Loblaw®

COMPANIES LIMITED

Information Security, Privacy and Compliance

Building Reference Security Architecture

Bob Steadman, Sr. Director

Predrag Zivic, Sr. Security Architect

Information Security

- “Too many organizations still consider their information security as an administrative cost, something that is done in the back office and in the nature of an insurance policy.
- Information security is the way we ensure the integrity of our data and protect the privacy and confidentiality of our competitive information and the data entrusted to us by our customers and employees.
- Information security is truly everybody’s business. As our customers often interface with us through our computer systems, information security is part and parcel of the goods and services that we offer.”

Jim Gaston

Information Security – Strategies for successful management

Loblaw Overview

- Loblaw Companies Limited (“Loblaw”) is Canada's largest food distributor and a leading provider of general merchandise products, drugstore, and, financial products and services
- *President's Choice Financial* services offer core banking, a popular MasterCard®, *PC Financial* auto, home, travel and pet insurance as well as the *PC* Points loyalty program

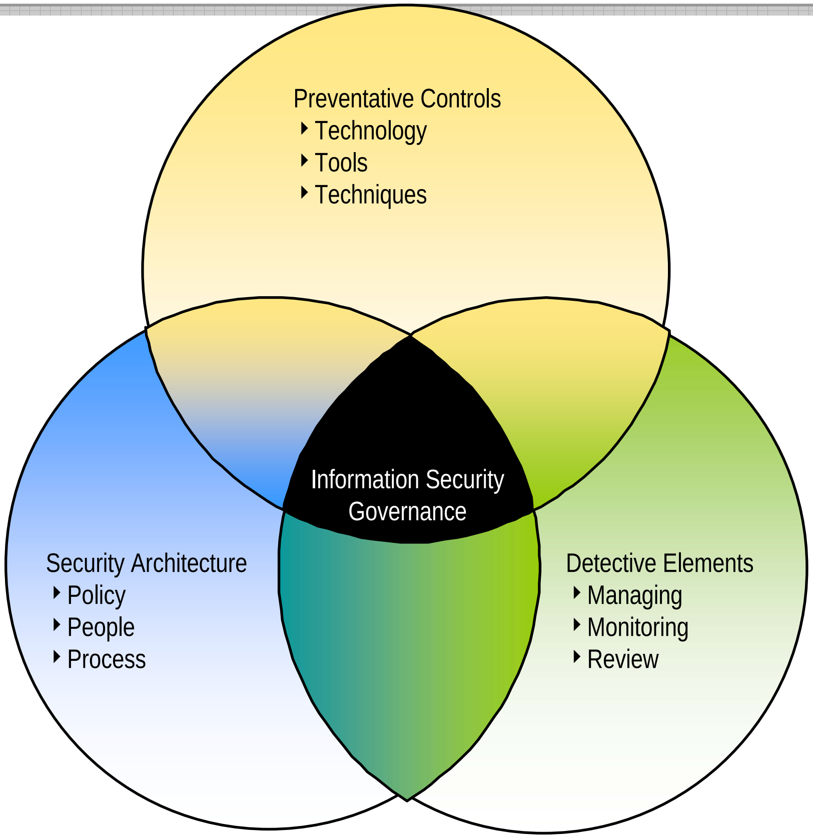
Loblaw Overview

- Over 134,000 full and part-time colleagues across Canada in over 1,000 stores
- Number of ongoing initiatives
  - ERP (SAP) implementation
  - Revamp of Supply Chain
    - Warehouse
    - Transportation
  - And many more

OVERVIEW OF INFORMATION SECURITY STRATEGY

Information Security's Three Spheres of Influence

Guided by our Three Spheres of Influence for Risk and Reward, we have been able to identify, define, and draft a “roadmap” for how information security should be implemented within the Loblaw operational environment.



