SECURITY SERIES

Open Enterprise Security Architecture (O-ESA)

A Framework and Template for Policy-Driven Security

Van Haren Publishing

THE Open GROUP

Open Enterprise Security Architecture (O-ESA):
A Framework and Template for Policy-Driven Security

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT management
- Architecture (Enterprise and IT)
- Business management and
- Project management

Van Haren Publishing offers a wide collection of whitepapers, templates, free e-books, trainer material etc. in the **VHP Knowledge Base**: www.vanharen.net for more details.

VHP is also publisher on behalf of leading organizations and companies:
ASLBiSL Foundation, CA, Centre Henri Tudor, Gaming Works, Getronics, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, Quint, The Open Group, The Sox Institute, Tmforum.

Topics are (per domain):

IT (Service) Management / IT Governance
ABC of ICT
ASL
BiSL
CATS CM®
CMMI
CoBIT
Frameworx
ISO 17799
ISO 27001
ISO 27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL®
ITSM
MOF
MSF
SABSA

Architecture (Enterprise and IT)
Archimate®
GEA®
SOA
TOGAF®

Business Management
Contract Management
EFQM
eSCM
ISA-95
ISO 9000
ISO 9001:2000
OPBOK
Outsourcing
SAP
SixSigma
SOX
SqEME®

Project/Programme/ Risk Management
A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP™
P3O®
PMBOK® Guide
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Open Enterprise Security Architecture (O-ESA)

A Framework and Template for Policy-Driven Security

Colofon

Title:	Open Enterprise Security Architecture (O-ESA)
Subtitle:	A Framework and Template for Policy-Driven Security
A Publication of:	The Open Group
Lead Author:	Stefan Wahe, University of Wisconsin – Madison
Consulting Author/Editor:	Gunnar Peterson, Artec Group
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 672 5
Edition:	First edition, first impression, September 2011
Design and Layout:	CO2 Premedia bv, Amersfoort – NL
Copyright:	© The Open Group, 2011

For any further enquiries about Van Haren Publishing, please send an email to:
info@vanharen.net

Comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza, Forbury Road
Reading
Berkshire RG1 1AX
United Kingdom

or by electronic mail to: ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® certification.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

More information is available at www.opengroup.org/certification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes white papers, technical studies, branding and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

As with all *live* documents, Technical Standards and Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards-compatible and those which are not:

- A new *Version* indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it *replaces* the previous publication.
- A new *Issue* indicates there is substantive change to the definitive information contained in the previous publication of that title, and

there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

Network Applications Consortium (NAC)

The Network Applications Consortium (NAC) was founded in 1990 as a strategic end-user organization whose vision was to improve the interoperability and manageability of business-critical applications being developed for the heterogeneous, virtual enterprise computing environment. Its mission was to promote member collaboration and influence the strategic direction of vendors developing virtual enterprise application and infrastructure technologies. Its diverse membership equipped it to explain the need for agile IT infrastructure in support of business objectives, aimed at consolidating, clarifying, and communicating infrastructure technology needs to influence the IT industry and drive the evolution of standards and products.

One of its significant achievements was publishing the NAC Enterprise Security Architecture (ESA) Guide in 2004. In late 2007, the NAC transitioned into the Security Forum. At that time, the members of the NAC who joined the Security Forum recognized the significant value of the ESA Guide. It contained much valuable information that remains as relevant today as when it was first published. Members also realized, however, that security practice had moved on since 2004, so parts of the ESA Guide would benefit from updates and additions. Accordingly, a new project was initiated to update this ESA Guide.

This document

Information security professionals today recognize the high value of having a clear enterprise security architecture for their business, and developing and migrating their security strategies within a sound and well-structured framework, driven by business priorities derived from sound risk management assessments. This Open Enterprise Security Architecture (O-ESA) Guide provides a valuable reference resource for practicing security architects and designers. It gives a comprehensive overview of the key

security issues, principles, components, and concepts underlying architectural decisions that are involved when designing effective enterprise security architectures. It does not define a specific enterprise security architecture, and neither is it a "how to" guide to design one, although in places it does indicate some of the "how".

This Guide updates the NAC 2004 ESA Guide to bring it up-to-date in those areas which have evolved since its 2004 publication date. In particular, it replaces the quoted extract licensed from the British Standards Institute Code of Practice for Information Security Management, by referencing rather than licensing reproduction of quoted extracts from the latest ISO/IEC 27001/2 standard.

Intended audience

The O-ESA Guide provides a valuable reference resource for practicing security architects and designers – explaining key terms and concepts underlying security-related decisions that security architects and designers have to make. In doing so it enables them to explain their architectures and decision-making processes to their associated architecture and management colleagues in related disciplines.

The description avoids excessively technical presentation of the issues and concepts, so making it also an eminently digestible reference for CxO-level managers, enterprise architects, and designers, so enabling them to appreciate, validate, and balance the security architecture viewpoints along with all the other viewpoints involved in creating a complete enterprise architecture.

