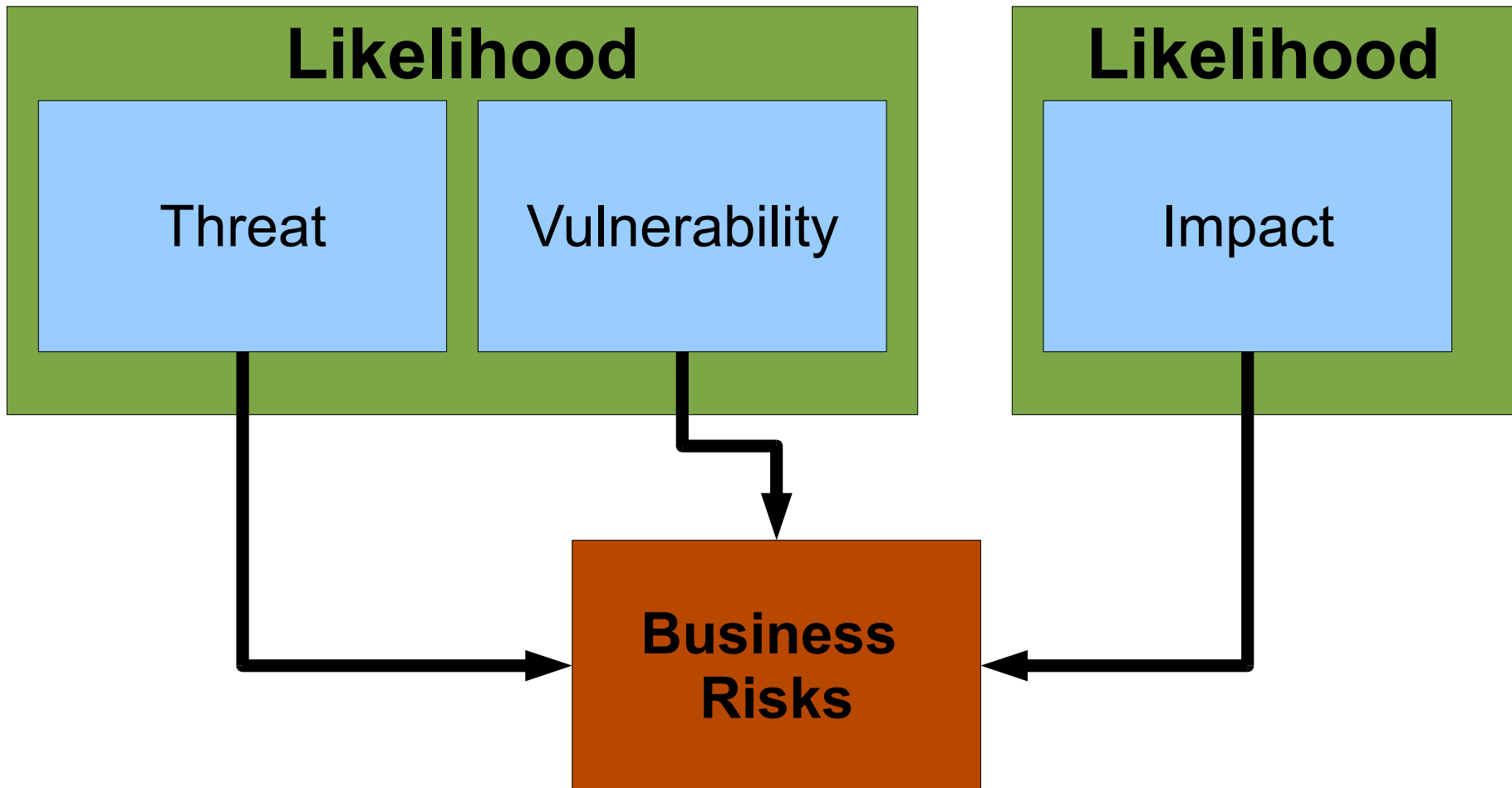
Traceability for Completeness



Traceability for Justification



Practical Use: Risk Assessment



Practical Use: Risk Assessment

User	Management	Operational	Risk Management	Legal/ Regulatory	Technical Strategy	Business Strategy
Accessible	Automated	Available	Access-controlled	Admissible	Architecturally Open	Brand Enhancing
Accurate	Change Managed	Detectable	Accountable	Compliant	COTS / GOTS	Business Enabled
Anonymous	Controlled	Error-Free	Assurable	Enforceable	Extendible	Competent
Consistent	Cost-Effective	Interoperable	Assuring Honesty	Insurable	Flexible / Adaptable	Confident
Current	Efficient	Productive	Auditable	Liability Mitigable	Immutable	Compliant
Duty Segregated	Maintainable	Recoverable	Authenticated	Resilient	Reversible	Reliable
Educated and Aware	Measured		Authorised	Legal	Imigratable	Providing Good Stewardship and Custody
Informed	Supported		Reviewed	Regulated	Multi-sourced	Providing Investment Re-use
Motivated	Controlled			Time-Bound	Scalable	Reputable
Protected	Monitored		Crime-Free		Simple	Culture Sensitive

Low Business Impact

High Business Impact

Use: Solution Evaluation Product A

User	Management	Operational	Risk Management	Legal/ Regulatory	Technical Strategy	Business Strategy
Accessible	Automated	Available	Access-controlled	Admissible	Architecturally Open	Brand Enhancing
Accurate	Change Managed	Detectable	Accountable	Compliant	COTS / GOTS	Business Enabled
Anonymous	Controlled	Error-Free	Assurable	Enforceable	Extendible	Competent
Consistent	Cost-Effective	Interoperable	Assuring Honesty	Insurable	Flexible / Adaptable	Confident
Current	Efficient	Productive	Auditable	Liability Managed	Future-Proof	Credible
Duty Segregated	Maintainable	Recoverable	Authenticated	Resolvable	Legacy Sensitive	Governable