Benefits of Information Security's Information Security Strategy

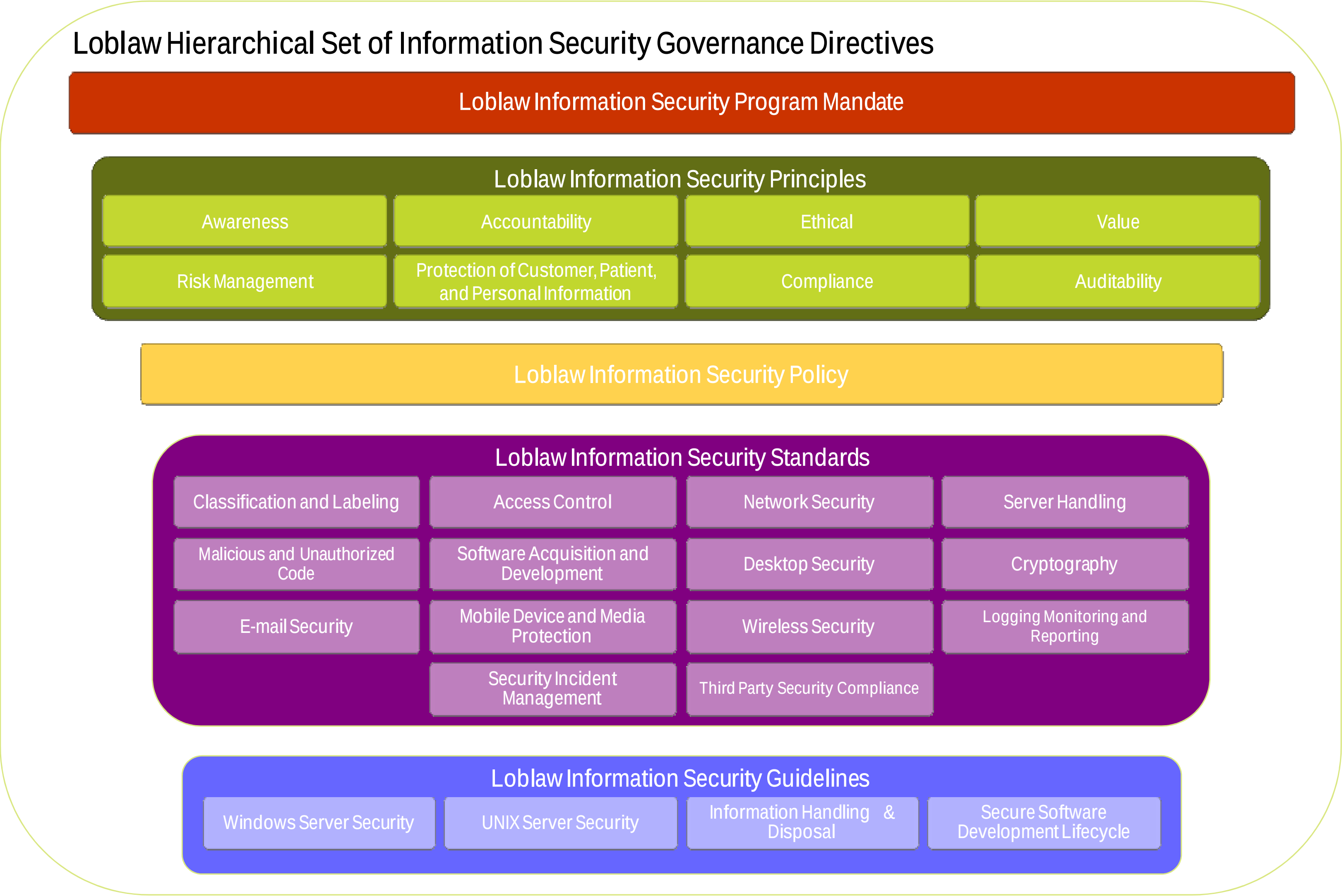
- Understanding our information security drivers by translating them into business requirements.
- Aligning the information security strategic plan with the business’ vision, mission and tolerance for risk.
- Developing strategies to align information security with Loblaw’s IT, business, and corporate strategies and initiatives.
- Establishing accountability, authority and responsibility for information security across Loblaw.
- Communicating and encouraging consistent and appropriate security decisions and investments.
- Monitoring the threat landscape and aligning the information security initiatives and plans to proactively address the threats.
- Integrating security into core business management processes.
- Defining information security measurement requirements on the state and success of the information security program to provide real-time indications of the health of information security.

ISPC Principles

- Guiding Principles:
  - Awareness of information handling and protection responsibilities;
  - Compliance with information security controls;
  - Ethics as an integral component of information handling and protection;
  - Appropriately protect information as a strategic resource that has value;
  - Information security controls are cost-effective and risk-responsive;
  - Protection of Customer, Patient and Personal Information;
  - Compliance with Laws and Regulations; and
  - Maintain auditability of decisions and actions.

- Technical Principles:
  - Access based on least privilege; and
  - Defence in depth approach to information security.

SECURITY DIRECTIVES STRUCTURE



Loblaw Hierarchical Set of Information Security Governance Directives

Loblaw Information Security Program Mandate

Loblaw Information Security Principles

- Awareness
- Accountability
- Ethical
- Value
- Risk Management
- Protection of Customer, Patient, and Personal Information
- Compliance
- Auditability

Loblaw Information Security Policy

Loblaw Information Security Standards

- Classification and Labeling
- Access Control
- Network Security
- Server Handling
- Malicious and Unauthorized Code
- Software Acquisition and Development
- Desktop Security
- Cryptography
- E-mail Security
- Mobile Device and Media Protection
- Wireless Security
- Logging Monitoring and Reporting
- Security Incident Management
- Third Party Security Compliance