Trademarks

Boundaryless Information Flow™ is a trademark and ArchiMate®, Jericho Forum®, Making Standards Work®, Motif®, OSF/1®, The Open Group®, TOGAF®, UNIX®, and the "X" device are registered trademarks of The Open Group in the United States and other countries.

The Open Group acknowledges that there may be other brand, company, and product names used in this document that may be covered by trademark protection and advises the reader to verify them independently.

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following people in the development of this O-ESA Guide:

- Project Leader:
  Stefan Wahe, University of Wisconsin – Madison

- Consulting Author-Editor:
  Gunnar Peterson, Managing Principal, Artec Group

- Reviewer Group:
  Security Forum members, in particular:
  - Vicente Aceituno, ISM3 Consortium
  - Ian Dobson, The Open Group
  - François Jan, Systems Architect and Security/IAM Specialist, Arismore
  - Mike Jerbic, Trusted Systems Consulting, and Chair of the Security Forum
  - Mary Ann Mezzapelle, Chief Technologist, HP Enterprise Security Services

Referenced documents

The following documents are referenced in this O-ESA Guide:

- Architectural Patterns for Enabling Application Security, Joseph Yoder & Jeffrey Barcalow (1998).
- Attack Surface Measurement and Attack Surface Reduction, Pratyusa K. Manadhata & Jeannette M. Wing; refer to: www.cs.cmu.edu/~pratyus/as.html.
- Building Secure Software: How to Avoid Security Problems the Right Way, John Viega & Gary McGraw, Addison-Wesley, 2001.
- Burton Group (now merged into Gartner) Enterprise Identity Management: It's about the Business, Version 1, July 2003.
- Computer Security: Art and Science, Matt Bishop, Addison-Wesley, 2002.
- Cyber Security and Control System Survivability, Howard Lipson, 2005; refer to www.pserc.org.
- HIPAA: (US) Health Insurance Portability and Accountability Act, 1996.
- Introduction to XDAS; refer to: www.opengroup.org/security/das/xdas_int.htm.
- ISO/IEC 10181-3:1996: Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework; refer to www.iso.org.
- ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements; refer to www.iso.org (also BS 7799-2:2005).
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management; refer to www.iso.org.
- Logging in the Age of Web Services, Anton Chuvakin & Gunnar Peterson, IEEE Security & Privacy Journal, May 2009; refer to: http://arctecgroup.net/pdf/82-85.pdf.
- NIST SP 800-27: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, June 2004; refer to: csrc.nist.gov/publications/PubsSPs.html.
- NIST SP 800-33: Underlying Technical Models for Information Technology Security, Special Publication, December 2001.

- NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010; refer to: csrc.nist.gov/publications/PubsSPs.html.
- NIST SP 800-55: Performance Measurement Guide for Information Security, July 2008; refer to: csrc.nist.gov/publications/PubsSPs.html.
- NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007; refer to: csrc.nist.gov/publications/PubsSPs.html.
- NIST SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009; refer to: csrc.nist.gov/publications/PubsSPs.html.
- NIST SP 800-63: Electronic Authentication Guideline, April 2006; r efer to: csrc.nist.gov/publications/PubsSPs.html.
- Open Information Security Management Maturity Model (O-ISM3), Technical Standard (C102), published by The Open Group, February 2010; refer to: www.opengroup.org/bookstore/catalog/c102.htm.
- OWASP Guide Project; refer to www.owasp.org/index.php/OWASP_Guide_Project.
- Payment Card Industry (PCI) Data Security Standard (DSS): Requirements and Security Assessment Procedures, Version 1.2; October 2008.
- Peer Reviews in Software: A Practical Guide, Karl E. Wiegers (Addison-Wesley, 2001).
- Problems with XACML and their Solutions, Travis Spencer, September 2010; refer to: http://travisspencer.com/blog/2010/09/problems-with-xacml-and-their.html#comments.
- Putting the Tools to Work: How to Succeed with Source Code Analysis, Pravir Chandra, Brian Chess, & John Steven, IEEE Security & Privacy; refer to www.cigital.com/papers/download/j3bsi.pdf.
- Risk Taxonomy, Technical Standard (C081), published by The Open Group, January 2009; refer to www.opengroup.org/bookstore/catalog/c081.htm.
- (US) Sarbanes-Oxley Act; refer to: www.sox-online.com.
- Secure Coding: Principles and Practices, Mark G. Graff & Kenneth R. Van Wyk, O'Reilly, 2003.
- Securing the Virtual Enterprise Network: Layered Defenses, Coordinated Policies, Version 2, May 2003 (inc. description of the Burton Group (now merged into Gartner) VEN Security Model).

