



Microsoft
GOLD CERTIFIED
Partner

Advanced Infrastructure Solutions
Networking Infrastructure Solutions

Avient Solutions Group Inc.

Developing the Corporate Security Architecture

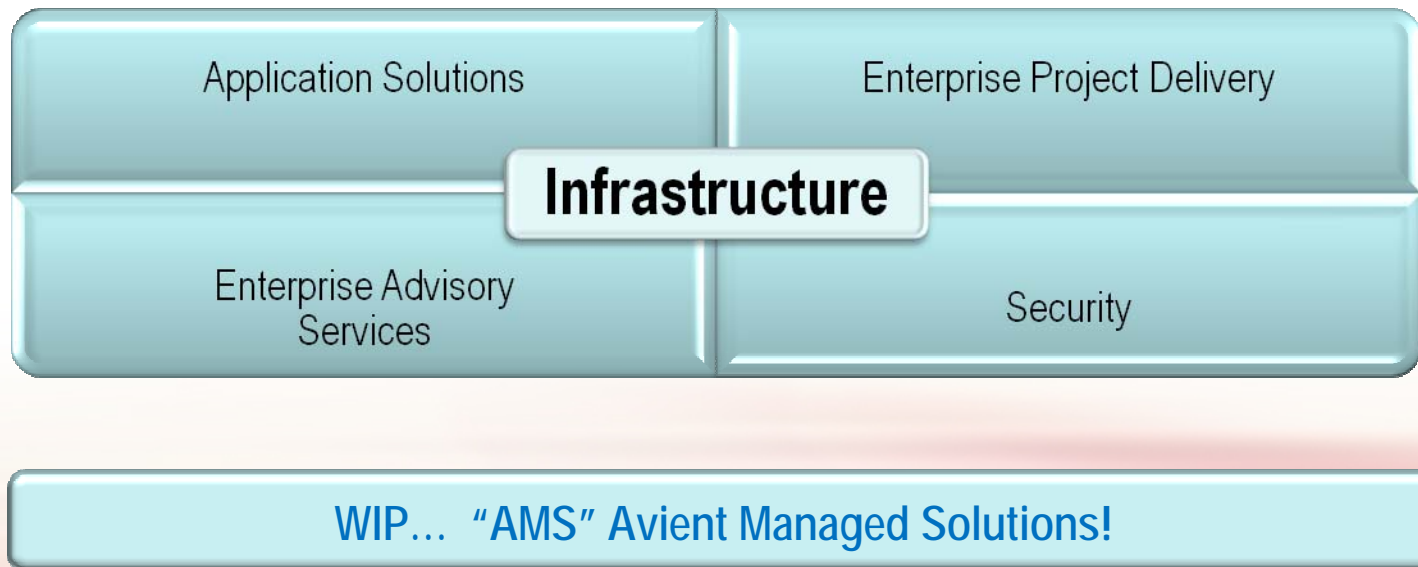


www.avient.ca

Alex Woda
July 22, 2009

Avient Solutions Group

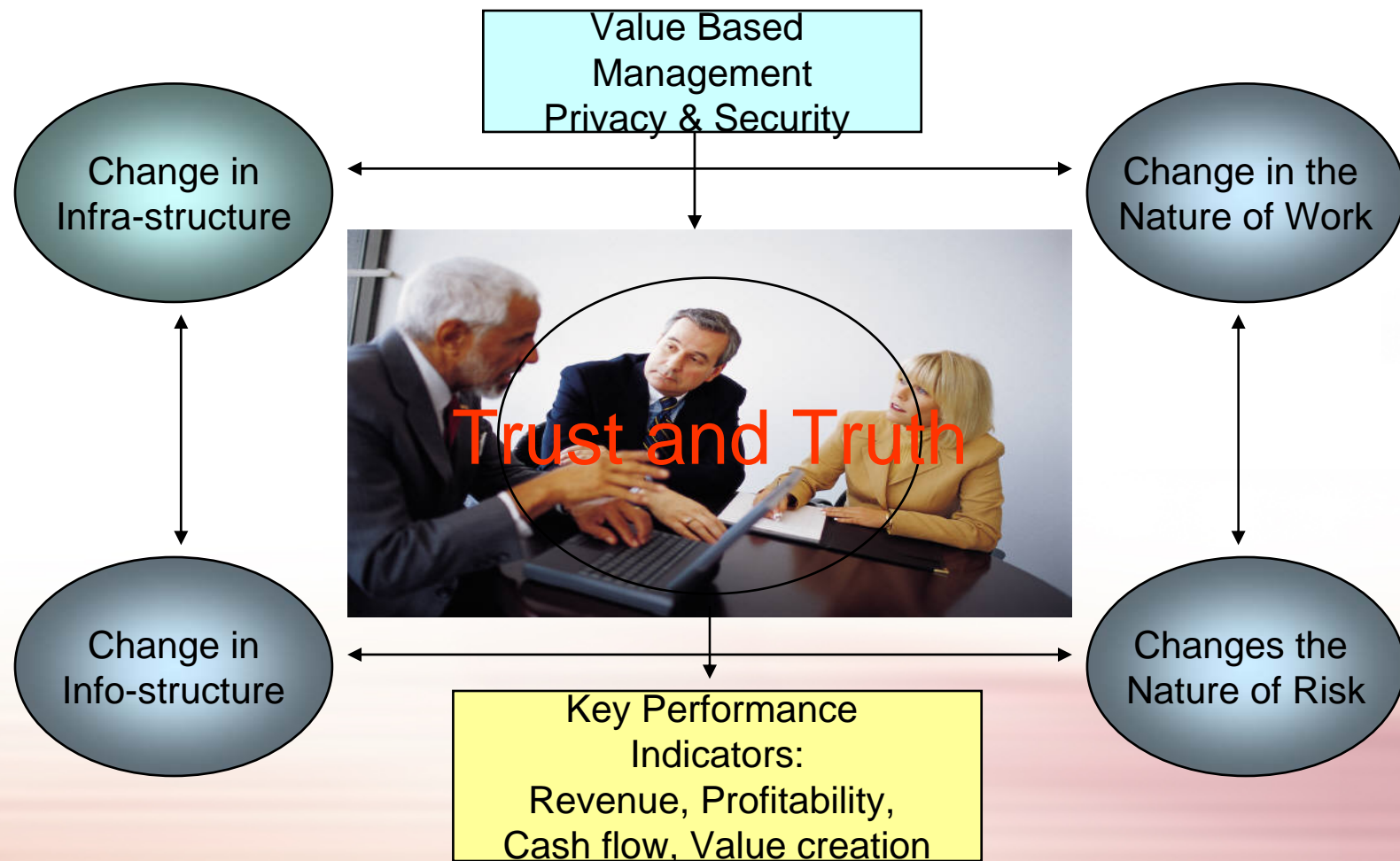
Avient Solutions Group is based in Markham and is a professional services firm specializing in infrastructure, architecture, applications security and project management.