Loblaw Information Security Guidelines

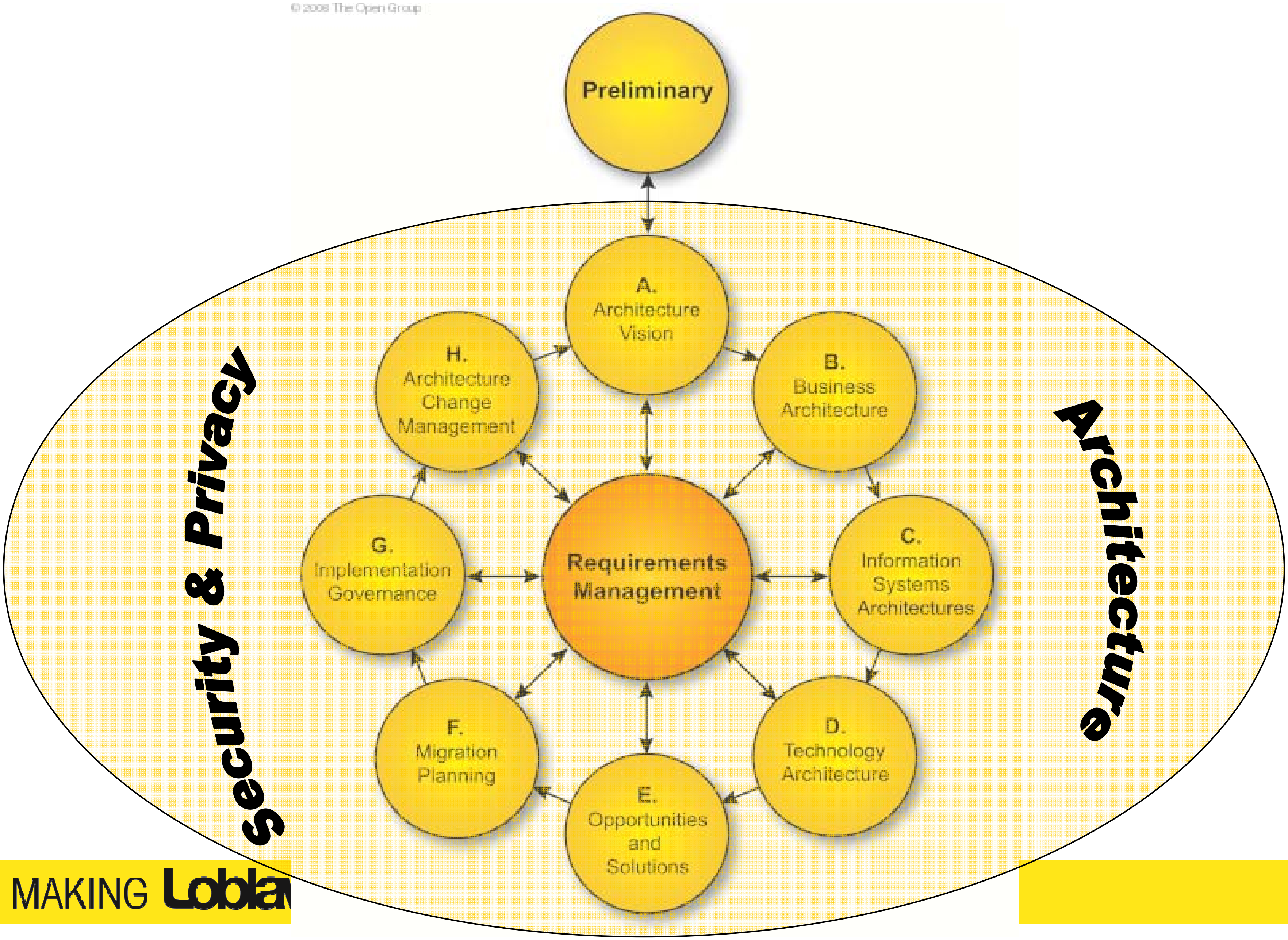
- Windows Server Security
- UNIX Server Security
- Information Handling & Disposal
- Secure Software Development Lifecycle

In efforts to establish the fundamental building blocks required for the information security program, Loblaw constituted a hierarchical directives structure that links the information security policy with the adopted principles and in turn with the supporting standards and guidelines.

