Open Group Security Forum Overview

To the I3C, July 23, 2003

THE Open GROUP

Mike Jerbic
Chair – Security Forum

Office: 408.257.1648

m.jerbic@opengroup.org

www.opengroup.org

The Open Group is . . .

- A global consortium committed to delivering greater business efficiency by bringing together ***buyers*** and ***suppliers*** of information technology to lower the time, cost and risk associated with integrating new technology across the enterprise.

What We Used to Do

- Security Standards Development
  - X/Open Basic Security Services (XBSS)
  - Common Data Security Architecture (CDSA)
    - With reference implementation
  - Authorization API (AZN API)
- Work on PKI
  - Architecture (APKI)
  - DCE/PKI Integration

Why We Don’t Do That Now

- Security standards development is being well addressed by some other organizations
  - IETF, OASIS
- Some of our high-profile standards did not achieve the desired uptake and effect
  - CDSA, AZN
- There are significant challenges in security that are not being addressed anywhere else on a systematic basis

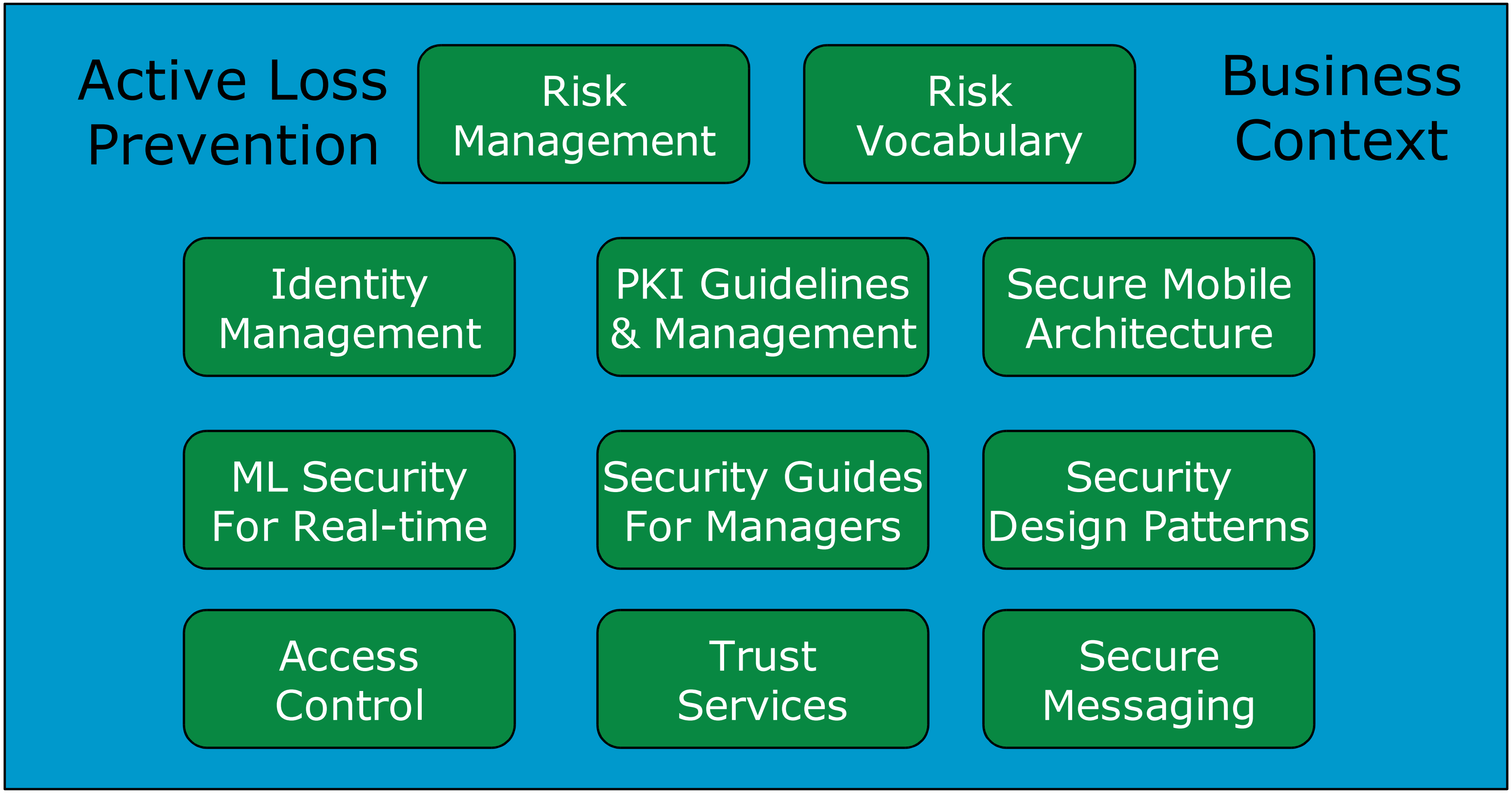
Classical Security Analysis

- Classical model in a cartoon
  - Analyze threats
  - Analyze vulnerabilities
  - Analyze risks
  - Design and implement countermeasures
- What’s wrong with the classical model?
  - It assumes closed domains
  - It starts with bad things to prevent
  - It assumes all risk is bad
  - The resulting solutions often prevents good things

Our Model Is Different

- We believe that security exists to ensure that business gets done according to policy
- Policies are business-driven, for example:
  - Comply with the law – to stay in business
  - Respect your customers - to keep them
  - Understand your risks and make business decisions about how to manage them - which to accept, which to offload, which to share, and how
- Security should enable right things & prevent wrong things – it's not all about "bad guys"
- Security in global networked environments raises new challenges and requires new approaches

