SIGN IN

prise Security

Enterprise Security Architecture—A Top-down Approach

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

STORE

SA SCF, TOGAF

n enterprises.
etective and
infrastructure

SIGN IN

s, controls,

The world has changed; security is not the same beast as before. Today's risk factors and threats are not the same, nor as simple as they used to be. New emerging technologies and possibilities, e.g., the Internet of Things, change a lot about how companies operate, what their focus is and their goals. It is important for all security professionals to understand business objectives and try to support them by implementing proper controls that can be simply justified for stakeholders and linked to the business risk. Enterprise frameworks, such as Sherwood Applied Business Security Architecture (SABSA), COBIT and The Open Group Architecture Framework (TOGAF), can help achieve this goal of aligning security needs with business needs.

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

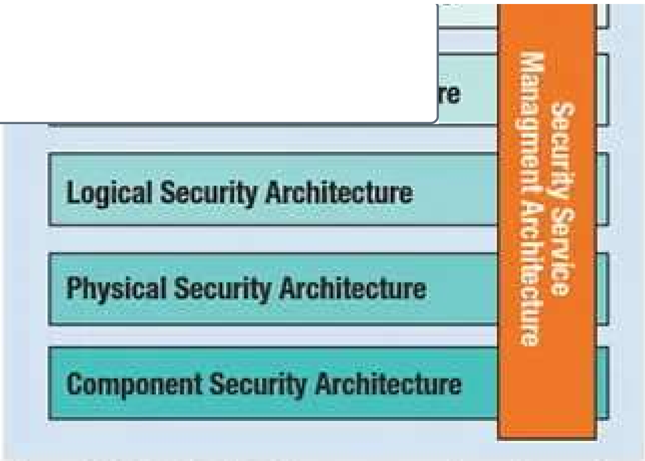
STORE

at is based on
ny specific
n for
ogy to assure

vertical). Each
he top and
e conceptual
of this

enterprises
of enterprise

SIGN IN


re
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Managment Architecture

Source: SABSA, *SABSA White Paper*, 2009, www.sabsa.org/sabsa-white-paper. Reprinted with permission.

optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use." COBIT 5 aligns IT with business while providing governance around it.

The COBIT 5 product family has a lot of documents to choose from, and sometimes it is tough to know exactly where to look for specific information. **Figure 2** shows the COBIT 5 product family at a glance.[2] COBIT Enablers are factors that, individually and collectively, influence whether something will work.

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

STORE

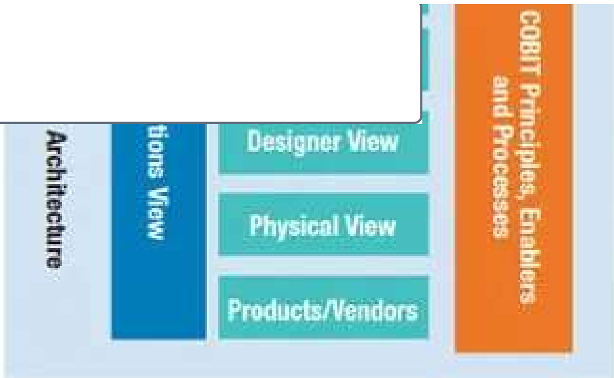
ing those

nt and process

SIGN IN

5. Separating Governance From Management
2. Covering the Enterprise End-to-end
COBIT 5 Principles
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

Source: ISACA, COBIT® 5, USA, 2012. Reprinted with permission.

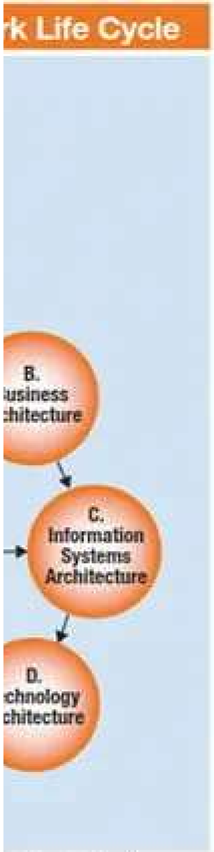


Source: R. Ghaznavi-Zadeh. Reprinted with permission.

By using a combination of the SABSA frameworks and COBIT principles, enablers and processes, a top-down architecture can be defined for every category in **figure 2**. As an example, when developing computer network

layers can be

CREDENTIALING
MEMBERSHIP
ENTERPRISE
PARTNERSHIPS
TRAINING & EVENTS
RESOURCES
JOIN/REACTIVATE
ABOUT US
CAREERS
SUPPORT
STORE



le. Reprinted with

SIGN IN

itor the

ould be.