The Security Balance

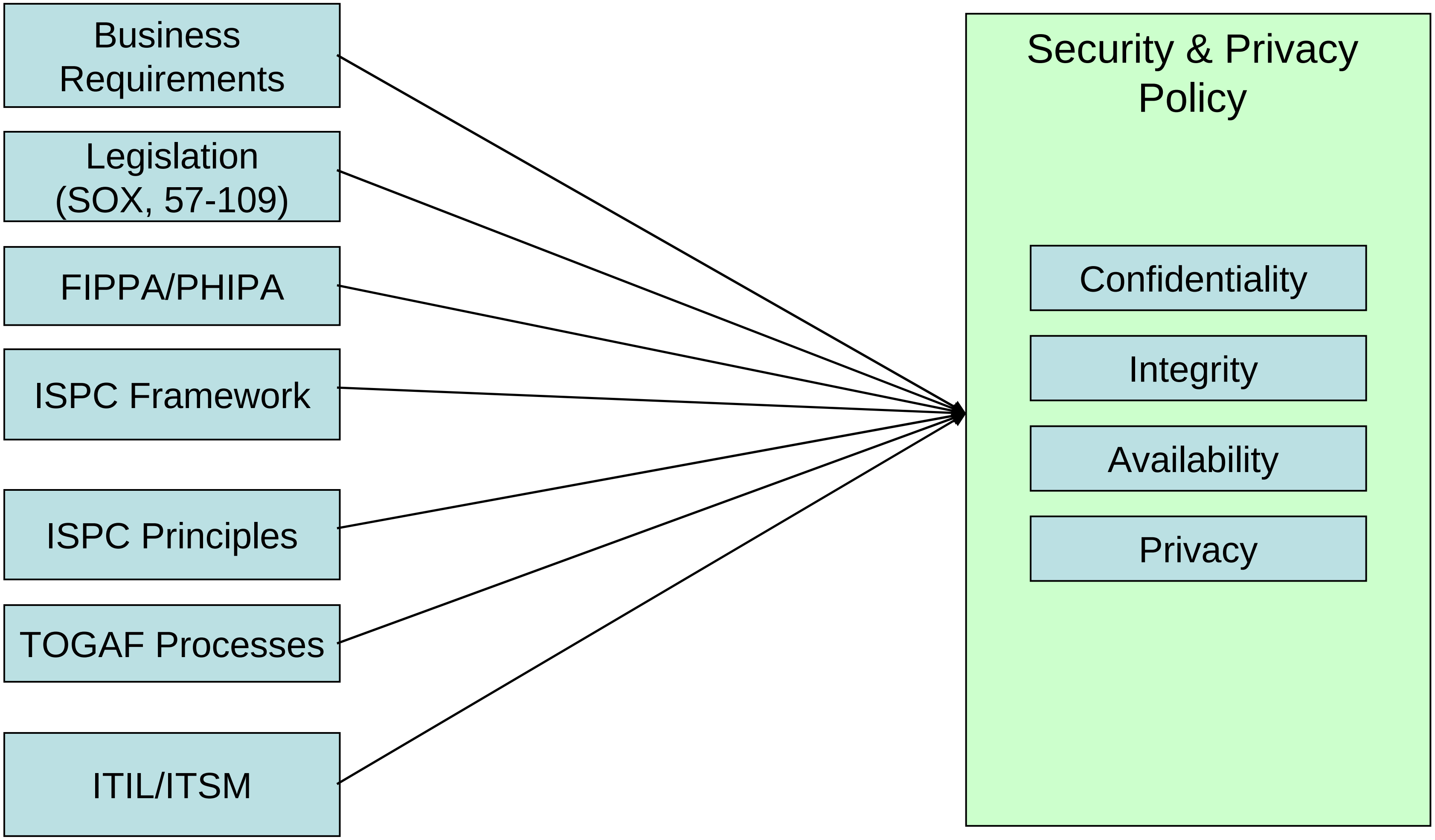
- Security is balancing act between ease of access to information and protecting information from increasing threats
- Not possible to make information processing resources available without restriction and still be able to offer reasonable protection of their integrity and trustworthiness.
- To maintain some feasible level of security, some balance must be found between two positions.
- Must consider the organization’s appetite for risk when assessing where the “appropriate” balance lies.

TOGAF & ISPC Architecture


© 2008 The Open Group

Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management
Security & Privacy
Architecture