Key Points

- Why do we need a Corporate security architecture?
- Enterprise Architecture Frameworks
- Examples of security architecture
- Designing and Implementing a Security Architecture
- How to assess the security architecture

Information Security Challenge



Business Drivers

➤ Government Regulations and Audits

- Sarbanes Oxley
- Bill C-198
- PIPEDA Bill C-6

➤ Industry Security Regulations

- Payment Card Industry Data Security Standards
- Open Web Application Security Project (OWASP)
- ISO 17799, ISO 27002

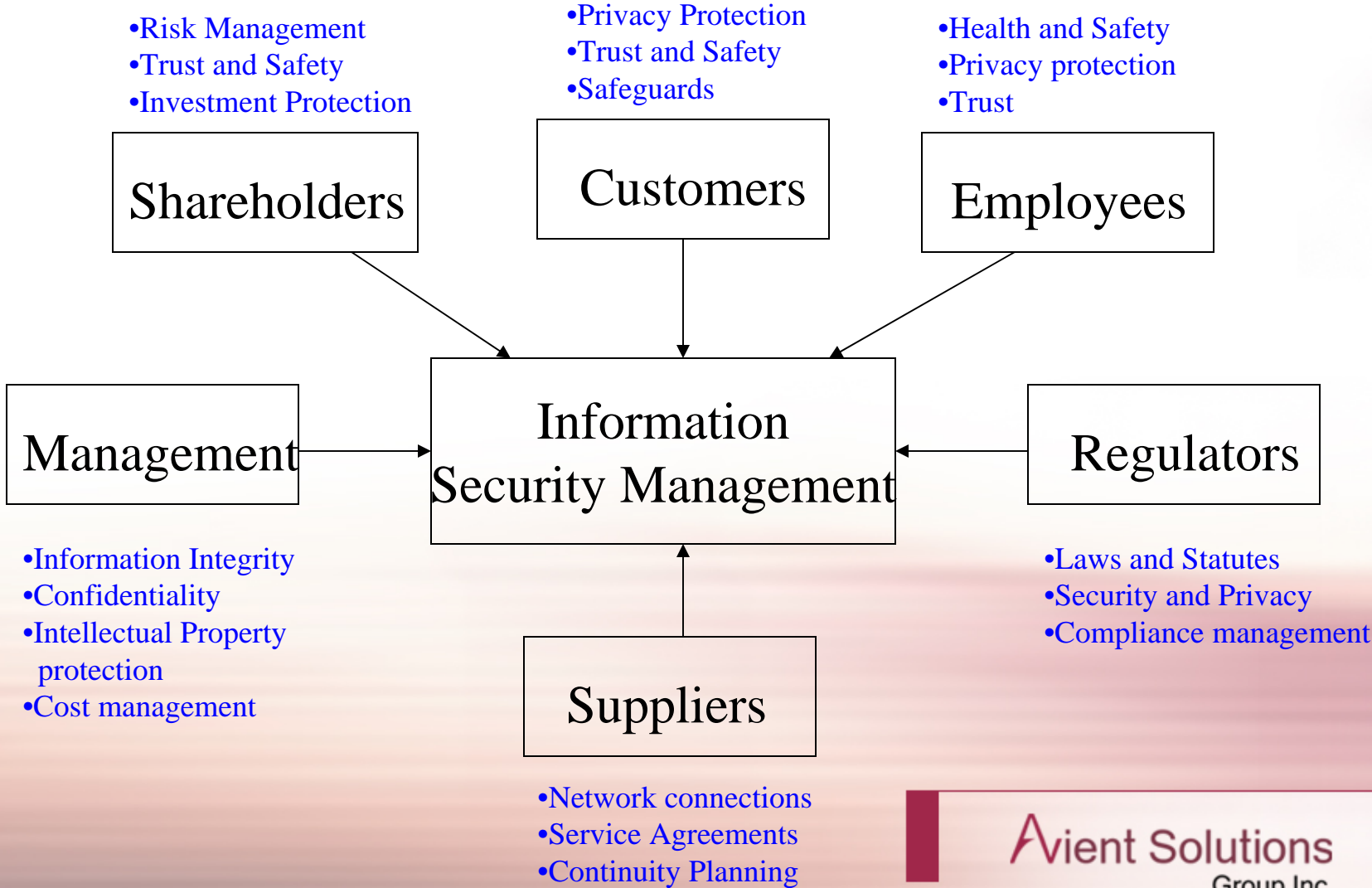
➤ Business Relationships

- Outsourced services
- Supply chain integration
- Remote access to internal systems

Technology Drivers

- **New Technologies and Infrastructure**
 - Purchased applications
 - Integration of systems
- **New information collection and storage**
 - Sensitive data and encryption
 - Data leakage
- **Cloud Computing**
 - Web based access to applications
 - Third party control
- **Malicious code**
 - Trojans, viruses
 - Vulnerabilities in software
- **External attack methods**
 - Cross site scripting
 - Buffer overflows
 - Memory parsers

Information Security Stakeholders



Enterprise Architecture Frameworks

- **TOGAF Enterprise Architecture Framework**
 - Integration of security into different domains
 - Architecture development method available

- **Zachman Enterprise Architecture Framework**
 - Set of models to represent WHAT, HOW and WHERE
 - Complete the design with WHO, WHEN and WHY
 - Systematic description of business models, processes, data requirements
 - Set of standard artifacts to foster communication and collaboration
 - Security Architecture called SABSA

- **Vendor Defined Architecture**
 - IBM Architecture Methods

Security Architecture Frameworks

- TOGAF Version 9
- SABSA - Sherwood
- ISO 17799 security framework
- Agile Security Strategies
- ISO 13335 - security practices
- ISO 7498-2
- NSA standards - Gold for Win2K
- Cisco SAFE

