

Security Forum

Who we are

The Security Forum is a membership group of security experts from both the customer and supply sides of industry, government, and academia, who share a common aim to raise confidence levels in IT business operations.

What we do

We identify information security business requirements and develop standards and guides that respond to them. Our global scope looks across all industries towards what's common to all, benefiting IT suppliers and consumers alike. Recently we have focused on information-centric security, open systems architectures including collaboration and service-oriented environments, risk management, and governance and compliance. We host quarterly Security Practitioners Conferences, where invited expert speakers address strategic issues within our interest areas.

Key accomplishments

In over 18 years of producing standards, technical guides, and best practice guides/papers, we have consistently led the way in helping practitioners understand and solve IT security problems. Our standards, technical guides, and best practice guides are all published in The Open Group Online Bookstore: www.opengroup.org/bookstore/catalog/se.htm.

Industry liaisons

The Open Group Forums work together to ensure security is addressed across all our Forums. We also have working relationships with other security consortia, and establish collaborative working arrangements with other groups where it is mutually beneficial to do so. These include the ABA Cyberspace Law Sub-group, BITS, Cloud Security Alliance, ETIS Security Working Group, EURIM, INCITS CS1, ISO JTC1 SC27, and Mitre.



Our security strategy

Our members understand how enterprise business IT is evolving from perimeter-based security practices towards information-centric security. We also recognize that today's security solutions must enable collaborative working with business partners, suppliers, customers, and employees, globally over the Internet. This significantly broadens the scope of what "information security" must cover. In a major 2008 White Paper (www.opengroup.org/bookstore/catalog/w075.htm), we established our security strategy as a Multi-Disciplinary Framework for Information-Centric Security, reflecting these requirements.

Today's business requirements need a new framework that supports global secure business collaboration:

- Corporate perimeter boundaries are crumbling as business demands greater connectivity with business partners, suppliers, customers, and employees, globally over the Internet.
- The Jericho Forum's Commandments and Collaboration Oriented Architectures (COA) Framework provide a design principles blueprint and practical framework for how to create secure architectures for business collaboration.
- Cloud computing offers huge computing power, storage, and applications resources, all at immediate availability and low cost. Business managers are now demanding their IT operations reap the great benefits this represents, so it's now urgent to extend secure business collaboration into cloud computing.

Becoming a member

The Forum welcomes participation from security professionals and practitioners. If you would like to influence our activities, participate in defining industry standards, and network with other security professionals, become a member – visit: www.opengroup.org/member.

More information

For more information, please email: securityforum@opengroup.org
or visit: www.opengroup.org/security

Security Forum

Current projects

Read more on all these projects at www.opengroup.org/projects/security.

Security Architectures

We take an architectural approach to information security. Currently projects includes:

- **Enterprise Security Architecture (ESA) Guide:** Updating our 1994 ESA Guide.
- **COA Framework Standard:** Developing a standard for a Framework for Collaboration Oriented Architectures.
- **COA Reference Architecture:** Developing a COA reference architecture within TOGAF 9, to demonstrate how to build secure enterprise architectures using the TOGAF Architecture Development Method (ADM).
- **SOA-Security Guide:** In collaboration with our SOA Working Group, developing a best practice guide to explain what additional security considerations SOA environments demand.
- **Secure Mobile Architectures (SMA) Standard:** We are liaising with other industry groups including the PCI Forum, ARC, SANS Institute, ISA, and TCG-TNC to identify the common technologies which need a standards-based SMA solution. The ability to maintain continuous connectivity in a mobile environment is critical in a number of application environments, including large manufacturing flow lines, and safety-critical SCADA environments.

IT Governance

- **Risk Management:** Business managers need effective IT risk assessments so they can make informed decisions on managing risk in their business. We have delivered our Risk Taxonomy standard, and our Guide to Evaluating Risk Assessment Methodologies. We are now developing a Risk Methodologies Cookbook.
- **Events & Logging:** We are updating our 1998 Distributed Audit Services (XDAS) standard to revise and extend it to meet today's more demanding requirements for event reporting, logging, and auditability, including working with Mitre on interoperability with their CEE standard.
- **Automated Compliance:** Our Automated Compliance Expert (ACE) standard will enable enterprises to achieve huge cost savings by defining security compliance configurations in standard XML (ACEML), and then monitoring for continued compliance. ACE complements, not competes with, compliance schemes from NIST/NSA/DHS, COBIT, ISO, PCI, and OASIS.
- **Ecosystem for Security:** Developing an authoritative guide on how Small & Medium Government/Business (SMGBs) can apply and maintain well-established, low-cost, easy-to-implement security processes and technologies to protect their information systems.

Security Management

- **Trust Management/Confidence Model:** The aim is to develop an industry standard defining common levels of sensitivity and classification for the value of data, and to specify responsive protection mechanisms to assure secure operation.
- **Identity & Access Management (IAM):** We are Category C contributors to the ISO Identity Management Framework (JTC1 SC27) standard, and contributors to UK EURIM. We are also developing a set of IAM requirements papers on managing business collaborations worldwide, including extending IAM into Cloud Computing.
- **Secure Enterprise 2.0:** Analysts list "consumerization of the enterprise" as one of today's most important corporate IT trends. In fact, consumer (i.e., Web 2.0) technologies are already finding their way into the enterprise, often without the approval of corporate IT management. This project is addressing how to secure Web 2.0 for enterprise business use.

About 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.

Further information on The Open Group can be found at www.opengroup.org.

TOGAF™ and Boundaryless Information Flow™ are trademarks and Making Standards Work®, The Open Group®, UNIX®, and Archimate® are registered trademarks of The Open Group in the United States and other countries.