ISPC Contextual Architecture



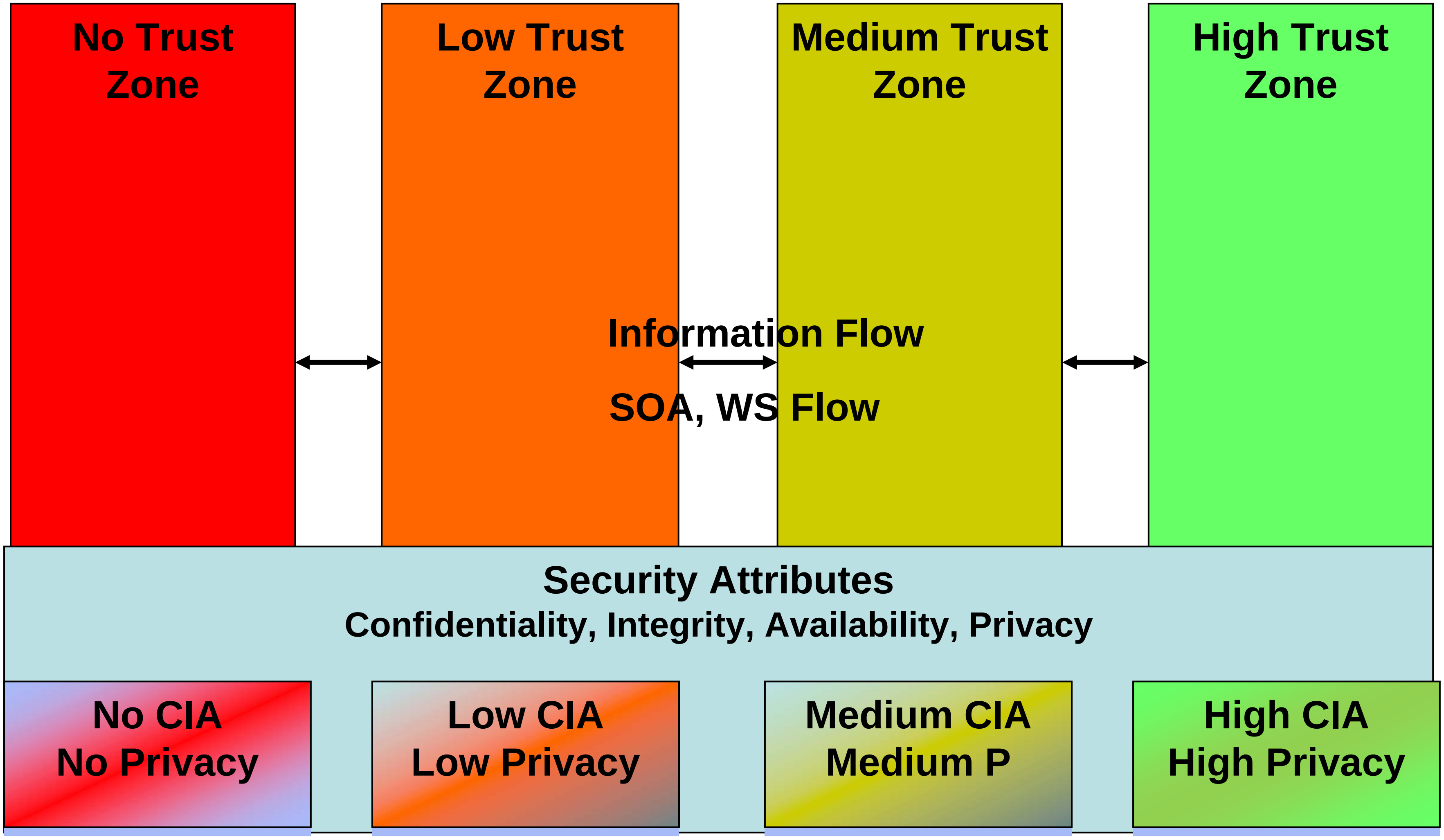
ISPC Architecture Baseline

- Definition of security attributes
  - Confidentiality, Integrity, Availability & Privacy

CONFIDENTIALITY	INTEGRITY	AVAILABILITY	PRIVACY
Restricted	High	High	High
Confidential	Medium	Medium	Medium
Internal	Low	Low	Low
Public	No	No	No

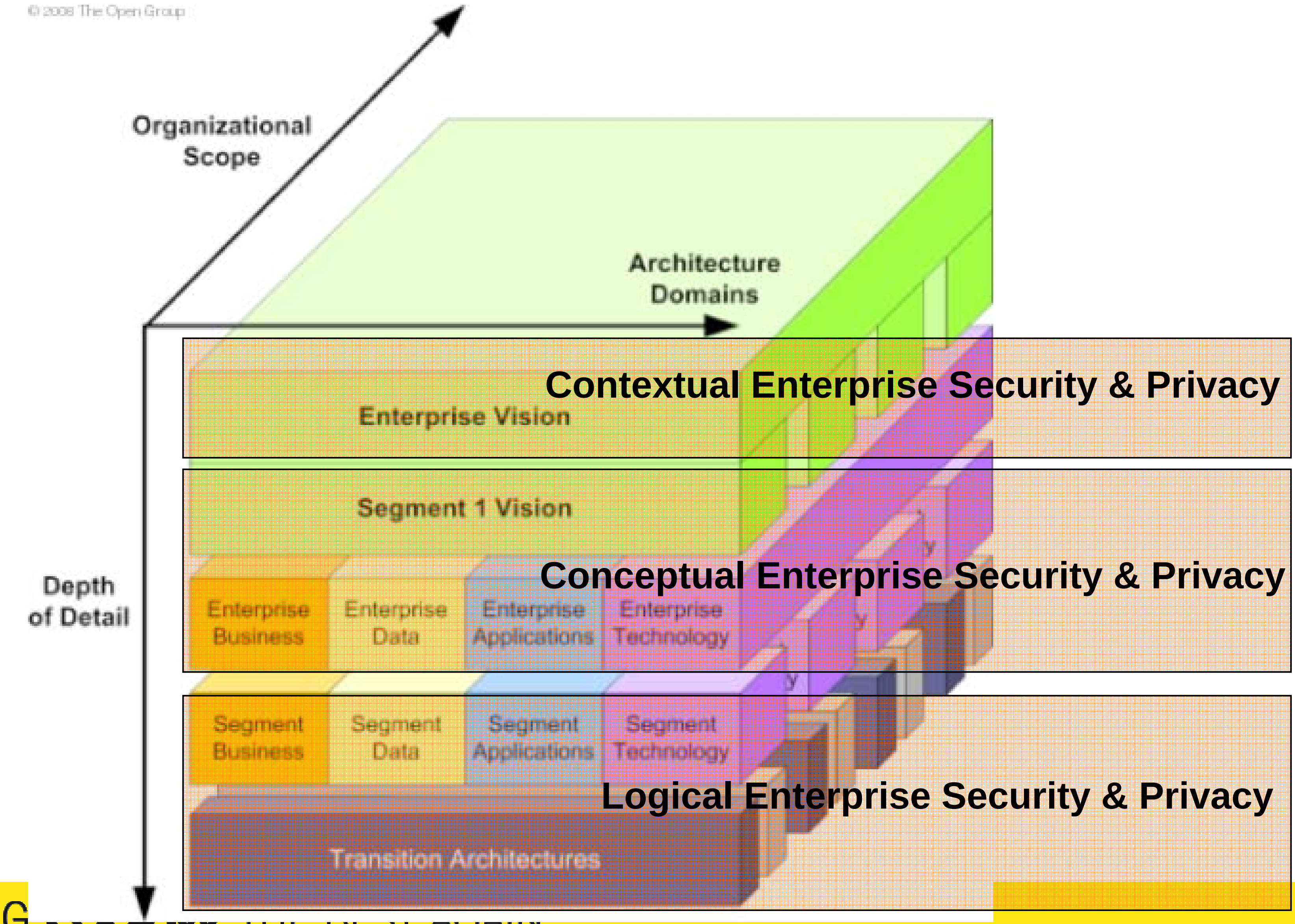
- Security Operations must support defined ISPC attributes