Using the Frameworks to Develop an Enterprise Security Architecture

The fair question is always, "Where should the enterprise start?"

If one looks at these frameworks, the process is quite clear. This must be a top-down approach—start by looking at the business goals, objectives and vision.

CREDENTIALING

prise security

MEMBERSHIP

ENTERPRISE

se goals

revent a

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

STORE

SIGN IN

        - Network security
        - Operating system security
        - File security
        - Database security, practices and procedures
    - Define component architecture and map with physical architecture:
        - Security standards (e.g., US National Institute of Standards and Technology [NIST], ISO)
        - Security products and tools (e.g., antivirus [AV], virtual private network [VPN], firewall, wireless security, vulnerability scanner)

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

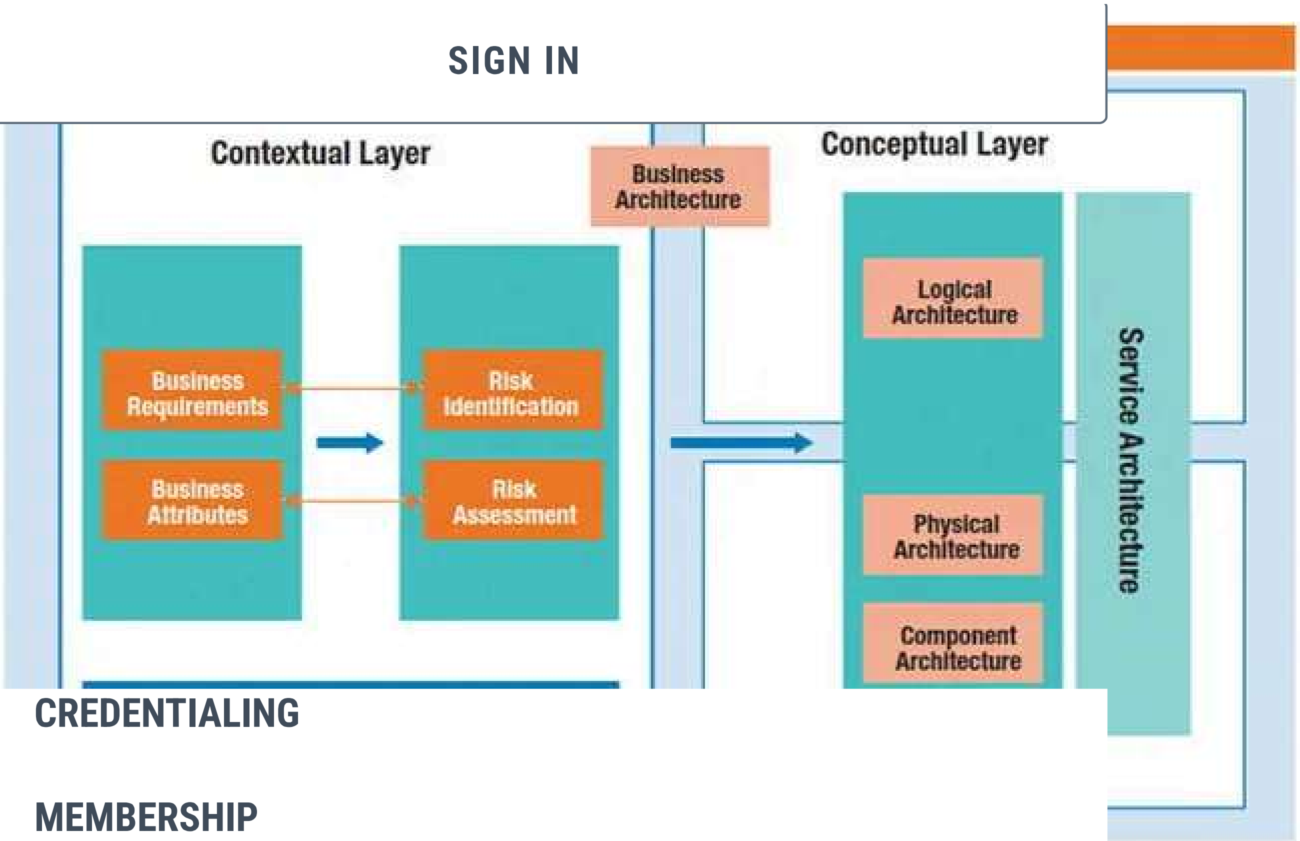
SUPPORT

STORE

col,
tion firewall

nterprise can
wareness,

SIGN IN



CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

STORE

s that can be

oal is to have
f the business

all times.
d.
accurate.
ndustry [PCI] in
s.