Current Security Activities in The Open Group



Active Loss Prevention

Risk Management

Risk Vocabulary

Business Context

Identity Management

PKI Guidelines & Management

Secure Mobile Architecture

ML Security For Real-time

Security Guides For Managers

Security Design Patterns

Access Control

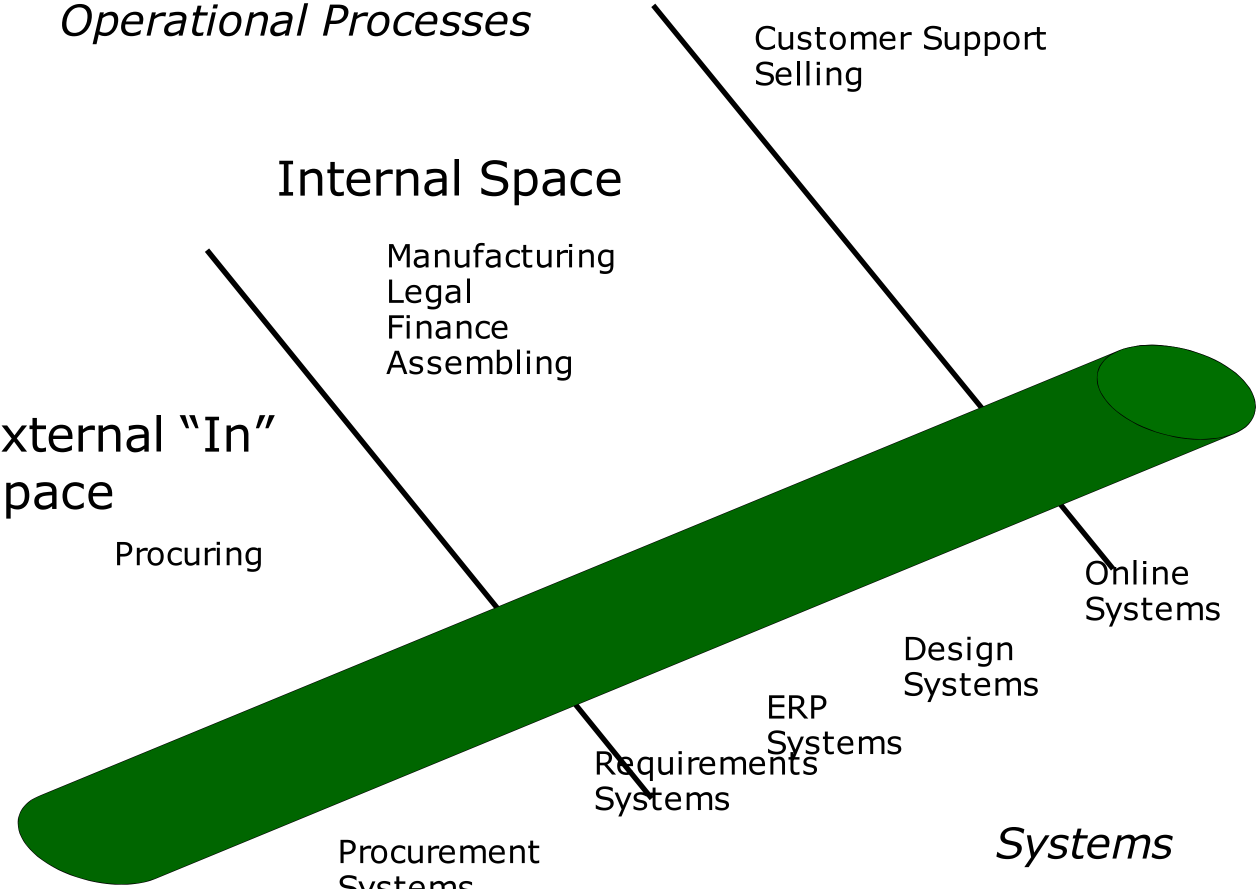
Trust Services

Secure Messaging

Problems from …

Need to integrate and optimize processes

Operational Processes



External "Out" Space

Customer Support
Selling

Internal Space

Manufacturing
Legal
Finance
Assembling

External "In" Space

Procuring

Online Systems

Design Systems

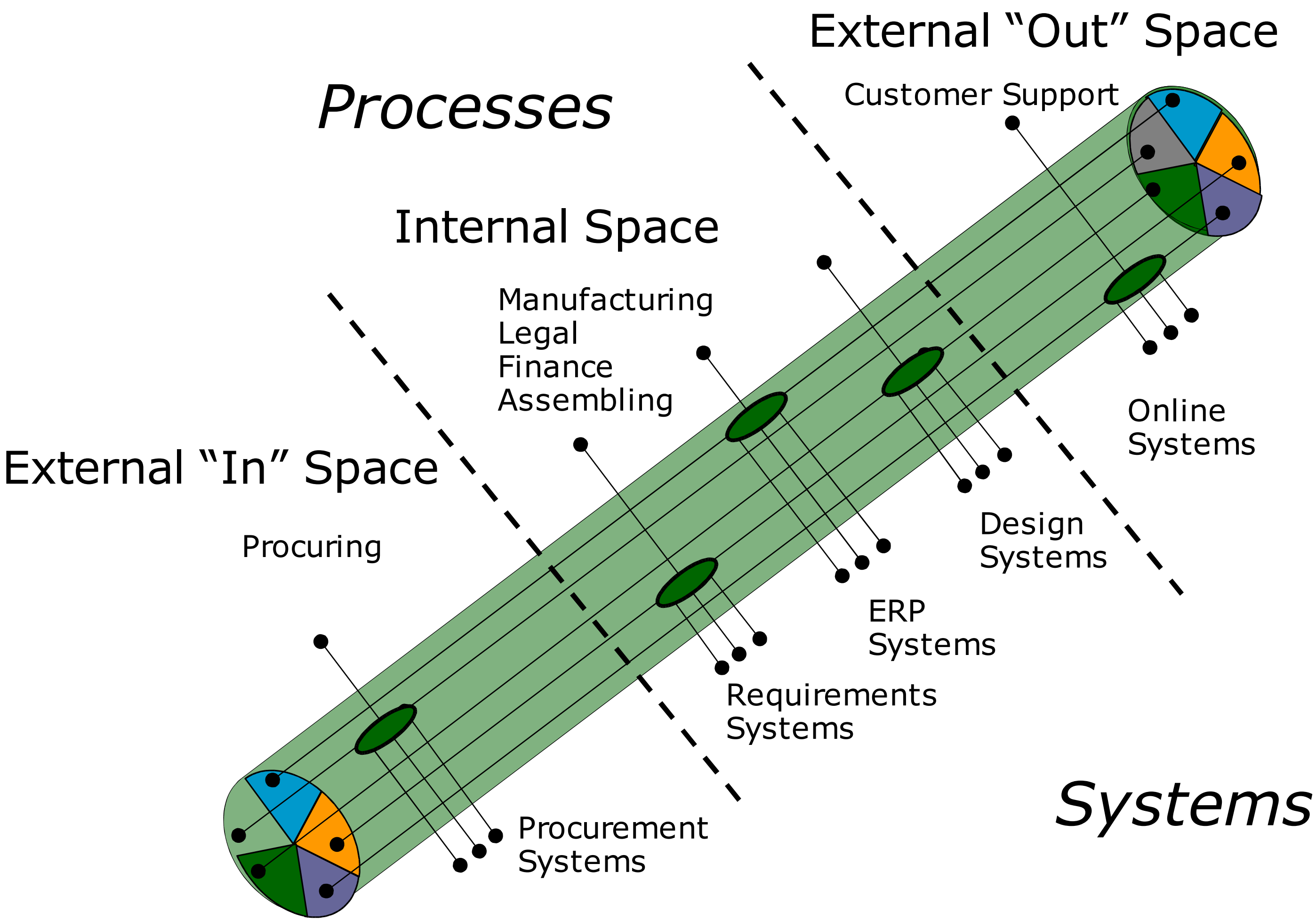
ERP Systems

Requirements Systems

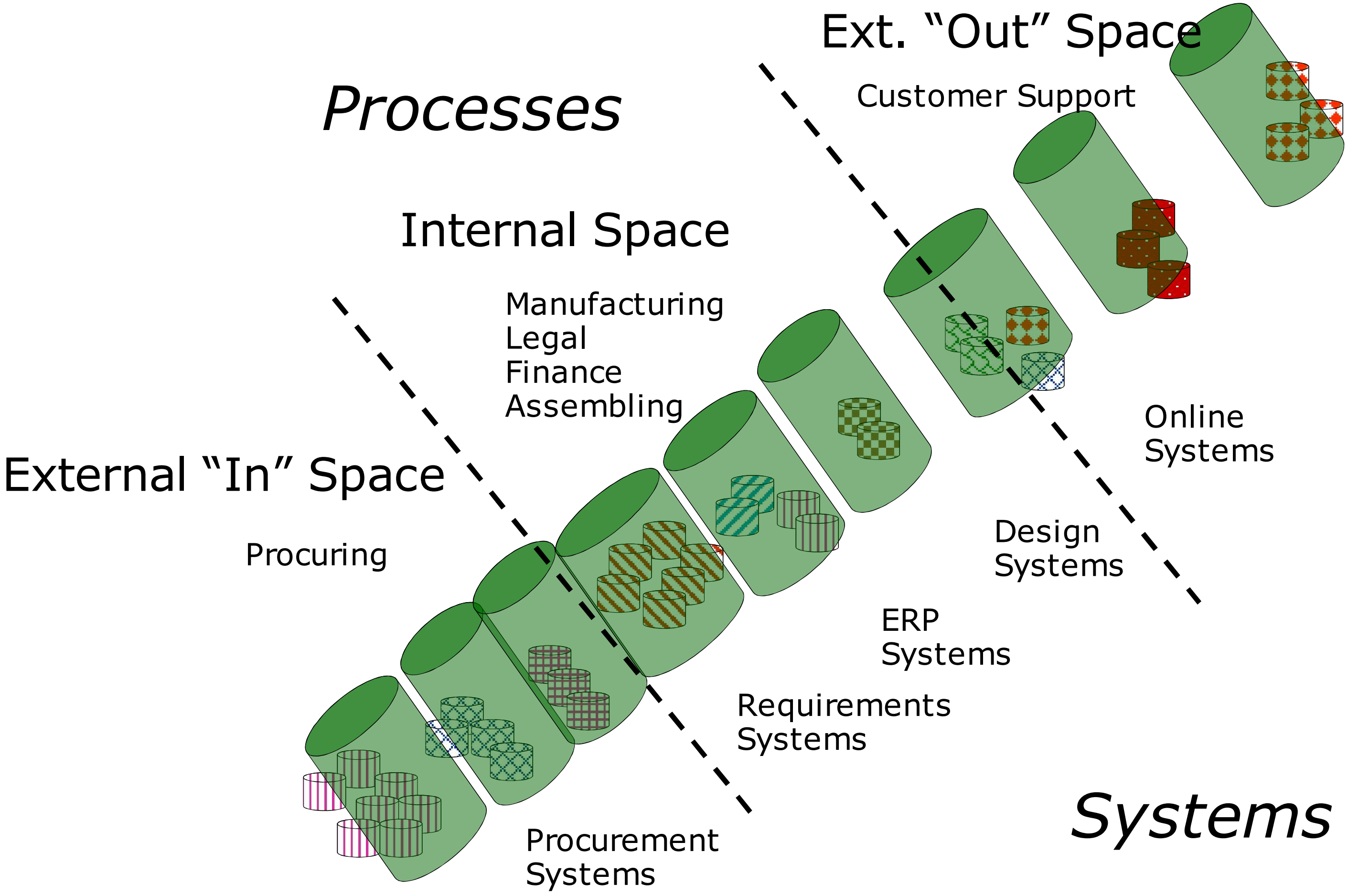
Procurement Systems

Systems

Actually Want This…