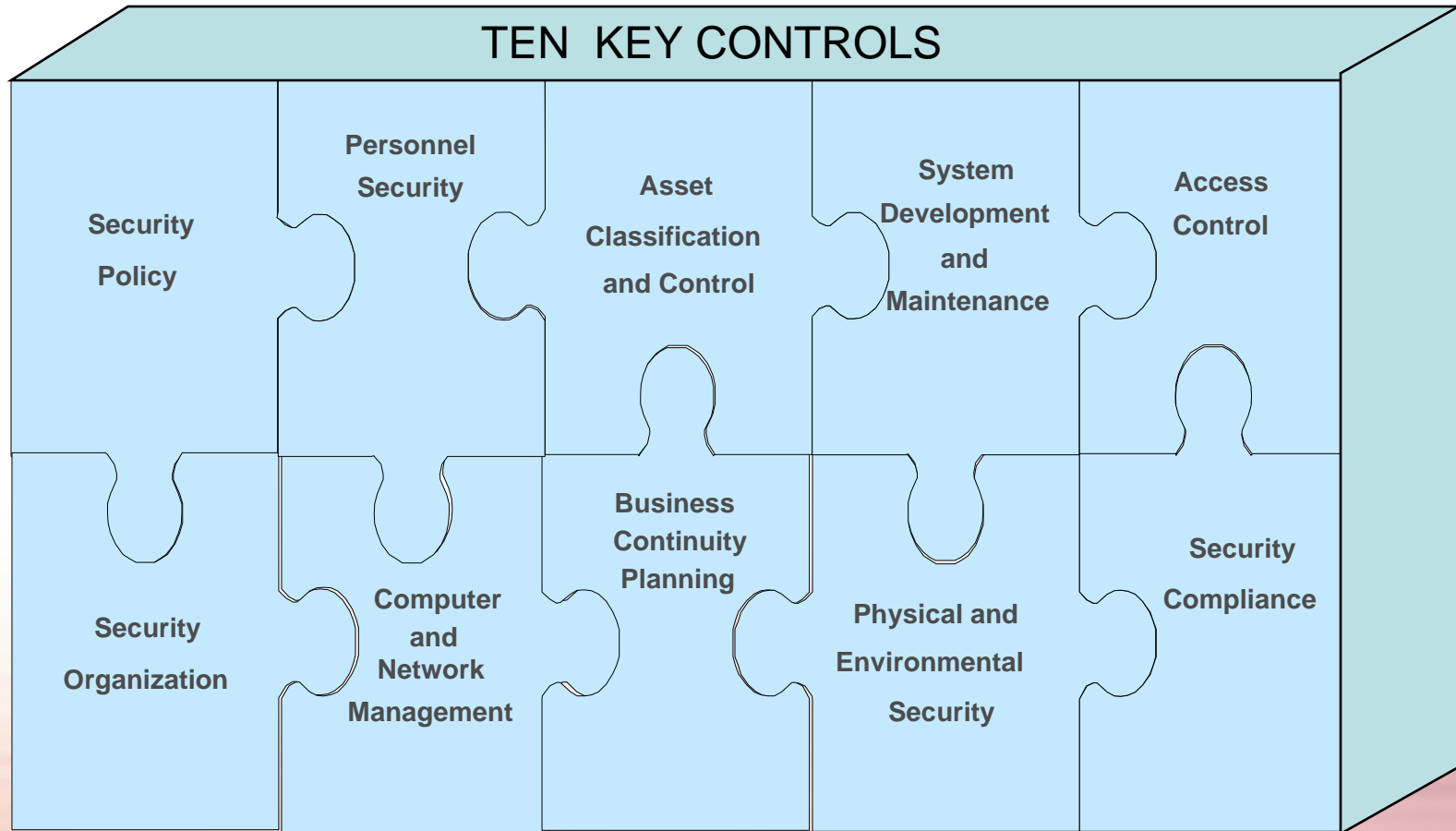
TOGAF and Security

- Security domain is pervasive across the other domains
- Areas of focus:
 - Authentication
 - Authorization
 - Audit
 - Assurance
 - Availability
 - Asset Protection
 - Administration
 - Risk Management

Security as part of Enterprise Architecture

- **Integrated with Enterprise Architecture**
 - Business architecture
 - Information architecture
 - Application architecture
 - Technology architecture
 - Security architecture
- **Security participation in project teams**
- **Creation of security analysis and design plans for each significant project**