- Security at Microsoft, Technical White Paper, Published: November 2003.
- Security Design Patterns, Part 1 v1.4, Sasha Romanosky, November 2001.
- Security Design Patterns, by Bob Blakley, Craig Heath, and members of The Open Group Security Forum (G031), published by The Open Group, 2004; refer to: www.opengroup.org/bookstore/catalog/g031.htm.
- Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson, ISBN: 978-0-470-06852-6, Wiley, 2008.
- Software Security: Building Security In, Gary McGraw, Addison-Wesley, 2006.
- The Security Development Lifecycle, Michael Howard & Steve Lipner, Microsoft Press, 2006.
- Uncover Security Design Flaws Using the STRIDE Approach, Shawn Hernan, Scott Lambert, Tomasz Ostwald, & Adam Shostack; refer to: msdn.microsoft.com/en-us/magazine/cc163519.aspx.
- Writing Secure Code, Second Edition, Michael Howard & David C. LeBlanc, Microsoft Press, 2002.
- XACML (Extensible Access Control Markup Language), OASIS; refer to www.oasis-open.org/committees/xacml.

Chapter 1

Executive overview

Information systems security has never been more critical around the world. As more data is collected, stored, and propagated, the protection of information systems grows increasingly complex. Demand for new and improved services in both the public and private sectors is intense, and as enterprises reinvent their services infrastructure to meet this demand, traditional boundaries are disappearing. The cyber security threats lurking outside those traditional boundaries are real and well documented. Security by exclusion – attempting to maintain hard perimeters – is no longer a viable approach. The enterprise must allow access to its information resources by the services that citizens, customers, suppliers, and business partners are demanding; to allow employees and independent agents to work effectively from home; or to support some other variation on user access to the services of the enterprise.

Late in 2003 a group of NAC[1] members began meeting the challenge of describing a common framework that would speed the process of developing enterprise security architectures for this complex environment and create the governance foundation for sustaining it into the future. How does one simplify the process of governing security by exclusion (keeping the bad guys out) and security by inclusion (allowing and encouraging legitimate users to come in)? The NAC members' premise[2] was that policy-driven security architecture is essential in order to simplify management of this increasingly complex environment. As the Corporate Governance Task Force Report[3] states: "The road to information security goes through corporate governance." At the heart of governance are policy definition, implementation, and enforcement. To simplify security management, there must be a direct linkage between governance and the security architecture itself – in other words, policy-driven security architecture.

1 Network Applications Consortium – merged in 2007 into membership of The Open Group Security Forum – refer to: www.opengroup.org/projects/sec-arch.
2 This premise was shared by many others in the industry, including the Open Group's Security Forum.
3 The full report is available at www.cyberpartnership.org/init-governance.html.

What is policy-driven security architecture? It starts with a policy framework for identifying guiding security principles; authorizing their enforcement in specific control domains through a set of policies; and implementing the policies through technical standards, guidelines, and procedures. It continues with a policy-driven technical framework for creating electronic representations of the policy standards, storing them in central policy repositories, and referencing them at runtime to make and enforce policy decisions. Finally, it provides a policy-driven security operations framework for ensuring that the technology as deployed both conforms to policy and enforces policy across the environment.

The approach to designing policy-driven security architecture taken in this O-ESA Guide starts with defining an enterprise security program framework that places security program management in the larger context.

It continues with in-depth focus on the three major components that make up enterprise security architecture:

- Governance
- Technology Architecture
- Operations

For governance, this approach establishes the overall process, defines the policy framework that is at the heart of governance, and provides templates for security principles and policies. The principles template is derived from the National Institute of Standards and Technology (NIST) Engineering Principles for IT Security, supplemented by principles from Open Group member organizations and others. The policy template is adopted directly from ISO/IEC 27002:2005: Code of Practice for Information Security Management, which is now well established and adopted globally in the enterprise security space.

For technology architecture, the approach defines a generic framework for the management of policy-driven security services, and then utilizes the framework as the basis of an overall conceptual architecture for implementing policy-driven security services. The framework is based in part on the Burton Group (now merged into Gartner) Virtual Enterprise Network

(VEN) Security Model,[4] and in part on current and evolving standards in the policy management space. It extends the policy-driven concepts beyond access management to include configuration of other security services such as border protection, cryptography, content management, and auditing. The adoption of effective open standards is critical to the implementation of general-purpose policy-driven security architecture. Without these standards, centralization of policy and interoperability of the many products in the federated environment will not be possible. The complete solution can't be purchased off-the-shelf today; however, the XACML standard[5] (see also Section 3.6.3 and Chapter 6) is today widely seen as the basis for solutions being implemented by vendors, private and public companies, and by government and educational institutions.

In addition to the overall conceptual architecture, two of the identified security services – identity management and border protection – are analyzed further to the level of service-specific conceptual and logical architecture. These two examples illustrate the logical decomposition of high-level services to the level of detail required to implement the architecture. For other identified security services, there is a template of high-level service definitions but no additional detailed perspective.

