
SABSA


SABSA
Sherwood Applied Business Security Architecture

SABSA

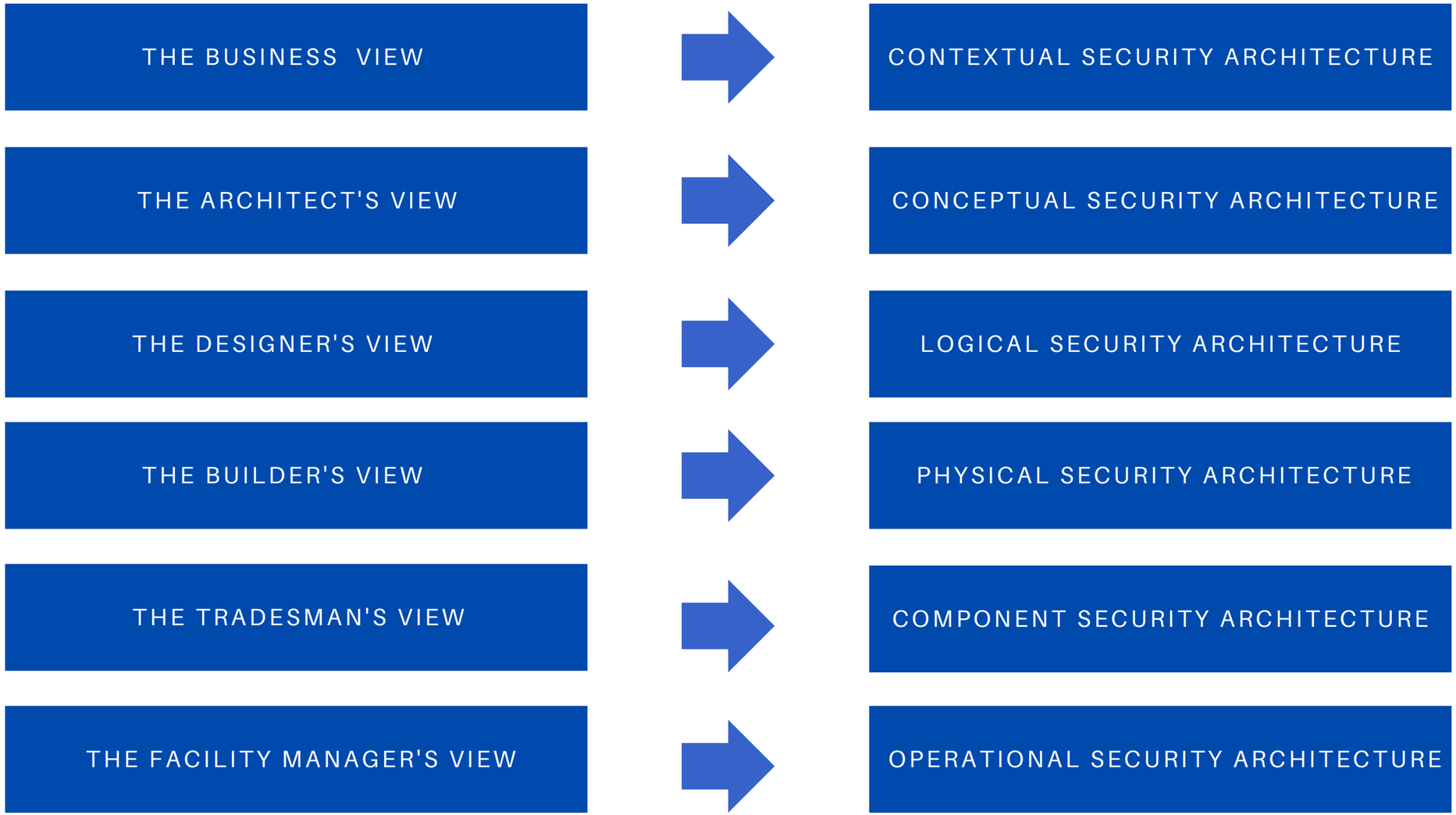
Framework and methodology for developing and documenting business and risk driven enterprise security and security solutions architectures.

SABSA

First released in October 1996 and adopted in over 50 countries to meet diverse needs under

- Risk Management
- Information Assurance
- Governance
- Continuity Management

SABSA Structure



SABSA: Six Questions

Each layer is analyzed by asking the following questions at each layer:

- What assets need to be protected?
- Why is protection needed?
- How will protection be achieved?
- Who will ensure the protection of the assets?
- Where is protection needed?
- When is protection needed?