Educated and Aware	Measured		Authorised	Legal	Migratable	Providing Good Stewardship and Custody
Informed	Supportable		Capturing New Risks	Regulated	Multi-sourced	Providing Investment Re-use
Motivated	Continuous		Confidential	Time-Bound	Scalable	Reputable
Protected	Monitored		Crime-Free		Simple	Culture Sensitive

Use: Solution Evaluation Product B

User	Management	Operational	Risk Management	Legal/ Regulatory	Technical Strategy	Business Strategy
Accessible	Automated	Available	Access-controlled	Admissible	Architecturally Open	Brand Enhancing
Accurate	Change Managed	Detectable	Accountable	Compliant	COTS / GOTS	Business Enabled
Anonymous	Controlled	Error-Free	Assurable	Enforceable	Extendible	Competent
Consistent	Cost-Effective	Interoperable	Assuring Honesty	Insurable	Flexible / Adaptable	Confident
Current	Efficient	Productive	Auditable	Liability Managed	Future-Proof	Credible
Duty Segregated	Maintainable	Recoverable	Authenticated	Resolvable	Legacy Sensitive	Governable
Educated and Aware	Measured		Authorised	Legal	Migratable	Providing Good Stewardship and Custody
Informed	Supportable		Capturing New Risks	Regulated	Multi-sourced	Providing Investment Re-use
Motivated	Continuous		Confidential	Time-Bound	Scalable	Reputable
Protected	Monitored		Crime-Free		Simple	Culture Sensitive

Summary

SABSA®



Developed from practical experience, around the same time as Zachman.

Fits well with other frameworks and standards, e.g. COBIT

Enterprise Security Architecture

Evolving

Summary

Business Attributes Profile

Business Drivers

Common Language

Measures & Targets

Many Practical Uses Beyond Requirements

References

SABSA Institute

<http://www.sabsa-institute.org/>

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books

ALC Training

<http://www.alctraining.co.nz/>

Andrew Stephen
Plinth Consulting
andrew@plinth.co.nz