The approach to security operations in this O-ESA Guide is to define the operational processes required to support a policy-driven security environment. These processes are of two types. One includes the administration, compliance, and vulnerability management processes required to ensure that the technology as deployed conforms to policy and provides adequate protection to control the level of risk to the environment. The other category includes the administration and event and incident management processes required to enforce policy within the environment. These operational processes are defined at a high level, not at the level of detail provided for governance and technology architecture.

Having developed the major components of open enterprise security architecture (O-ESA), this Guide goes on to describe the vision, technical

4 This VEN Security Model is described in Securing the Virtual Enterprise Network: Layered Defenses, Coordinated Policies.

5 XACML (Extensible Access Control Markup Language) is an OASIS standard. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.

model, and roadmap for achieving automated definition, instantiation, and enforcement of security policy. It begins by defining the policy layers and policy automation vision:

- Starting with the high-level definition of a business policy
- Mapping that to appropriate standards such as ISO/IEC 27001/2 security policies
- Translating the security policies to detailed technical standards
- Instantiating an electronic representation of those standards
- Then using that representation to drive the automated decision-making and enforcement process

The Guide then describes a technical model for implementing the vision, and establishes a roadmap of user and industry actions required to enable that technical model. The intent is to use this portion of the Guide as a catalyst to drive awareness of the need for the required industry standards and technologies.

This document concludes with recommendations in the policy-driven security space. The key recommendation is that security architects and designers proceed with implementation of the O-ESA policy and technology frameworks, recognizing that they must map business policies to the detailed technical standards required for decision-making and enforcement, which today can be increasingly though not yet fully automated. Incremental transition to policy automation products as business drivers and technology warrant can then follow. Vendors and standards organizations are encouraged to adopt O-ESA as a common vocabulary; support current and emerging standards related to policy-driven security; and consider the opportunities for open, standards-based products that support a common policy automation vision.

Chapter 2

Introduction

There is general agreement among certified security professionals and others that the overall objective of information security is to preserve the *availability*, *integrity,* and *confidentiality* of an organization's information. Effective IT security management also calls for providing *accountability* and *assurance*. Enterprise security architecture is the component of the overall enterprise architecture designed specifically to fulfil these objectives. A critical element of enterprise information security is physical security, which is the linchpin of a secure environment.

Enterprise security architecture may also be thought of as the overall framework for fulfilling these objectives while satisfying the security demands placed on the IT service organization by its customers. It includes all aspects of security governance, security technology architecture, and security operations required to protect the IT assets of the enterprise.

The objective of this document is twofold:

- To provide a framework that serves as a common reference for describing enterprise security architecture and technology both within and between organizations
- To provide a template that allows user organizations to select the elements of enterprise security architecture they require and to tailor them to their needs

2.1 General description of an enterprise security program

This Guide's enterprise security architecture must be understood in the larger corporate context, where it is part of an overall enterprise security program, as shown in Figure 2.1.

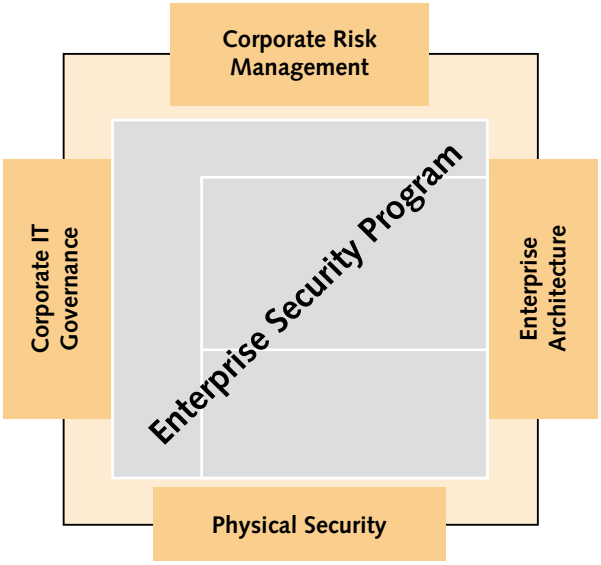

Figure 2.1: Corporate enterprise security context

It must relate appropriately to the corporate risk management, corporate IT governance, enterprise architecture, and physical security programs of the enterprise. The specifics of how it relates may vary from one organization to another.

The overall enterprise security program is expanded in Figure 2.2 as four concentric rings of responsibility:

- Overall program management responsibility lives in the outer ring.
- Security governance responsibility lives in the second ring.
- Security technology architecture responsibility lives in the third ring.
- Security operations responsibility lives in the inner ring.

Each ring identifies key components and processes that fall within that responsibility domain. Viewed in the context of a constraints-based methodology, the components of each ring represent deliverables that further narrow the definition of what must be provided by the inner rings. Thus the requirements, strategy, planning roadmaps, and risk management assessments from the outer ring narrow the definition of what must be provided in the governance and technology architecture rings. For example, a new privacy requirement may dictate the definition of new governing principles, policies, and standards as well as the implementation of new technology architecture.