But Have This



Processes

Ext. “Out” Space

Customer Support

Internal Space

Manufacturing
Legal
Finance
Assembling

External “In” Space

Procuring

Online
Systems

Design
Systems

ERP
Systems

Requirements
Systems

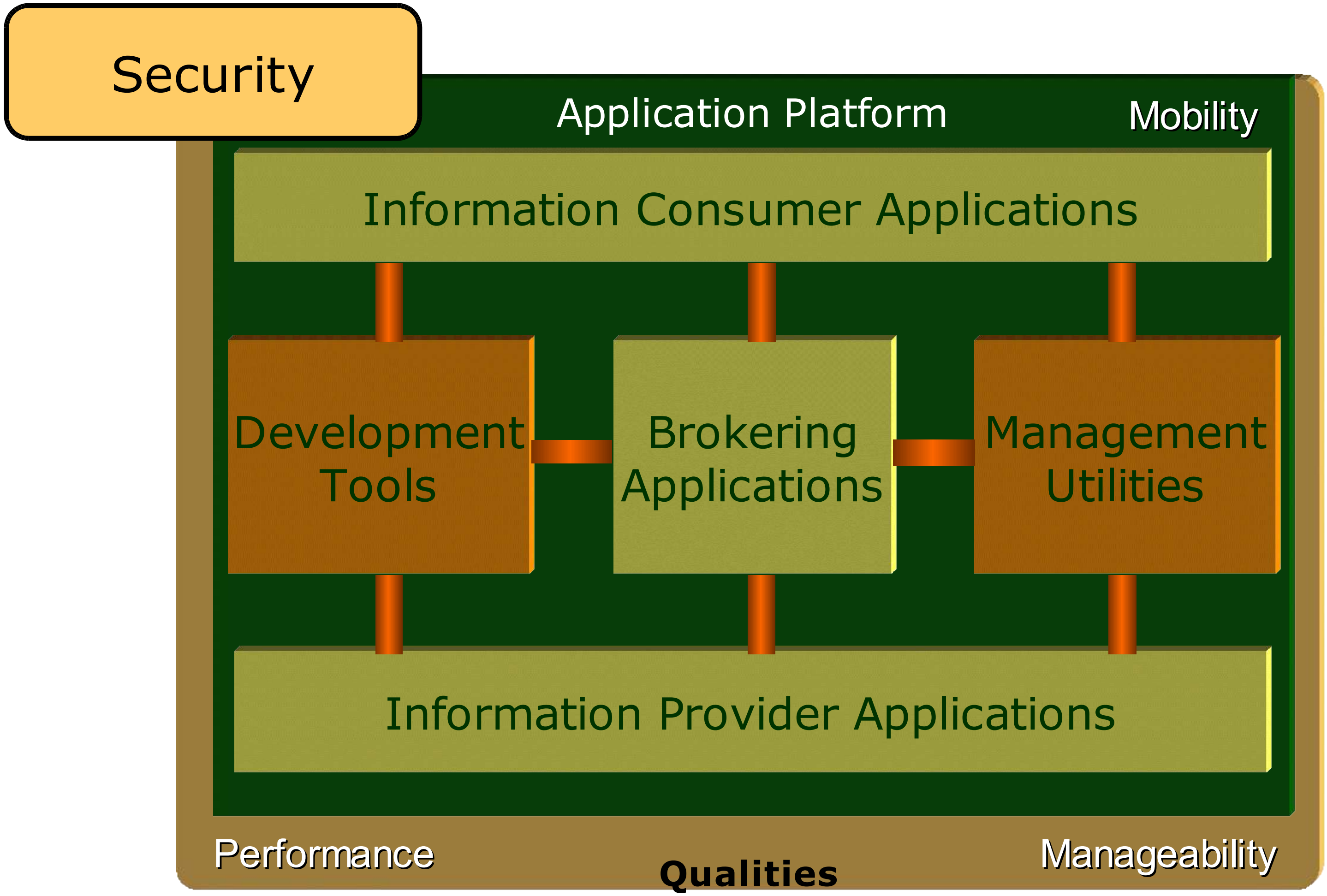
Procurement
Systems

Systems

Vision

- **Boundaryless Information Flow**™
  achieved through global interoperability
  in a ***secure***, reliable and timely manner.
- Security is important to this vision – it is a "quality" that has to be in place throughout the environment.

Boundaryless Information Flow™ - Technical Taxonomy



Mission

To drive the creation of **Boundaryless Information Flow**™ by:

- Working with **customers** to capture, understand and address current and emerging requirements, establish policies and share best practices;
