Security Architecture
- Week 7 -

Mid-term Review

Mid-Term Review Session

- Week 6 Assignment
- Items in the news
- Semester Project
- Mid-term Review
- Mid-term Exam

Semester Project

REQUIRED: any diagrams necessary to complete the work proposed in your abstract and outline.

Example:

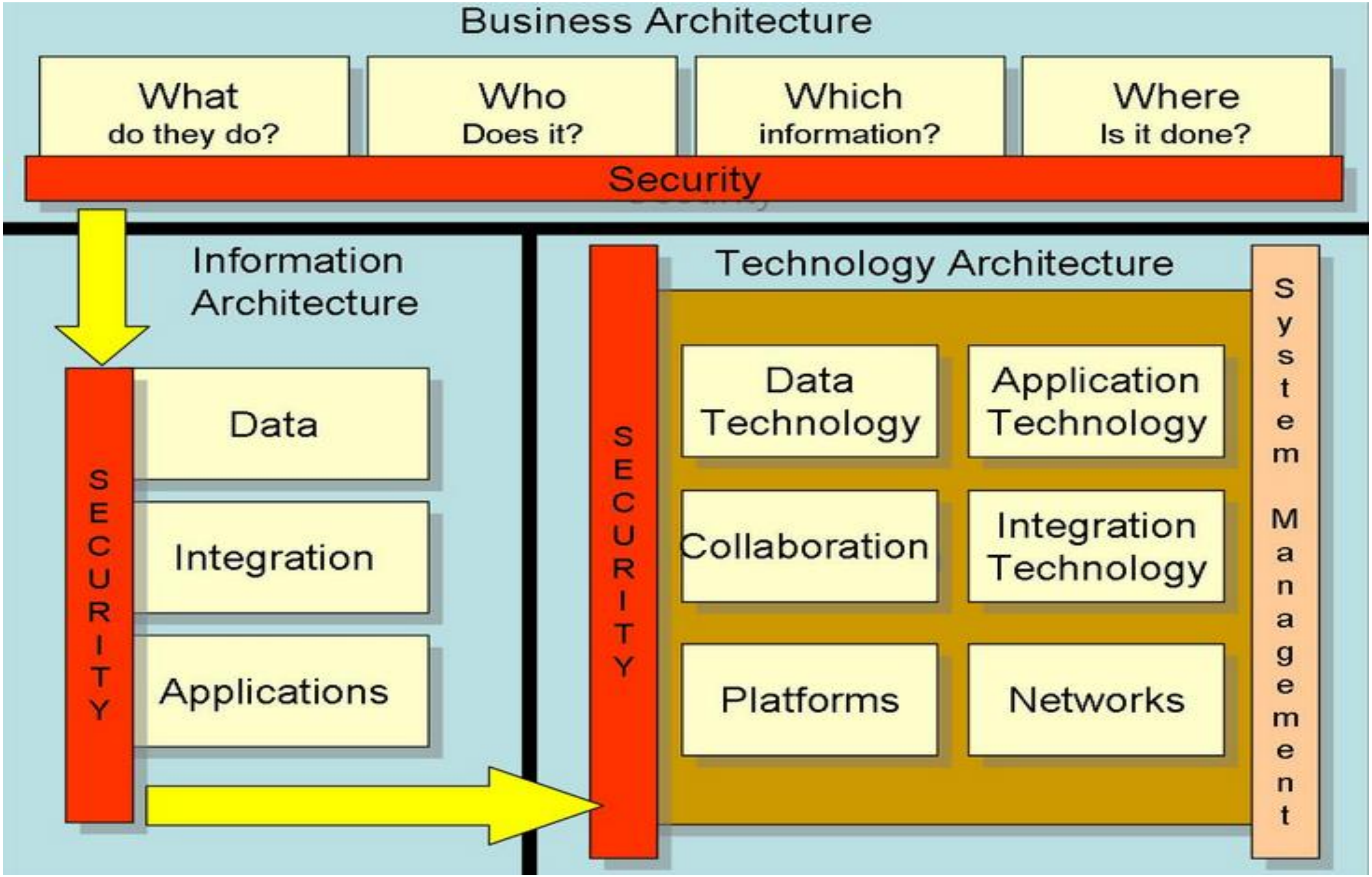
- Logical diagram
- Enterprise diagram
- Security system-specific diagram(s) for clarification
- Any notes required to explain the diagram (can be annotations directly on the diagram(s)