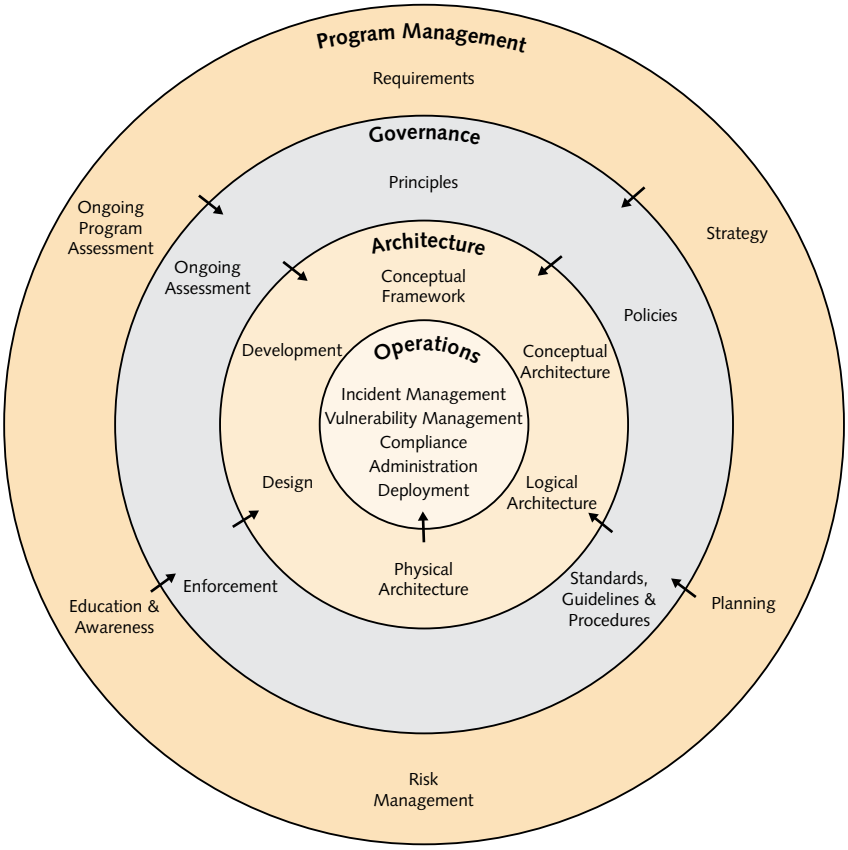

Figure 2.2: Enterprise security program model

The implementation of new standards and new architecture may in turn dictate the creation of new security processes or other capabilities within operations.

The program management functions identified in the outer ring of the enterprise security program model are considered outside the main scope of this O-ESA Guide's security architecture focus. In the next major section, the document focus will shift to O-ESA components identified in the inner rings: security governance, security technology architecture, and security operations. First, however – in recognition of the importance of the program management functions – the following section describes an overall enterprise security program framework. The goal is to provide a more complete overview of the security drivers and the program management functions, and also to provide a preview of the O-ESA structure and show how it relates to program management.

2.2 Enterprise security program framework

Figure 2.3 provides a more complete framework view of the enterprise security program. *Note that the rectangular boxes represent components or deliverables, while the octagonal boxes represent processes.* The framework starts with the four security drivers shown at the top, which identify the primary sources of security requirements that must be addressed. The key sources of internal requirements are the business areas, which have service-level business requirements they must meet to serve their current customers and to take advantage of new business opportunities. External requirements include security threats and legal and regulatory compliance requirements. Privacy and confidentiality are key examples of functional requirements driven by legal requirements. Risk management may also be affected for business areas within the purview of external regulatory commissions.

Requirements drive the development of the security program strategy deliverables as well as the planning process. Risk management is the crucial process of determining the acceptable level of security risk at various points in the enterprise IT system and implementing the optimal level of management and technical control; too little control may result in financial exposure, and too much may result in unnecessary cost. Education and awareness processes are critical to the success of any security program. Ongoing program assessment and gap analysis processes provide continual requirements feedback.

The functions of the O-ESA components and processes are summarized below and will be described further in the subsequent sections of the document.

Governance

- **Principles**: Basic assumptions and beliefs providing overall security guidance.
- **Policies**: The security rules that apply in various control domains.
- **Standards, guidelines, and procedures**: The implementation of the policies through technical requirements, recommended practices, and instructions.
- **Audit**: The process of reviewing security activities for policy compliance.
- **Enforcement**: The processes for ensuring compliance with the policies.