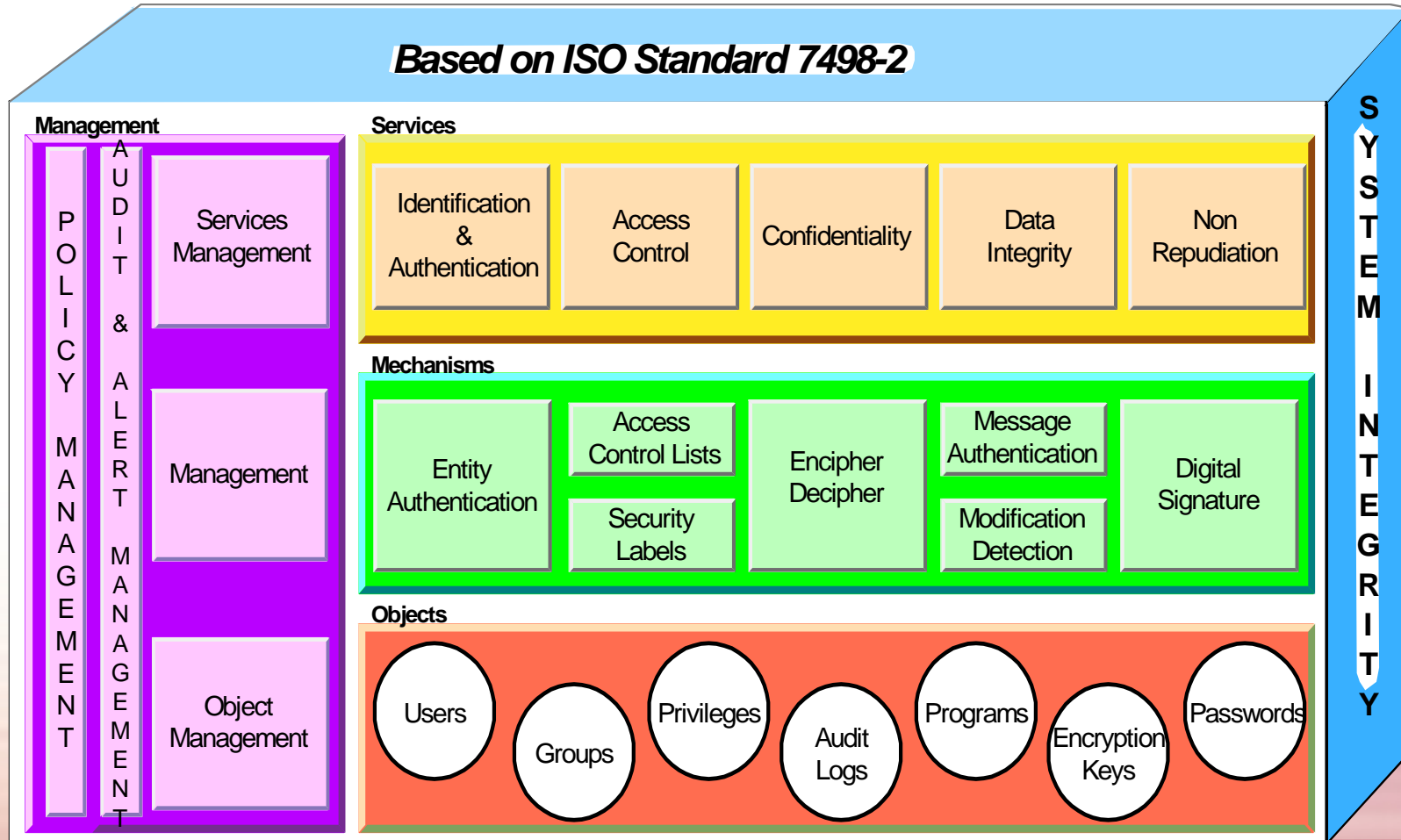
Conceptual Security Framework









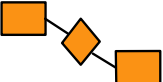
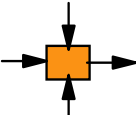
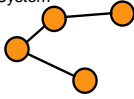
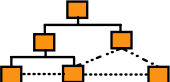
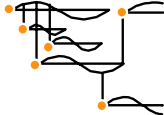
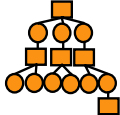
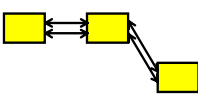
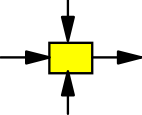
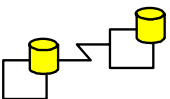
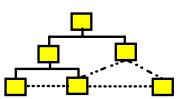
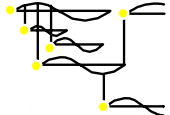
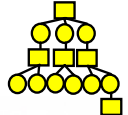
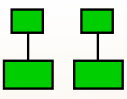
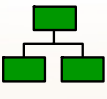
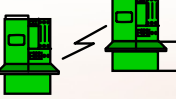
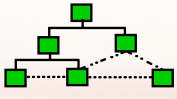
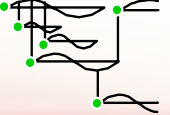
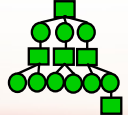






1. Based on British Standard 7799: "Code of Practice for Information Security Management" and NIST

Example of a Security Architecture Model

IBM has a model for **Security Architecture**. This is illustrated in the following diagram. The Security Services correspond to the logical Components within the IT Architecture. As such there is a natural linkage between the two Architectures.