Security Architecture

Devising the means of managing the secure implementation between business processes in the enterprise system context is a principle mission of security architecture. The security architecture context encompasses the complete business context more than any other business discipline.

Security architecture therefore focuses on the development of security solutions based on the mapping among the control architectures, protection processes and systems life cycles in a business context.

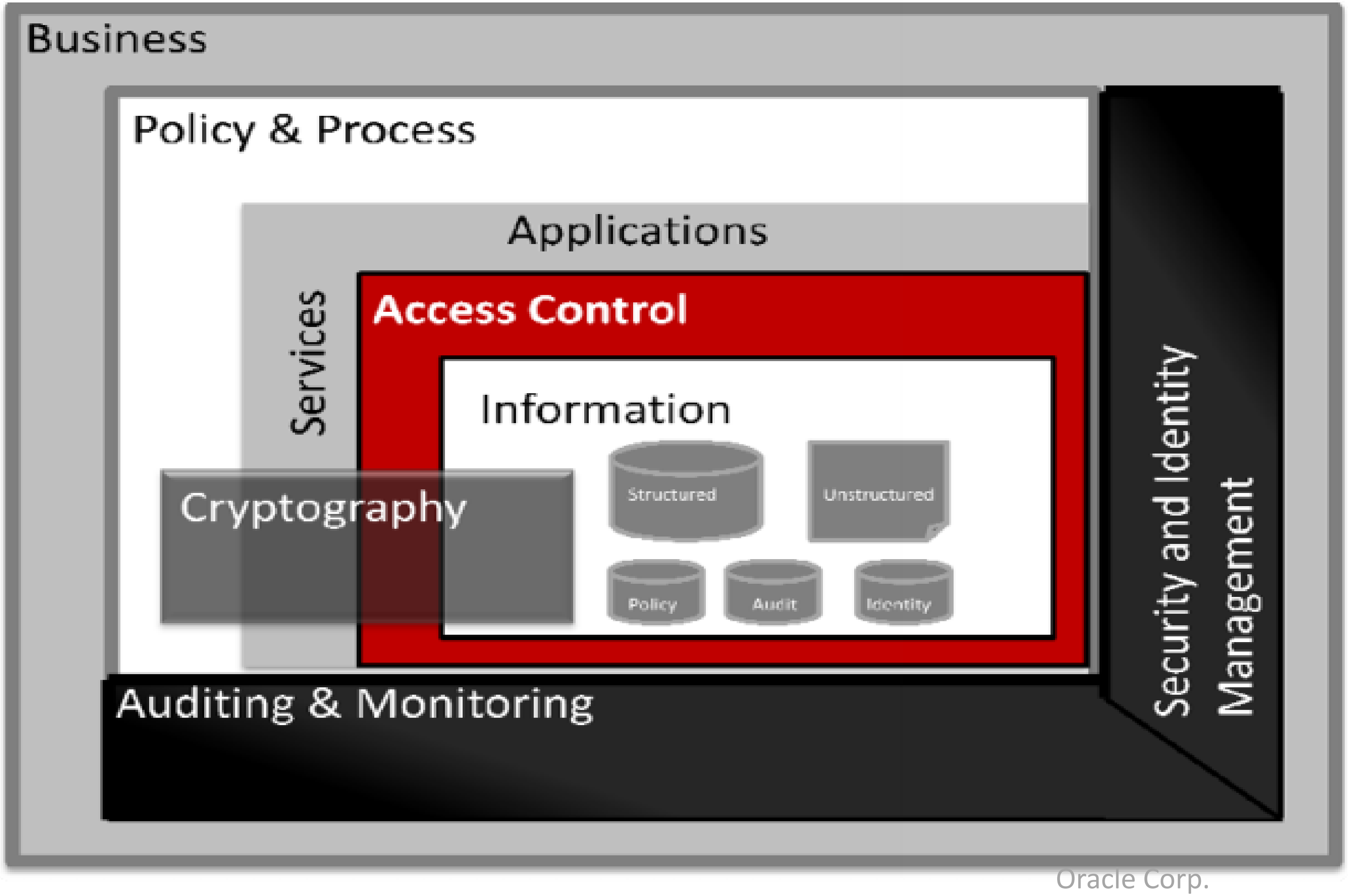
Enterprise Architecture Context



Source: Wikipedia 2014

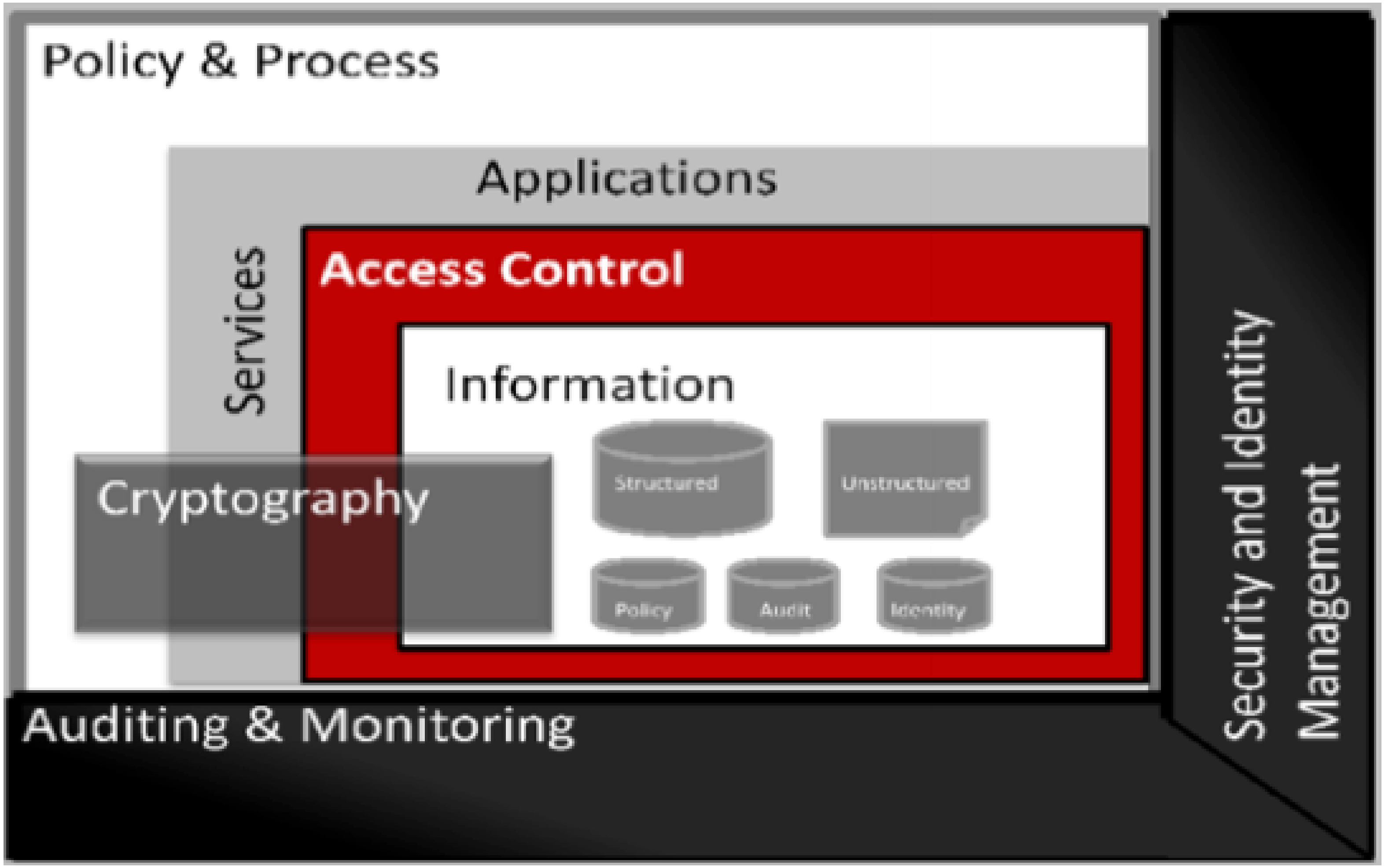
MIS 5214 Security Architecture
Greg Senko