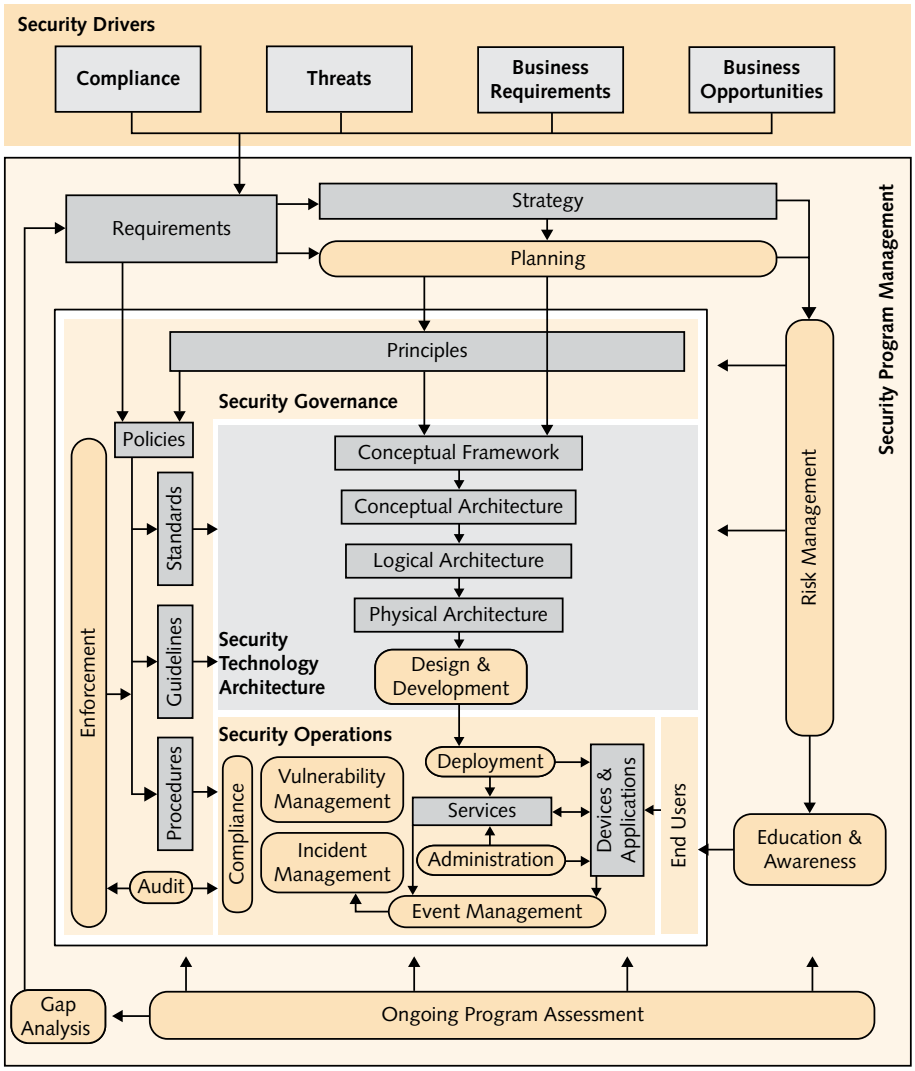

Figure 2.3: Enterprise security program framework

Technology architecture

- **Conceptual framework**: Generic framework for policy-based management of security services.
- **Conceptual architecture**: Conceptual structure for management of decision-making and policy enforcement across a broad set of security services.
- **Logical architecture**: Provides more detail on the logical components necessary to provide each security service.

- **Physical architecture**: Identifies specific products, showing where they are located and how they are connected to deliver the necessary functionality, performance, and reliability.
- **Design/development**: Guides, templates, tools, re-usable libraries, and code samples to aid in the effective utilization and integration of applications into the O-ESA environment.

Security operations

- **Deployment**: Assumed to be the normal IT deployment process, not a security operations process.
- **Services**: The core security functions defined by the security technology architecture that support devices and applications, as well as other security operations processes.
- **Devices and applications**: Devices and applications that use O-ESA services and are supported by the security operations processes.
- **Administration**: The process for securing the organization's operational digital assets against accidental or unauthorized modification or disclosure.
- **Event management**: The process for day-to-day management of the security-related events generated by a variety of devices across the operational environment, including security, network, storage, and host devices.
- **Incident management**: The process for responding to security-related events that indicate a violation or imminent threat of violation of security policy (i.e., the organization is under attack or has suffered a loss).
- **Vulnerability management**: The process for identifying high-risk infrastructure components, assessing their vulnerabilities, and taking the appropriate actions to control the level of risk to the operational environment.
- **Compliance**: The process for ensuring that the deployed technology conforms to the organization's policies, procedures, and architecture.

2.3 Enterprise security architecture

With the enterprise security program framework as background, the focus for the remainder of the document shifts to the O-ESA components. As shown in Figure 2.4, the security program management functions now assume a background role and become part of the larger corporate context, as the focus

shifts to security governance, security technology architecture, and security operations. Our goal is to describe an O-ESA framework and templates that user organizations can understand, tailor to their needs, and use as a starting point for an O-ESA implementation.