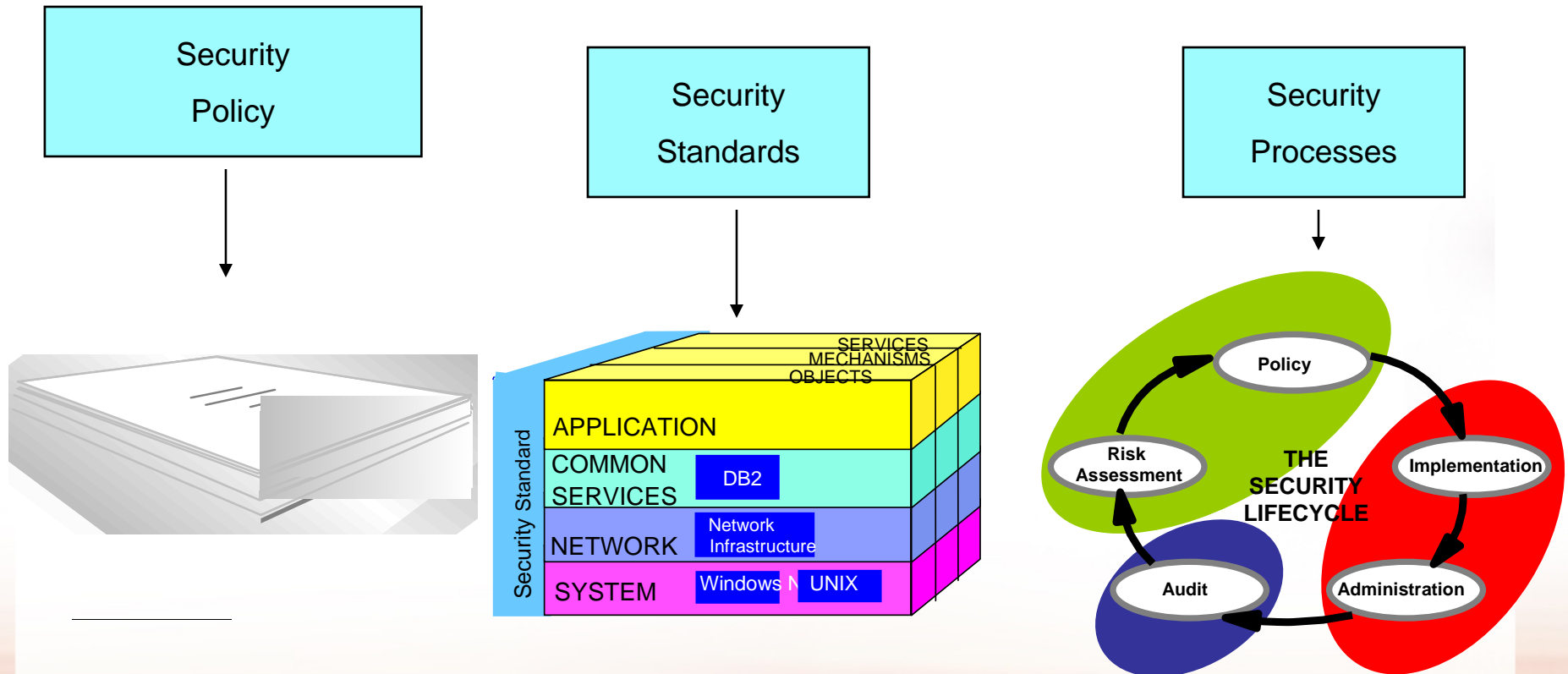
ENTERPRISE ARCHITECTURE - A FRAMEWORK TM

	DATA <i>What</i>	FUNCTION <i>How</i>	NETWORK <i>Where</i>	PEOPLE <i>Who</i>	TIME <i>When</i>	MOTIVATION <i>Why</i>	
SCOPE (CONTEXTUAL) <i>Planner</i>	List of Things Important to the Business  ENTITY = Class of Business Thing	List of Processes the Business Performs  Function = Class of Business Process	List of Locations in which the Business Operates  Node = Major Business Location	List of Organizations Important to the Business  People = Major Organizations	List of Events Significant to the Business  Time = Major Business Event	List of Business Goals/Strat  Ends/Mean=Major Bus. Goal/ Critical Success Factor	SCOPE (CONTEXTUAL) <i>Planner</i>
ENTERPRISE MODEL (CONCEPTUAL) <i>Owner</i>	e.g. Semantic Model  Ent = Business Entity ReIn = Business Relationship	e.g. Business Process Model  Proc. = Business Process I/O = Business Resources	e.g. Business Logistics System  Node = Business Location Link = Business Linkage	e.g. Work Flow Model  People = Organization Unit Work = Work Product	e.g. Master Schedule  Time = Business Event Cycle = Business Cycle	e.g. Business Plan  End = Business Objective Means = Business Strategy	ENTERPRISE MODEL (CONCEPTUAL) <i>Owner</i>
SYSTEM MODEL (LOGICAL) <i>Designer</i>	e.g. Logical Data Model  Ent = Data Entity ReIn = Data Relationship	e.g. Application Architecture  Proc. = Application Function I/O = User Views	e.g. Distributed System Architecture  Node = I/S Function (Processor, Storage, etc) Link = Line Characteristics	e.g. Human Interface Architecture  People = Role Work = Deliverable	e.g. Processing Structure  Time = System Event Cycle = Processing Cycle	e.g., Business Rule Model  End = Structural Assertion Means = Action Assertion	SYSTEM MODEL (LOGICAL) <i>Designer</i>
TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>	e.g. Physical Data Model  Ent = Segment/Table/etc. ReIn = Pointer/Key/etc.	e.g. System Design  Proc. = Computer Function I/O = Data Elements/Sets	e.g. Technology Architecture  Node = Hardware/System Software Link = Line Specifications	e.g. Presentation Architecture  People = User Work = Screen Format	e.g. Control Structure  Time = Execute Cycle = Component Cycle	e.g. Rule Design  End = Condition Means = Action	TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) <i>Sub-Contractor</i>	e.g. Data Definition  Ent = Field ReIn = Address	e.g. Program  Proc. = Language Stmt I/O = Control Block	e.g. Network Architecture  Node = Addresses Link = Protocols	e.g. Security Architecture  People = Identity Work = Job	e.g. Timing Definition  Time = Interrupt Cycle = Machine Cycle	e.g. Rule Specification  End = Sub-condition Means = Step	DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) <i>Sub-Contractor</i>
FUNCTIONING ENTERPRISE	e.g. DATA	e.g. FUNCTION	e.g. NETWORK	e.g. ORGANIZATION	e.g. SCHEDULE	e.g. STRATEGY	FUNCTIONING ENTERPRISE

Zachman Based Security Architecture (SABSA)

Level	Data (What)	Function (How)	Network (Where)	People (Who)	Time (when)	Motivation (why)	Deliverables
Contextual	Identify general nature of data (personal, confidential, financial, critical) Collection Methods	Business driven information security management program	Business field operations management Interfaces to trading partners – Data collection and usage (Sensitivity)	Stakeholders, users, external parties (Privacy, Sensitivity)	Business Calendar Probability of threats occurring Importance of service (Critical?)	Why are threats present? Consequences and impact Corporate Policies	Charts 1, 2 and 3 of TRA High level PIA
Conceptual	Business Continuity Management Identify data of sensitive or personal nature (Privacy, Integrity)	Identify sensitive and critical Processes and resources Risk identification	Location and network protection requirements (firewalls, encryption)	User authentication and authorization requirements Privacy impact	Availability and recovery requirements Service Levels	Identify specific assets and functions at risk Vulnerability analysis	Identification of security mechanisms and components (PKI, encryption)
Logical	Security requirements for Personal and Critical data fields (Isolation, edits, encryption)	Security requirements for sensitive processes (logging, access control)	Middleware security and data transfer security requirements	Access to functions and transactions Security Administration requirements	Business and system impact analysis When is security enforced?	Determine level of protection required for assets, functions and data (accepted risk)	Chart 4 & 5 of TRA Complete PIA Select security products
Physical	Database security mechanisms File security Audit trails and log security	Security components, objects and mechanisms	Network communication security mechanisms	Security interface for users and administrators Authentication mechanism	Security logging, access control, security reports Backup plans	Integration of security components and mechanisms	Security test strategy and test plans

Security Building Blocks



Policy

- A security policy outlines an organization's position on security issues. It must be endorsed and supported by Management.
- A good security policy can be simply stated, easily understood and in a form that can be widely communicated.

Standards

- Security standards make specific mention of technologies, methodologies, implementation procedures and other details.
- It is used by the enterprise to implement the security policy.