Security Process Context



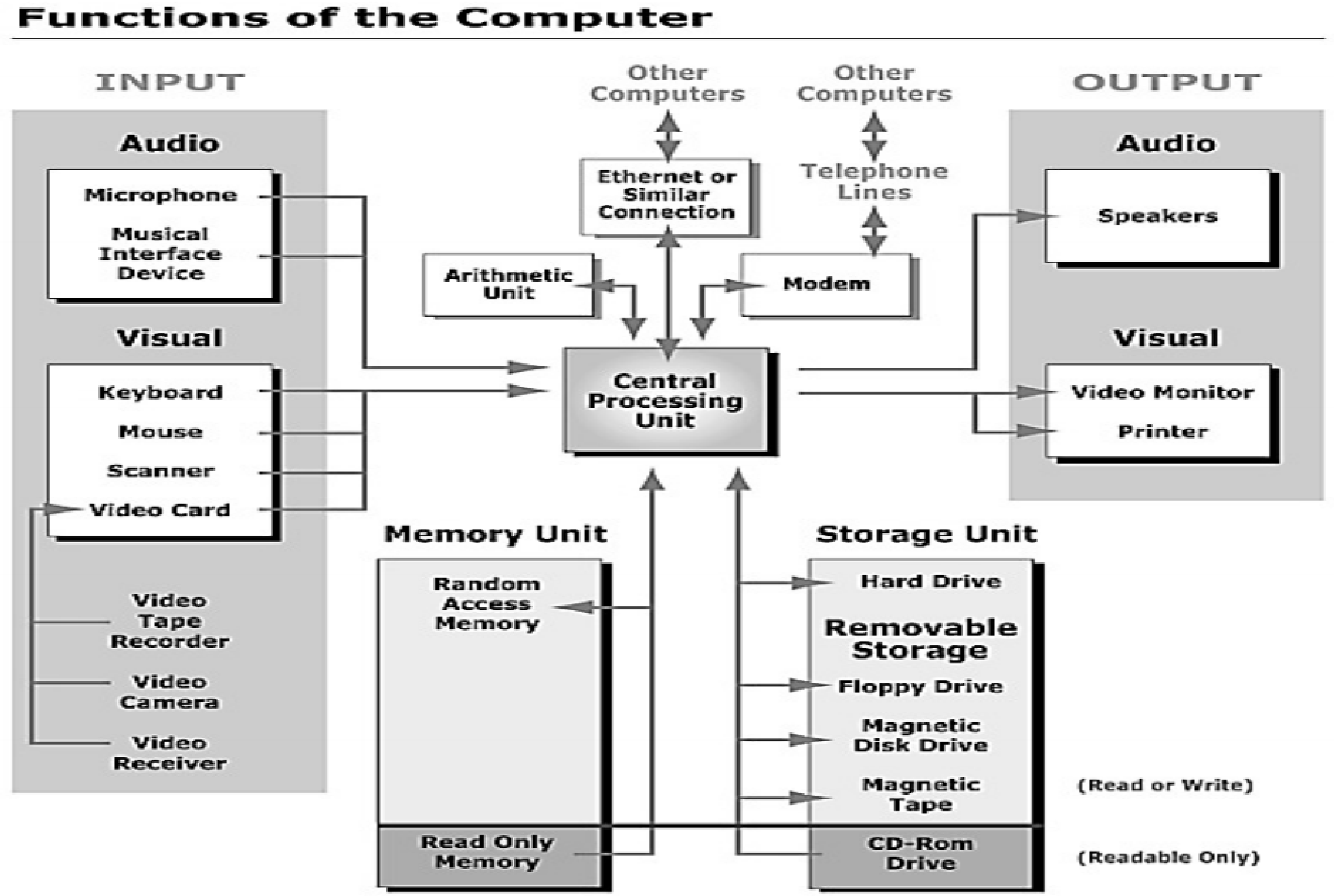
Oracle Corp.