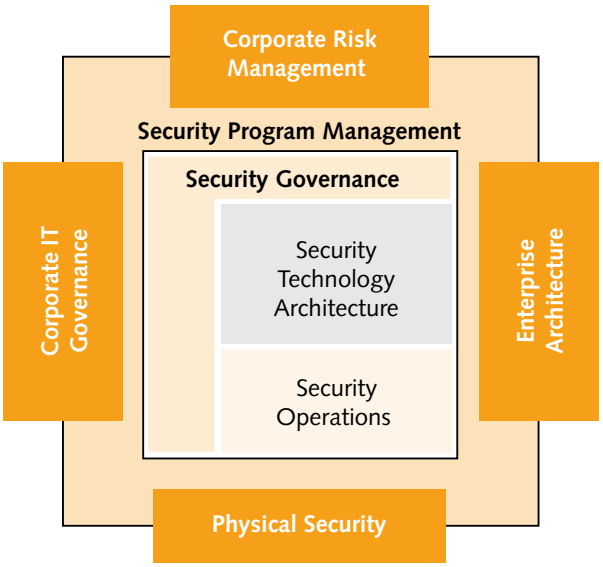

Figure 2.4: Enterprise security architecture components

To effectively design and implement O-ESA, one needs to understand the purpose and relationships of the O-ESA components. To aid in that understanding, the following discussion draws an analogy to a more commonly understood architectural model – designing a house. This discussion opens with a brief comparison of the house design model and the design of the enterprise security system model.

2.3.1 The house design model

It is helpful to begin with a brief review of the issues involved in the house design model:

- **Community standards**: The specific external and internal standards required by the housing community.
- **Design requirements**: The specific design criteria that are settled on after considering wants, needs, costs, etc. such as passive solar design with star wiring topology (LAN/telephony) and home entertainment system, plus fully disability-accessible downstairs with master bedroom and utilities.

- **Building codes and engineering practices**: The building standards and practices that support the design requirements and the architecture.
- **Architectural plan**: This is the resulting set of the artist's renderings and blueprints that document what the house will look like from various perspectives. Also a necessary part of the plans are the detail drawings for the major components of the overall construction such as framing and the plumbing, electrical, and HVAC systems.
- **Bill of materials**: The detailed list of materials needed to build the house.
- **Maintenance**: The specific considerations for keeping the house up and its systems operational. Although not typically a significant part of the house design process, these specifications are relevant.

2.3.2 The enterprise security system design model

- **Corporate standards**: The specific corporate standards that affect the enterprise security system.
- **Design requirements**: The specific design criteria that are settled on after consideration of wants, needs, costs, etc. One of these is already specified: the policy-driven security services. Other examples might include support for service-oriented application designs and role-based access control.
- **Governance**: The principles, policies, and implementing standards that support the design requirements and the specific architecture.
- **Architectural plan**: This is the resulting set of conceptual diagrams and blueprints that document what the resulting security system will look like from various perspectives. The plan includes the conceptual and detail drawings for major subsystems such as identity management, access control, and border protection services, as well as the required products, applications, platforms, etc.
- **Security services**: The itemization of the services and ultimately the individual applications and products needed.
- **Operations**: The considerations for day-to-day-operation of the security services and supporting infrastructure.

Let's take a look at each of these in detail and compare and contrast the components of the two models.

2.3.3 Community standards versus corporate standards

It is important to keep in mind that both designs take place in a larger context that may impose constraints on the design – the house is part of a

larger residential development or community, and the enterprise security system is part of a larger enterprise IT system.

In the house example, the community may impose standards to maintain a certain level of quality and appearance. It may, for example, restrict the use of certain types of siding and certain colors, and it may require a Jacuzzi and ceramic tile floor in the master bath and wood floors in certain rooms.

In the security example, corporate standards may be imposed to ensure that investments leverage existing technology or support infrastructure. They may, for example, require that all user-interfacing products support Lightweight Directory Access Protocol (LDAP) interoperability with their standard Network Operating System (NOS) or corporate directory to avoid proliferation of additional user registries and sign-on requirements.

2.3.4 Building codes and engineering practices versus governance

In both models, development of the architectural plan must consider the constraints imposed by this component, based on experience and good judgment.

In the house example, building codes and engineering practices are constraints developed through years of experience to ensure a sound and safe dwelling. Considerations here include such things as structural integrity, a healthy environment, and fire safety. The finished architectural plan for each house may vary widely, but all must comply with these requirements.

In the security example, governance defines the principles, policies, standards, guidelines, and procedures that constrain the design and operation of the security system. As with the house example, the governance elements are based on experience and good sense. Considerations include such things as simplicity, defense in depth, resilience, and common policy enforcement. As with the house example, security infrastructure implementations may vary widely, but all should comply with these requirements.

2.3.5 House architecture versus security technology architecture

In both cases the architectural plan represents the blueprints for implementation. In the house example, the industry has built enough houses to clearly understand the various levels of detail and perspectives necessary

for successful construction. Unfortunately, not many security infrastructures have been built using a comprehensive plan, so we are not nearly so clear on the levels of detail or perspectives needed.