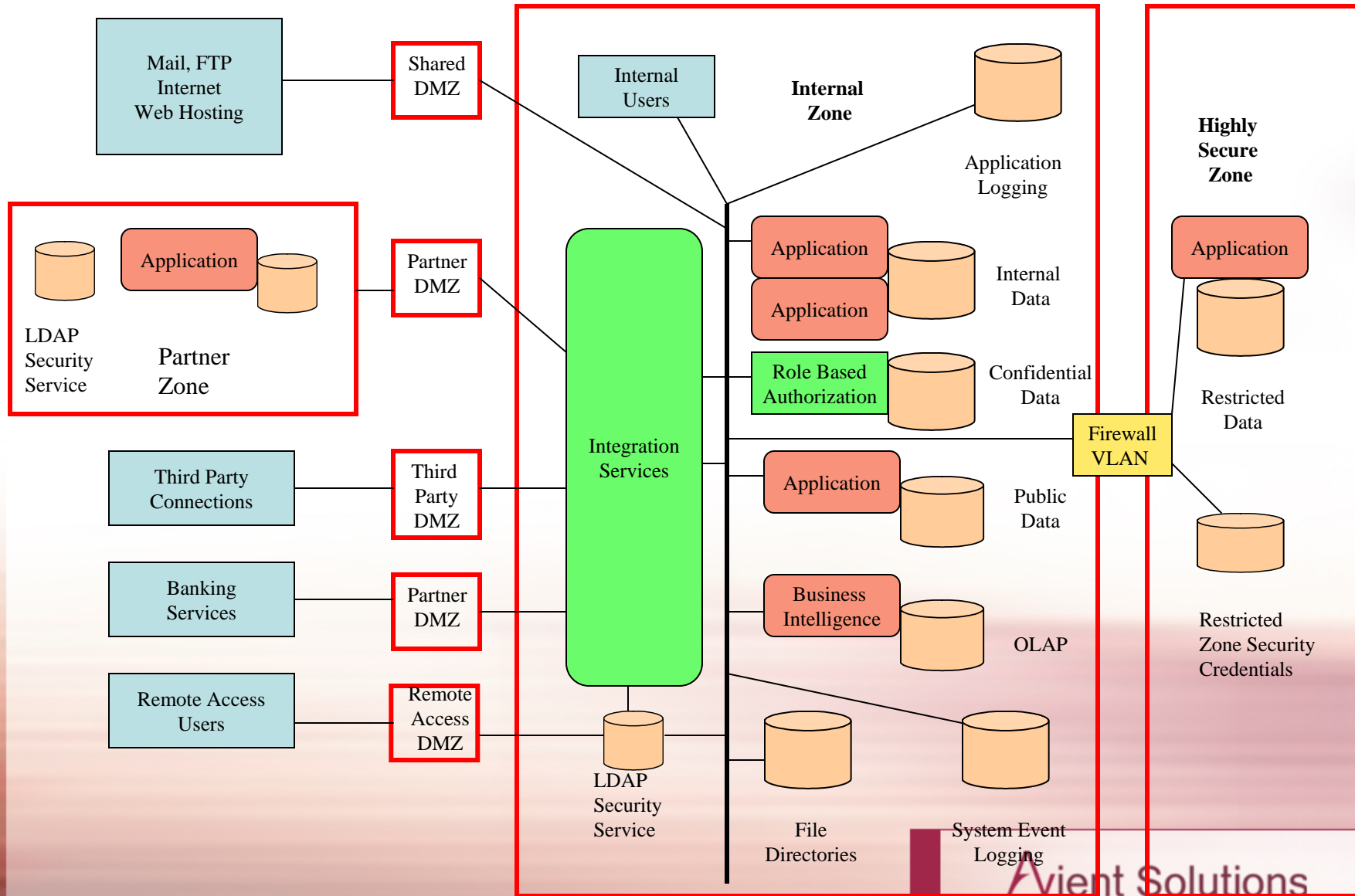
Processes

- Processes are created and implemented with respect to polices and standards.
- Part of the process is an assessment of existing process to ensure business needs are still met.

Security Architecture Foundation Deliverables

- Risk Management Templates and Guidelines
 - Threat risk assessment process
- Privacy Management guide and forms
- Enterprise security architecture vision
- Security Architecture Design Document templates
- Technical security standards - Baseline
- Project team training program
- Enterprise security architecture migration plan

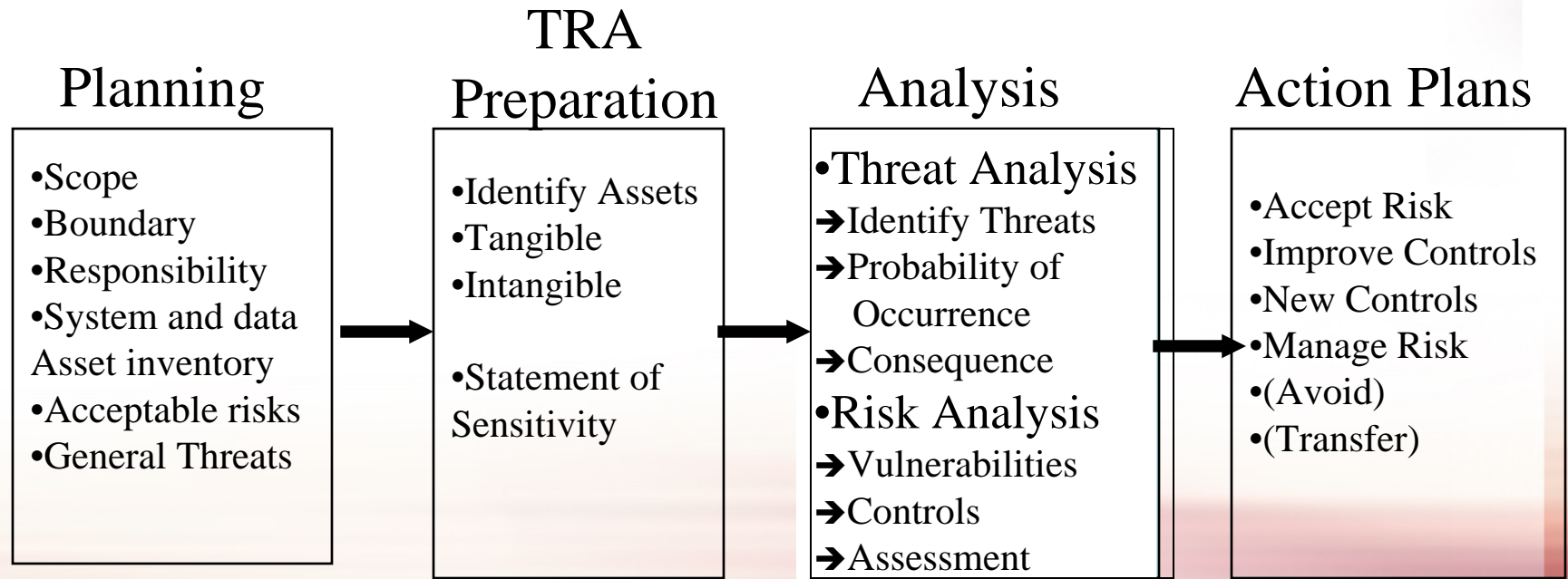
Security Vision



Risk Assessment Methods

- › Spans across all domains and is applied in context
- › Formal methods and deliverables must be used
- › Should be facilitated or reviewed by security experts
- › Industry Standards (samples)
 - › Operationally critical threat asset vulnerability evaluation (OCTAVE)
 - › NIST SP 800 Threat risk assessment guide
 - › New Zealand / Australia AZ/NZS 4360 method
 - › IRM, ALARM

Threat Risk Assessment Process



Threat Risk Assessment Deliverables

- Security Plan for the system
 - Description of the risks and environment
 - Component placement, server functions, diagrams
 - Data classification
- Description of risks and key controls to be used
- List of baseline security components
- Identify new security methods or components
- Security testing methods
- Logging and Monitoring requirements

Privacy Risks

- Unauthorized disclosure of data to external parties
- Construction of data profiles
 - Data matching and user monitoring
- Unauthorized use of private data
- Inadequate protection and safeguards
- Incorrect data used for decision purposes

Privacy Impact Assessment

- Assessment of privacy risks during systems under development
- Privacy risk assessment document to be completed
- Identify and classify personal private data
 - Where and how is it collected?
 - Where is it processed?
 - Where is it stored and with what other data?
 - Is the data disclosed to other users or systems?
- Document data flow and user actions
- Select controls and establish processes

Security Architecture Benefits

➤ Business Alignment

- Risk driven selection and management of controls
- Participation during system development
- Business support and business enablement