SIGN IN

accuracy

attributes)

- Lack of segregation of duties (SoD) (this is linked to the privacy attribute)
- Not Payment Card Industry Data Security Standard (PCI DSS) compliant (this is linked to the regulated attribute)

Some of the controls are:

- Build a disaster recovery environment for the applications (included in COBIT DSS04 processes)
- Implement vulnerability management program and application firewalls (included in COBIT DSS05 processes)

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

STORE

ntrols

S05

ectly

cycle needs
tributes and
s.

TOGAF
als,
g and

SIGN IN

nance indicators (KPIs) in place to measure the maturity of the architecture over time.

The first phase measures the current maturity of required controls in the environment using the Capability Maturity Model Integration (CMMI) model. The CMMI model has five maturity levels, from the initial level to the optimizing level.[6] For the purpose of this article, a nonexistent level (level 0) is added for those controls that are not in place (**figure 7**).

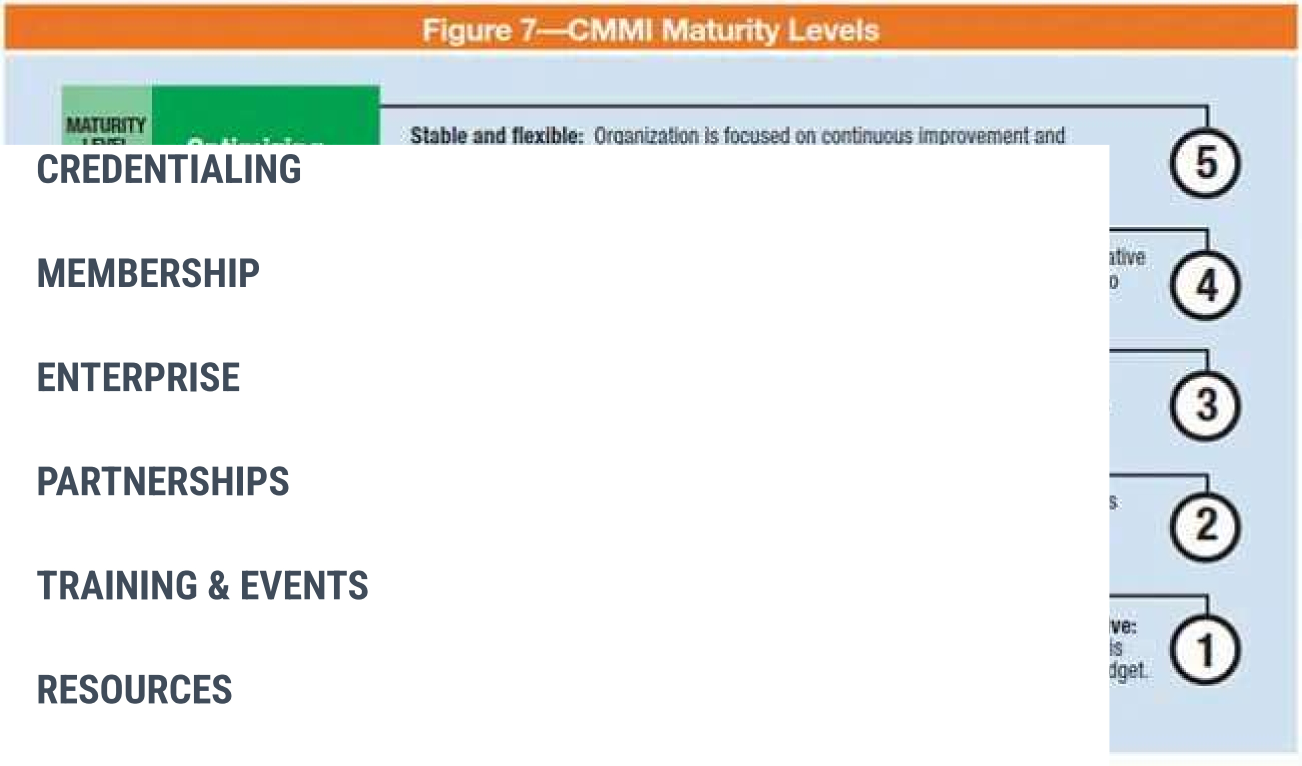


Figure 7—CMMI Maturity Levels
MATURITY LEVEL
Stable and flexible: Organization is focused on continuous improvement and
5
ative
o
4
3
s
2
ve:
is
dget.
1