ISPC Conceptual Architecture



Conceptual Trust Tiers with Security Attributes Applied

TOGAF & ISPC Architecture



Contextual Enterprise Security & Privacy

Conceptual Enterprise Security & Privacy

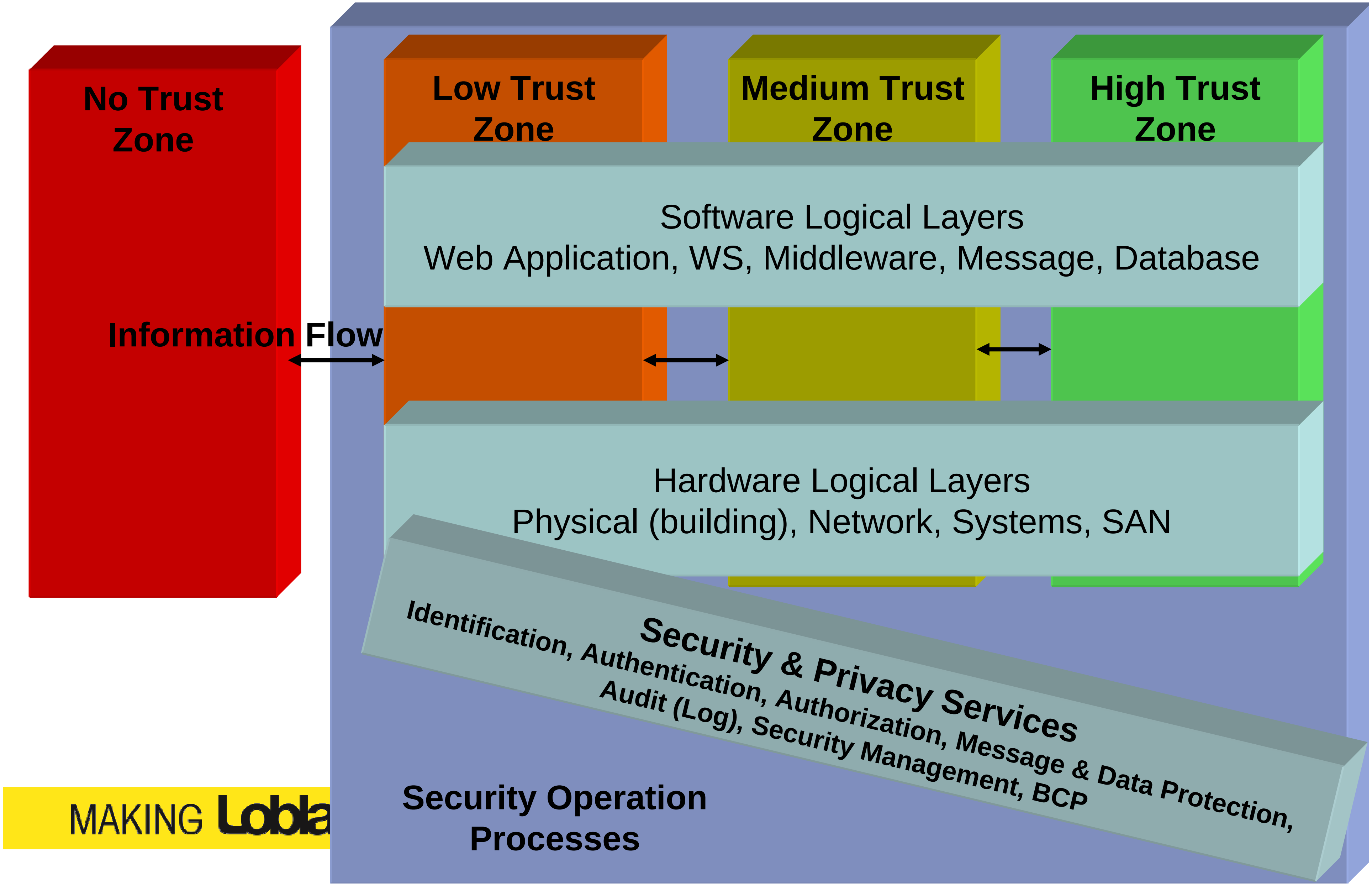
Logical Enterprise Security & Privacy

ISPC Logical Services

Security & Privacy Attribute	**Logical Security Service**
Confidentiality	Identification, Authentication, Authorization, Encryption. Security Management
Integrity	Authentication, Authorization, Digital Sign, Hashing, Data Input Validation., Content Inspection, Security Management
Availability	Clustering, Load Balancing, High Availability, Security Management, BCP
Privacy	Consent, Authorization, Anonymous /Pseudo, Digital Sign, Encryption, Audit Log
Security Operation Processes (Operational Services)	Vulnerability Management, Incident Management, Audit Log Management (Event Management), User Administration, Change Management