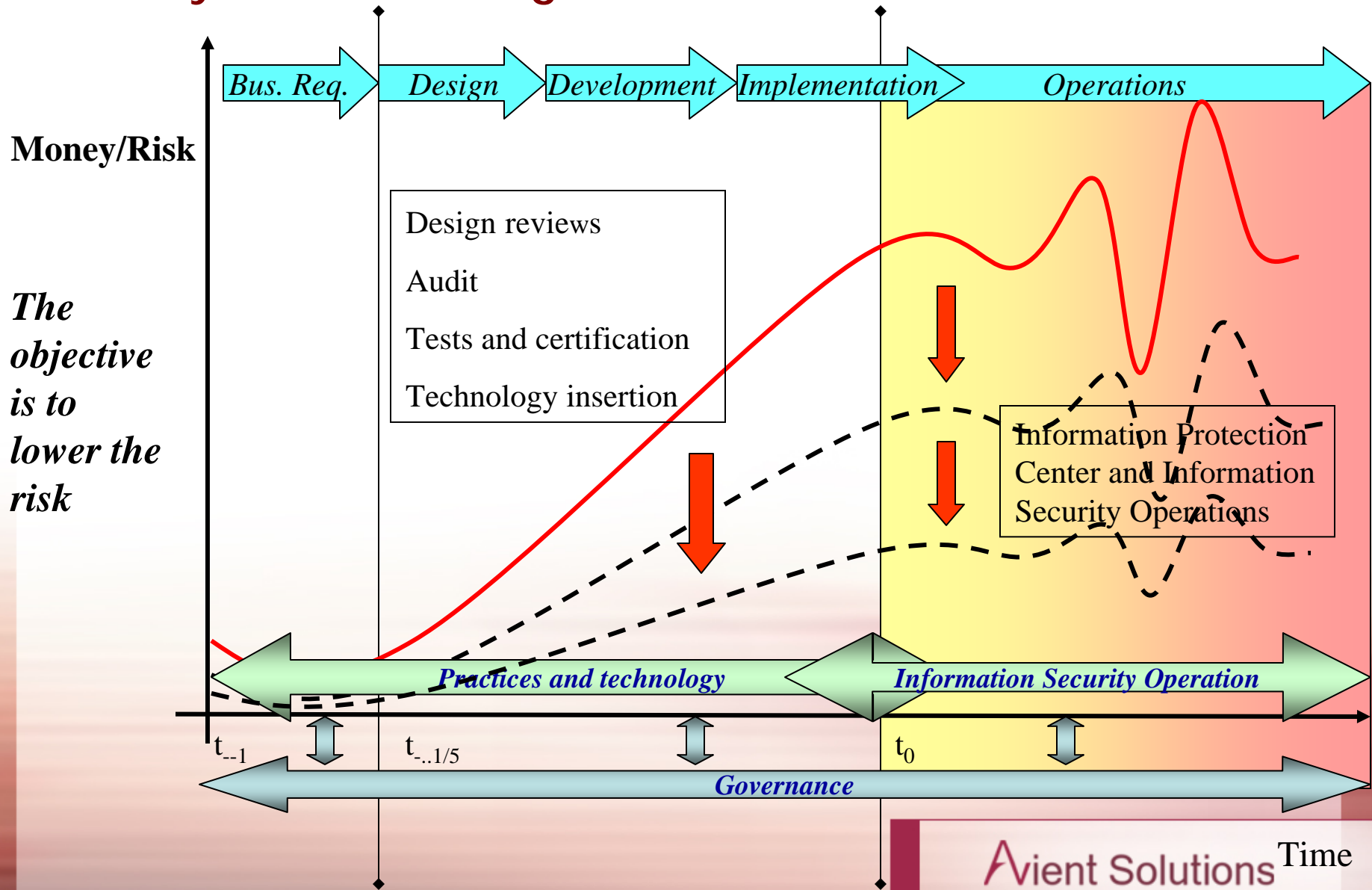
➤ Cost Management

- Reusability of components and processes
- Efficient administration and maintenance

➤ Ease of Integration

- Scalability of solutions
- Trusted solutions

Life Cycle Risk Management



Security at the Systems Layer

› Logical Security Architecture

- › Compliance to Policies and Standards
- › Identity management
- › Authorizaton services
- › Messaging security
- › Data encryption
- › Audit and logging facilities
- › Malicious code protection
- › Application Integration
- › Deliverables:
 - › Logical Threat Risk assessment
 - › Privacy impact assessment

Security at the Technology Layer

› Infrastructure Protection

- › Network Perimeter security protection
- › Network Segmentation
- › Network identity management
- › Authorization
- › Intrusion detection
- › Remote System Access
- › VPN and Encryption
- › Logging and monitoring
- › Deliverables:
 - › Physical Threat Risk assessment
 - › Testing Methods
 - › Logging and monitoring tests

Security Strategy

› Technology

- › Network protection methods
- › Intrusion detection
- › Logging and monitoring
- › Channel level encryption
- › Security Standards
- › Security Administration
- › Code protection

› Security Analysis and Management

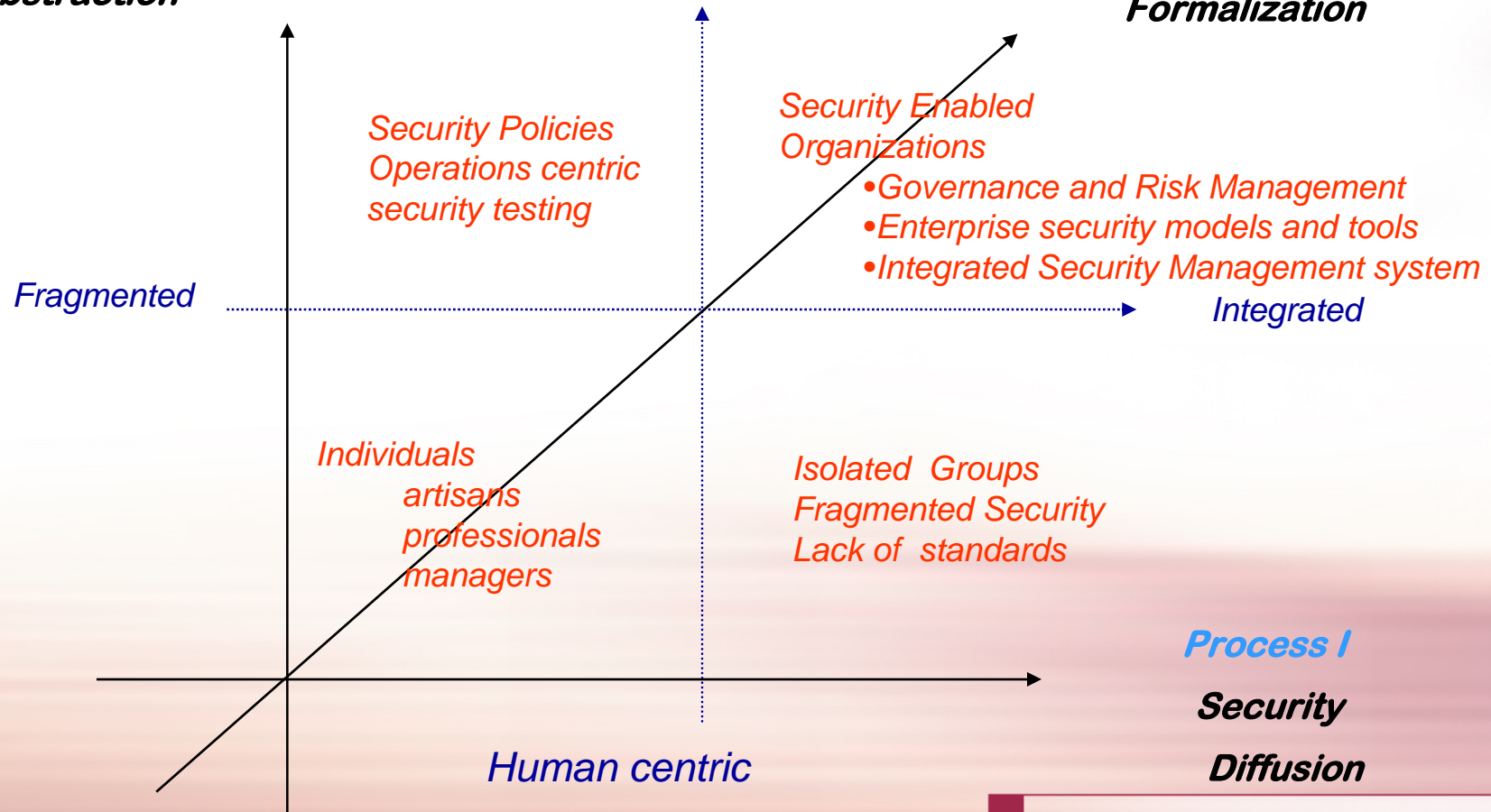
- › Enterprise Architecture Methods
- › Risk Management Methods
- › Privacy assessment methods
- › Identity, authentication and authorization
- › Multi-layered Security architecture
- › Incident management
- › Governance, Risk and Compliance processes