SABSA: Business View

Developing security architectures must always begin from a business perspective

- WHAT: Business drivers for securing the system being built
- WHY: Business risks that need to be addressed
- HOW: Business processes that need security
- WHO: Business organizations that will take part in security
- WHERE: Business locations where security is needed
- WHEN: Time dependencies of business processes

The answers will enable the development of the contextual security architecture

SABSA: Architect's View

Conceptualizing solutions that will meet the security needs of the business

- WHAT: Desired protection in terms of business attribute profile
- WHY: Rationale behind the desired protection in terms of control objectives
- HOW: Method for achieving desired protection in terms of high-level security strategies
- WHO: Players involved in security management
- WHERE: Relevant security domains where protection must be achieved
- WHEN: Time-related aspects of security

The answers will enable the development of the conceptual security architecture.

SABSA: Designer's View

Translating the architect's conceptual design into a logical system design.

- WHAT: Business information that needs to be protected
- WHY: Security policy requirements
- HOW: Logical security services needed to protect the business information
- WHO: Users that will interact with business information
- WHERE: Relevant security domains where protection must be achieved
- WHEN: Security processing life cycle

These answers will enable the development of the logical security architecture

SABSA: Builder's View

Translating the designer's logical design into an actual physical system design

- WHAT: Business information that needs to be protected
- WHY: Rules, practices and procedures
- HOW: Security mechanisms and controls needed to protect business data
- WHO: Users, applications and interfaces
- WHERE: Security technology infrastructure, platforms and networks
- WHEN: Time-related dependencies

The answers will enable the development of the physical security architecture

SABSA: Tradesman's View

Turning the builder's physical design into an actual implementation

- WHAT: Detailed data structures that need to be protected
- WHY: Relevant security standards
- HOW: Vendor products are tools needed to protect data structures
- WHO: Users, their privileges, roles and access controls
- WHERE: Servers, computers, appliances, protocols, etc
- WHEN: Security step timing and sequencing

The answers will enable the development of the component security architecture

SABSA: The Facility Manager's View

Operating, maintaining and monitoring the system and the services it provides

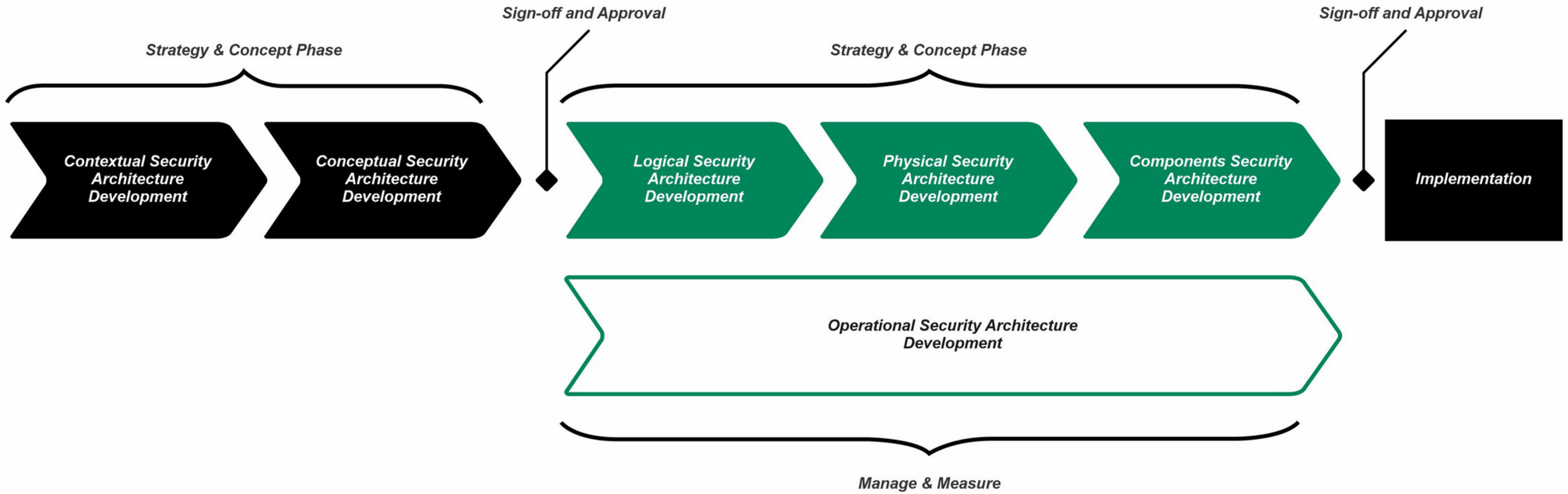
- WHAT: System performance and security maintenance
- WHY: Reduce operational failure and security incidents
- HOW: Security-related operations
- WHO: Users involved in providing security-related operational support
- WHERE: All system components, platforms and networks
- WHEN: Scheduling and executing security-related operations

The answers will enable the development of the operational security architecture.

SABSA: The Inspector's View

Will provide security architecture assurance and will ensure that the security architecture is complete and meets the security needs of the business.

SABSA: Development Process



SABSA: LIFE CYCLE