- Hash/sign, encryption, content inspection, validation, anonymous, pseudo, consent are going to be referred to “message & data protection” controls hereinafter

ISPC Logical Architecture



No Trust Zone

Low Trust Zone

Medium Trust Zone

High Trust Zone

Software Logical Layers
Web Application, WS, Middleware, Message, Database

Information Flow

Hardware Logical Layers
Physical (building), Network, Systems, SAN

Security & Privacy Services
Identification, Authentication, Authorization, Message & Data Protection,
Audit (Log), Security Management, BCP

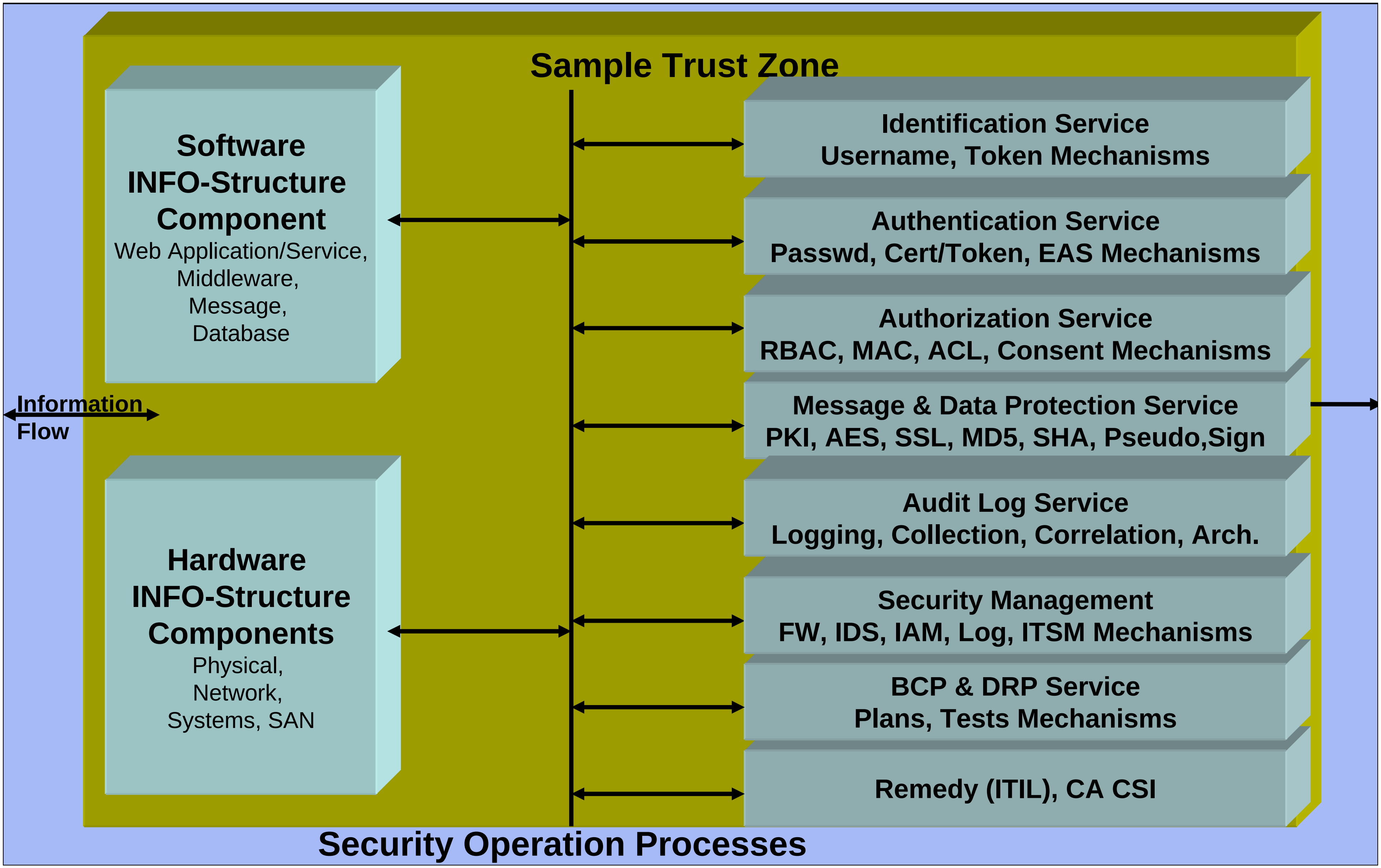
Security Operation Processes

MAKING Lobla

ISPC Physical Services

Logical Security Service	**Physical Security Mechanism**
Identification	Username, Token/Card, Biometric
Authentication	Password, Token/Card, Biometric, EAS, OTP, PKI, Combination of Mechanisms
Authorization	MAC, RBAC, ACL (FW), Consent, DAC
Message and Data Protection	PKI, SSL, AES, DES (encryption), Anonymous, Pseudo Algorithm, MD5, SHA-1 (hashing), Scrambling, Proxy, Application firewall, Field level checks, Anti-virus/worm/trojan, IPS
Audit Log Service	Action log, error log, message log, event log, transaction log collection & correlation,
Security Management	Mgmt of FW, IDS, HIDS, IAM, Security Awareness, Security Policy, ITSM processes
BCP & DRP	BIA, Documented Plans and Tests
Vulner. Mgmt, Incident Mgmt, Change Mgmt	ITIL – Remedy, Scanners
User Administration	IAM/CSI toolset