Security Management Maturity model

Process II
Security
Abstraction

Technology
centric

Process III
Security
Formalization



Process I
Security
Diffusion

Developing the Corporate Security Architecture

- › **Define Security Principles and Standards**
 - › Security Policies, Principles and Standards
 - › Security Vision
 - › Baseline security methods and controls
 - › Define Security Artefacts and templates
 - › Integrate with Technology and application domains
- › **Define and document Core security tools and services**
 - › Identity management
 - › Logging and Monitoring
 - › Network protection (firewalls and IDS)
 - › Malicious code protection
- › **Define IT Security Governance processes**
 - › Participation in Systems development and technology procurement projects
 - › Integration with Project management methods
 - › Phased approach for development of security artefacts (Risk Management Plan and security diagrams)
 - › Define Security testing requirements
 - › Assess if the security methods / tools will be sustainable
 - › Define a refresh process for the security architecture

Security Architecture Development

- What architecture development methods are right for you?
- Can the security architecture be developed as a stand alone domain?
- Formal ADM (Strategic)
 - Formal templates and processes
 - Architecture Vision and Definition
 - Architecture Core Teams and Review Boards
 - Architecture Foundation and reference library
- Guidelines (Tactical)
 - Just in time architecture
 - Architecture LITE
 - Security Vision and templates

Security Architecture Development Methodology

Conceptual Risk Assessment

- › Identify Security business requirements
 - › Description of current environment and processes
 - › High level Risk Assessment of business practices, data and technology
 - › Assess applicability of government or industry regulations
 - › Refine risk assessment and include future plans
 - › Create conceptual risk report
 - › Business risks
 - › Technology risks
 - › Operational / financial risks
- › Decide level of project involvement

Security Architecture Development Methodology

Logical Risk Assessment

- Logical Security Model Development
 - Review with project team and create logical security architecture using core components
 - Identify new security components or methods
 - Create logical threat risk assessment document
 - Risk assessment of each component in system
 - Security methods and controls to be implemented
 - Assess data protection methods and privacy impact
 - Review with Enterprise Architecture

Security Architecture Development Methodology

Physical Security Assessment

- › Information Security Deployment and Testing
 - › Review physical deployment diagrams
 - › Validate that security requirements are implemented
 - › Review security methods and activities
 - › System logging and monitoring
 - › User management
 - › Source Code validation
 - › Define / Execute Security test strategy and plan
 - › Security Scans
 - › Vulnerability assessments
 - › Penetration tests
 - › Disaster Recovery Test
 - › Update Enterprise Architecture documents
 - › Update governance risk and compliance processes

Assessing the Security Architecture

- **Control Objectives for IT (COBIT)**
 - Developed by ISACA as a governance framework
 - Plan and Organize
 - Acquire and Implement
 - Deliver and Support
 - Monitor and Evaluate
 - Includes a guide for measuring maturity
- **Capability Maturity Model**
 - Must be tailored for the organization
 - Applied to security functions and services

Corporate Security Architecture Assessment

Step 1 - Preliminary Review of Security Architecture

- › Review the scope of the security architecture
- › Review target security architecture
- › Review security policies and standards
- › Review security principles and vision
- › Assess security organization and staffing
- › Identify Regulatory Compliance requirements
- › Evaluate the Risk Assessment methods in use for projects and systems
- › Identify and map out the Architecture governance process for security
- › Review Risk issue management process
- › Assess Security Design Plan templates and completed forms
- › Review security management procedures
- › Assess Business Continuity Plan and maintenance

Corporate Security Architecture Assessment

Step 2 - Evaluate Security foundation and components

- › Validate security plans to actual implementation
- › Assessment of security methods, technology
- › Security awareness and risk management training
- › Assess how security is integrated with other architecture domains
- › Assess Security Components
 - › Identity management
 - › Logging and Monitoring systems
 - › Network protection
 - › Encryption key management processes
 - › Malicious code protection

Corporate Security Architecture Assessment

Step 3 - Assess the Technical Security Architecture

- › Security implemented for the Technology and Application layers
- › Vulnerability Assessment methods in use
- › Security Scan test methods
- › Security Reviews completed by third parties
- › Source code reviews and testing
- › Physical security
- › Technical support access
- › Backup and Recovery processes
- › Network security

Summary and Conclusions

- › New risks created by new technologies and business processes
- › Regulatory compliance, including privacy is driving enhanced security requirements
- › Increase risk of attacks from external sources
- › Enterprise Architecture is growing in popularity
- › Challenge to implement and maintain
- › Security architecture is pervasive across the other domains of architecture - Business, data, technology and applications
- › Security architecture is completed in layers
 - › Conceptual, Logical, Technical
- › Requires a framework of risk management methods, baseline standards and governance process
- › Comprehensive risk management plan for security, privacy and business continuity