- Working with **suppliers**, **consortia** and **standards bodies** to develop consensus and facilitate interoperability, to evolve and integrate open specifications and open source technologies;
- Offering a comprehensive set of **services** to enhance the operational efficiency of consortia; and
- Developing and operating the industry's premier **certification service** and encouraging procurement of certified products.

Security Forum Vision

- Security is about achieving business objectives within applicable law and policy
  - Managing risk
  - Not merely preventing bad things
- Security creates protected systems with controlled perimeters
  - A controlled perimeter is “boundaryless” where (and only where) it needs to be
- Security design is necessarily pervasive

Security Forum - Mission

- Bridge the gap between business objectives and traditional "security" technology
  - Identification of gaps in both understanding and technology
  - Better understanding between buyers and suppliers of IT
  - Positioning within the Security Life Cycle – Concept, Requirements, H-L Design, L-L Design, Implementation, Integration, Test & Certification, Operation & Maintenance, Obsolescence & Succession.
- Develop collaborative activities with other consortia to
  - avoid duplication of effort
  - leverage best-of-breed solutions
- A big part of the problem is just *defining* exactly what problem we're solving

Advancing the Vision: Architecture

- No one security technology just “solves” a business security problem
- Real solutions are composed of multiple technical elements working in concert to achieve a business objective
- Little guidance exists to help architects analyze security problems and choose solution elements – our “Reference Architecture” and “Family of Architectures” concept addresses the gap
- Develop Reference Architecture, and Family of Architectures - the “Security Clan” within the family

Advancing the Vision: Design Patterns

- Certain design elements are common to many security problems
- In software engineering, common elements are sometimes described as “design patterns”
  - Based on Christopher Alexander’s concept – A Timeless Way of Building
  - Following Gang-of-Four seminal work: Gamma, Helm, Johnson, Vlissides
- Security Forum is about to publish its catalog of “security design patterns”