ISPC Physical Architecture (per zone)



Sample Trust Zone

Software INFO-Structure Component
Web Application/Service,
Middleware,
Message,
Database

Hardware INFO-Structure Components
Physical,
Network,
Systems, SAN

Information Flow

Identification Service
Username, Token Mechanisms

Authentication Service
Passwd, Cert/Token, EAS Mechanisms

Authorization Service
RBAC, MAC, ACL, Consent Mechanisms

Message & Data Protection Service
PKI, AES, SSL, MD5, SHA, Pseudo,Sign

Audit Log Service
Logging, Collection, Correlation, Arch.

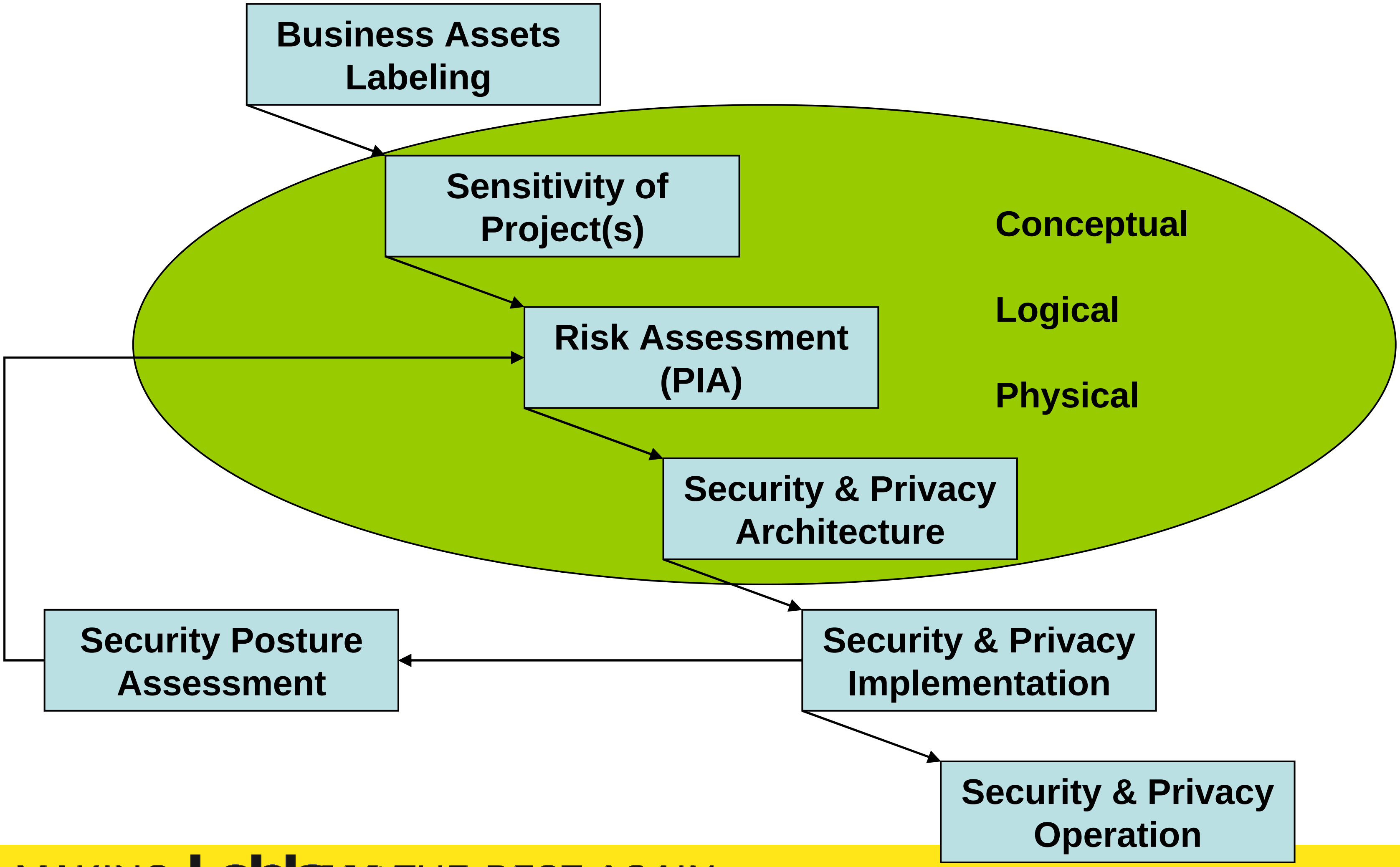
Security Management
FW, IDS, IAM, Log, ITSM Mechanisms

BCP & DRP Service
Plans, Tests Mechanisms

Remedy (ITIL), CA CSI

Security Operation Processes

ISPC Architecture Methodology



Business Assets Labeling
Sensitivity of Project(s)
Risk Assessment (PIA)
Security & Privacy Architecture
Security & Privacy Implementation
Security & Privacy Operation
Security Posture Assessment
Conceptual
Logical
Physical

ISPC Reference Security Architecture

Questions?

Thank you!