One thing we do seem clear on is that any good plan starts with some high-level pictures and successively expands the detail in some organized fashion until the physical construction blueprints have been completed and construction can begin. In the computing industry these levels of detail are commonly termed the conceptual, logical, and physical architectures.

At the conceptual level, our design has the artist's renderings of various views of the house. We see what the house looks like, possibly from various perspectives, but without any of the construction details or internal system components. In the security context, this should be a picture or pictures of the infrastructure as a whole, defining the key design concepts – hence, a conceptual architecture.

At the logical level, our house design has floor plans to specify the layout of each floor and show how the rooms are connected. There is still no detail of construction or the systems such as plumbing, heating, or framing. In the security design, this is where we see major services (such as identity management, access control, and border protection) decomposed into a set of related components and supporting services. For identity management, we see provisioning services, external and internal directories, policy administration systems, HR systems, identity mapping services, and more.

At the physical level, our house design has details for assembling the framing, electrical, plumbing, and HVAC components. In the security context, we see deployment of products and applications that make up the various functional components; we see computing platforms and connectivity.

2.3.6 Bill of materials versus security services

The security services are the security infrastructure bill of materials. These are the core functions we need to actually assemble a cohesive security infrastructure. To better understand this area, it's useful to look at the similarities between a house bill of materials and security services.

In both cases it is easy to start by itemizing a high-level bill of materials. We all know what kinds of material it takes to build a house. We need lumber, concrete, pipes, fixtures, ducting, fasteners, etc. We can easily make this list, but without the detailed plan we are not able to specify the quantities and types of each component. Similarly, we all know what security services are needed, but without the plan we cannot accurately list the specific products and platforms. The bill of materials is not an integral part of the plan, although it is a necessary part of the overall effort. The detailed bill of materials is *derived* from the plan. The list of security services at the detailed product level allows us to know what we need to build or buy to implement our plan.

Although natural, it is a mistake to think we can start with this bill of materials (list of security services) and somehow derive the plan (this is discussed a little more in Section 2.3.8).

2.3.7 Maintenance versus operations

Once we have completed our house or security infrastructure, we need some processes and tools to maintain our work in a quality state. Furthermore, we probably need to take maintenance requirements into account in the design phase to facilitate our maintenance activities after completion.

In our house example, design elements related to maintenance might include selection of siding and flooring materials, installation of a built-in vacuum system, or placement of hose bibs to facilitate washing exterior components. Typical maintenance considerations after construction might be a daily cleaning plan, periodic painting and structural repair, regular heating and plumbing maintenance, and an occasional upgrade or addition.

In the security context, operations includes processes and tools for day-to-day vulnerability management, event management, and incident management, as well as other aspects of daily security administration and operation. These elements ensure continued effective and efficient functioning of the security environment.

2.3.8 The remodeling

Most enterprises do not start with a green field in the security infrastructure space. We all have existing environments developed over the years, typically started with independent proprietary platforms, each with its own security silo. The advent of the Internet has been the primary driver for the deployment of a variety of products and solutions that attempt to integrate these disparate systems. For most of us the current state is a hodge-podge of environments and tools in various states of interoperability. The good news is:

- These point and reactive solutions have been built by smart people. Even if they did not use a comprehensive plan, these smart people typically made decisions and deployed solutions with a vision of what the plan should ultimately look like.
- There is increasing focus on the development of security standards to deliver interoperability among these disparate platforms. Many standards are in the early stages of development or adoption, so it is likely that interoperability will improve with time. At the same time, however, the interoperability challenge is increasingly complex.
- For the solutions we already have deployed, the marketplace is driving the vendors to continually enhance their interoperability, thus making our lives easier.

What this means as we work to articulate our new enterprise security infrastructure design is that we already have much of our bill of materials and we can probably use a substantial portion of our existing deployment.

So in the context of our analogy, we are possibly talking about house remodeling, not new construction. Somewhat contrary to what was stated earlier, the bill of materials will not be completely derived from the plan. There will now be some consideration of the existing construction (and inherent bill of materials) incorporated into our new design. However, in this case it is probably not wise to overemphasize the existing deployment when laying out the conceptual and upper-level aspects of the logical design. Consideration of the existing infrastructure will have more influence on the details of the logical design subcomponents and the physical design.

In our security context this remodeling probably means:

- Leveraging existing work to identify the security drivers and governance components. Care should be taken to be comprehensive at this point in the effort and not to assume that previous work is up-to-date in our rapidly changing environment.
- Assessing our existing environment and products as we work through the lower-level logical design and physical design. Much of what we have should be usable in our new comprehensive vision.
- Identifying gaps and areas for improvement in our existing infrastructure and then making plans for closing the gaps and implementing the improvements.

With the house analogy as background, let's move on to describe the O-ESA framework and templates, starting with security governance and then describing security technology architecture and security operations. Hopefully the house analogy has provided a basis for clearer understanding of some of the terms we use, and at appropriate points, we'll refer to the analogy again to clarify the discussion.