CREDENTIALING
MEMBERSHIP
ENTERPRISE
PARTNERSHIPS
TRAINING & EVENTS
RESOURCES
JOIN/REACTIVATE
ABOUT US
CAREERS
SUPPORT
STORE

nt level with

l.

on the

- Security policies and standards

- **Operational controls**
  - Asset management
  - Incident management
  - Vulnerability management
  - Change management
  - Access controls
  - Event management and monitoring
- **Application controls**

[WAF], SIEM,

ctivity

gle sign-on

IPS], patch
ment)
device

ounting [AAA],

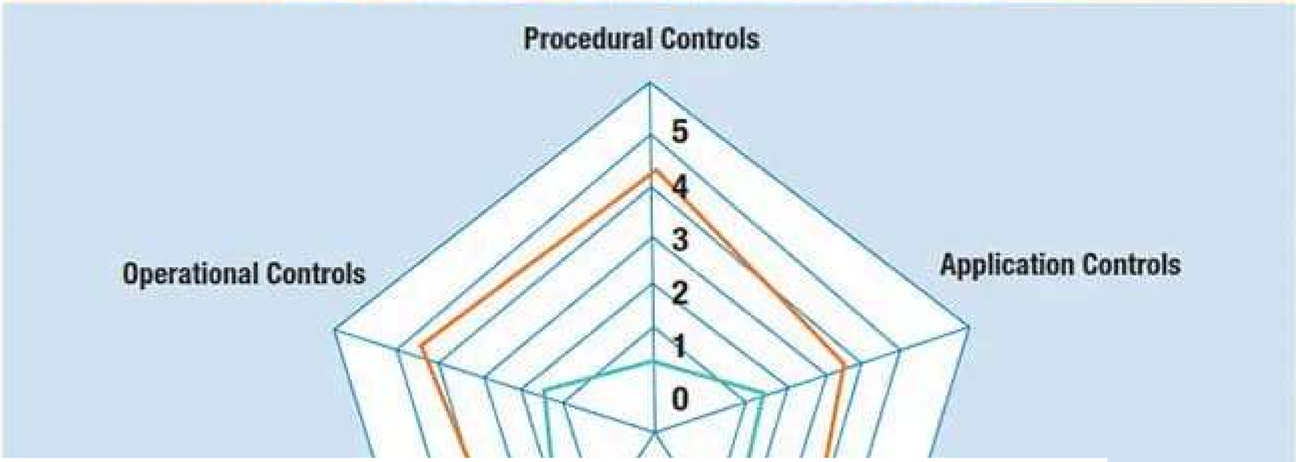
prevention

rols for
and controls

SIGN IN

architecture.

Figure 8—Maturity Reporting and Dashboard Example



CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN/REACTIVATE

ABOUT US

CAREERS

SUPPORT

STORE

curity
able risk to
GAF
als and

SIGN IN

uidance on

- The COBIT Process Assessment Model (PAM) provides a complete view of requirement processes and controls for enterprise-grade security architecture.
- SABSA layers and framework create and define a top-down architecture for every requirement, control and process available in COBIT.
- The TOGAF framework is useful for defining the architecture goals, benefits and vision, and setting up and implementing projects to reach those goals.
- The CMMI model is useful for providing a level of visibility for management and the architecture board, and for reporting the maturity of the architecture over time.

The simplified agile approach to initiate an enterprise security architecture program ensures that the enterprise security architecture is part of the business requirements, specifically addresses business needs and is automatically justified.

Endnotes

[1] ISACA, COBIT 5, USA, 2012
[2] Thomas, M.; "The Core COBIT Publications: A Quick Glance," *COBIT Focus*, 13 April 2015
[3] *Op cit*, ISACA
[4] The Open Group, "Welcome to TOGAF 9.1, an Open Group Standard, http://pubs.opengroup.org/architecture/togaf9-doc/arch/
[5] The Open Group, "TOGAF 9.1 Architecture Development Cycle," http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html
[6] CMMI Institute, "CMMI Maturity Levels," http://cmmiinstitute.com/capability-maturity-model-integration

network and security professional and developed his knowledge around enterprise business, security architecture and IT governance. Ghaznavi-Zadeh is an IT security mentor and trainer and is author of several books about enterprise security architecture and ethical hacking and penetration, which can be found on Google Play or in the Amazon store.

< PREVIOUS ARTICLE

NEXT ARTICLE >

Contact Us

Terms

Privacy

Cookie Notice

Cookie Settings

Fraud Reporting

Bug Reporting