Advancing the Vision: Education

- *Manager's Guide to Information Security*
  - Relating security to business objectives
  - Written in plain English
  - Helping business people relate to what information security can do (and what it can't do)
- *Intrusion Attack & Response* - white paper & video:
  - Illustrating a security incident in multiple simultaneous contexts: operations, financial, legal, PR, technical
- *Manager's Guide to Data Privacy*
- Under way - Secure Messaging, PKI in Practice, Identity & Authentication, Security Managed Risk
- Security culture – do right because it's the right thing to do

Advancing the Vision: Risk Management

- Management of Risk is the business driver for information security technologists to produce solutions
- Collaborate with experts on Active Loss Prevention:
  - Integrating business, legal, insurance, and audit aspects of information security
  - Measuring/quantifying IT-related risk and effectiveness of security solutions
  - Developing Trust Services to support growth of e-Business

Managing Risk

- Risk is not necessarily a bad thing
  - Every business transaction carries risk
- Some ways to deal with risk
  - Disclaim it
  - Transfer it by contract
  - Hedge against it
  - Insure against it
  - Accept it
- Security helps you manage risk by design
- Active Loss Prevention provides a framework for mitigating risk and loss in the context of law, insurance, audit

Advancing the Vision: Security for Industry Sectors

- Collaborate with experts from industrial sectors on information security requirements and solutions:
  - Ongoing discussions with the bio-technical industry – the Interoperable Informatics Infrastructure Consortium (I3C)
  - They are grappling with specific (yet common) problems in security, so provide a good source of vertical industry case studies for security work:
    - Patient record security and privacy
    - Regulatory requirements for audit (Sarbanes-Oxley) and electronic records & digital signatures – US FDA regulation 21 CFR Part 11
    - Secure messaging
- Leverage solutions into open systems standards

So what is the Security Forum doing?

- Technical Guide to Security Design Patterns Working on Architectures for Security within context of Boundaryless Information Flow
- Identity Management:
  - Business Scenario to verify real requirements
  - Roadmap White paper
  - Implementations Catalog
  - Business Perspectives –architectural principles models
  - Collaboration with Securities Industry Middleware Council (SIMC)

More on what we're doing (2)

- Managers Guides:
  - MGIS published
  - Privacy Guide published
  - Guide to Identity & Authentication
  - Guide to PKI in Practice
  - Guide to Security Managed Risk
  - Guide to Secure Messaging
- Risk Vocabulary project well advanced:
  - Pilot Seminar in June – London
  - Plan formal launch of Risk Vocabulary in q403

More on what we’re doing (3)

- ALPINE (Active Loss Prevention for ICT eNabled Enterprise) project, supported by EU funding:
  - Security Policy Management for Small & Medium Enterprises
  - Liability in Mobile Transactions
  - Trust Services Mapping
  - Trustmarks
  - Dependable Embedded Systems
  - Roadmap

Future project proposals

- Selected proposals for potential new technical work projects:
  - Identity Theft
  - PKI Trust Models
  - Role-Based Access Control
  - Perimeter security outside the Desktop – Securing Data
  - Additional security implications in grid computing - e.g. identity in virtual environments, scaling, workflow, data security, business implications.
- What are your requirements?…Suggestions please

Why we should work together

- ❑ Some of your problems aren't unique
  - Some have already been solved - we'd like to share what we've learned
  - Some haven't
- ❑ For your unique problems our approaches may help
- ❑ Your requirements may be bellwethers in other Open Group member industries
- ❑ Regulatory concerns affect all of us if not now, in the future
- ❑ We can help with jump-starting your processes

The future …

- The Open Group's Security Forum welcomes anyone who wants to work with seriously capable security experts on hard problems that really matter:
  - Business requirements analysis
  - Active Loss Prevention – Risk Management
  - Technology solutions to real problems
- Contact Ian Dobson – i.dobson@opengroup.org

Thank You