Security Process Context



Source: Oracle Corp.

Device Level Security



SAMSA Security Service Management Architecture

Contextual Layer

Business driver development, business risk assessment, service management, relationship management, point-of-supply management and performance management.

Conceptual Layer

Developing the Business Attributes Profile, developing operational risk management objectives through risk assessment, service delivery planning, defining service management roles, responsibilities, liabilities and cultural values, service portfolio management, planning and maintaining the service catalogue and managing service performance criteria and targets (service level definition).

Logical Layer

Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted
power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup

Physical Layer

Asset management, policy management, service delivery management, service customer support, service catalogue management, and service evaluation management.

Component Layer

Tool protection, operational risk management tools, tool deployment, personnel deployment, security management tools and service monitoring tools.

Business Context

What do we mean by

“Security Architecture

Business Context?”

Business Context

- Strategic Context
- Market context
- Competitive context
- Regulatory context
- Enterprise context
- Systems context
- Business Lifecycle context
- Budget context
- Product Lifecycle context
- Risk Profile
- Risk Tolerance
- Security Portfolio
- Security Projects
- SIEM organization

Identity and Access Management

The ability to verify an individual's identity and, on that basis, restrict the facilities and resources to which they are privileged

Identity and Access Management

- Taking on more importance
- Used to be, principally, the process of managing user IDs and passwords
- Integrated network permissioning and single sign-on capabilities have made management processes essential
- Questions about the sufficiency of perimeter security have highlighted importance
- The multitude of devices, including personal devices, on the business network creates new needs
- Internet-of-things will complicate and magnify the impact

Identity Verification

- One ID for all activities
- Problem: how do you do this across different technologies
- The power of role-based privileging

Business Context

What do we mean by

“Security Architecture

Business Context?”

Business Context

- Strategic Context
- Market context
- Competitive context
- Regulatory context
- Enterprise context
- Systems context
- Business Lifecycle context
- Budget context
- Product Lifecycle context
- Risk Profile
- Risk Tolerance
- Security Portfolio
- Security Projects
- SIEM organization

Network Architecture

“Perimeter Security is still the first line of defense against intruders and network architecture provides the basis for perimeter security”

Netowrk Architecture

- Evolution of Networking
- Internet Protocol
- Local Area Networks
- Wide Area Networks
- Sub-netting strategies
- Impact of the cloud
- Changes in creating POPS

Application Security

The evolution from monolithic application architectures to client/Server, N-tier and Service Oriented Architectures has allowed for greater responsiveness and improved user experience. But, it has complicated the job of securing application processes and data.

Application Security

- What do we mean by “application?”
- Tradition connotation
- Web facing
- Mobile
- Back Office
- Model for instantiation
- Risks and mitigation

Mid-term Exam