Software Technology Conference 2002

Building and Implementing Secure Architectures

Dr. Michael Martin
National Defense University
April 30, 2002

Topics

- Overarching Considerations
- Review of Standards Based Security Architectures
- Toward the Development of a Security Process
- A New Security Paradigm

Part I

Overarching Considerations

Principles

1. Computer Security Supports the Mission of the Organization
2. Computer Security Is an Integral Element of Sound management
3. Computer Security Should be Cost-effective
4. System Owners Have Security Responsibilities Outside Their Own Organizations
5. Computer Security Responsibilities and Accountability Should Be Made Explicit
6. Computer Security Requires a Comprehensive and Integrated Approach
7. Computer Security Should Be Periodically Reassessed
8. Computer Security Is Constrained By Societal factors

Understanding Generally Accepted Principles and Practices for Securing Information Technology Systems *NIST 1996*

Guidance

1. Senior executive support is crucial
2. Security is seen as an enabler
3. Hold program and Business managers accountable
4, Establish a central management focal point
5. Designate a central group to carry out key activities
6. Provide the central group ready and independent access to sr. execs
7. Link policies to business risks
8. Support policies through the central security group
9. Designate dedicate funding and staff

Learning from Leading Organizations, GAO AIMD 98-68 May 1998

Major Issues

- Policy - still a research issue
- Risk Analysis- immature discipline, non-standard
- Culture - does the culture support security?
- People- do they have the skills, ethics,commitment?
- Process - how do you implement and integrate?
- Technology- enterprise technologies not scalable
- Laws/Regulations - which ones apply?

Characteristics of a wicked problem

A wicked problem:

- cannot be definitively stated
- has no rules or guidelines to indicate when it is solved.
- has no right or wrong solutions only good or bad ones.
- cannot be definitively tested
- has solutions that are too significant to be experimented with
- has no bound on the solutions and the means of obtaining them
- is a singularity

IT Architectures as a Wicked Problem

- Difficult to bound the problem and constrain components
- Requires excruciating detail
- Existing rules and guidelines are descriptive not prescriptive
- Difficult to go from strategy to implementation
- Once you have built an infrastructure, you are stuck with it.
- Unlimited potential solutions --most are not cost effective
- Cannot test final results because the process is iterative
- Every solution is specific to an agency or corporation

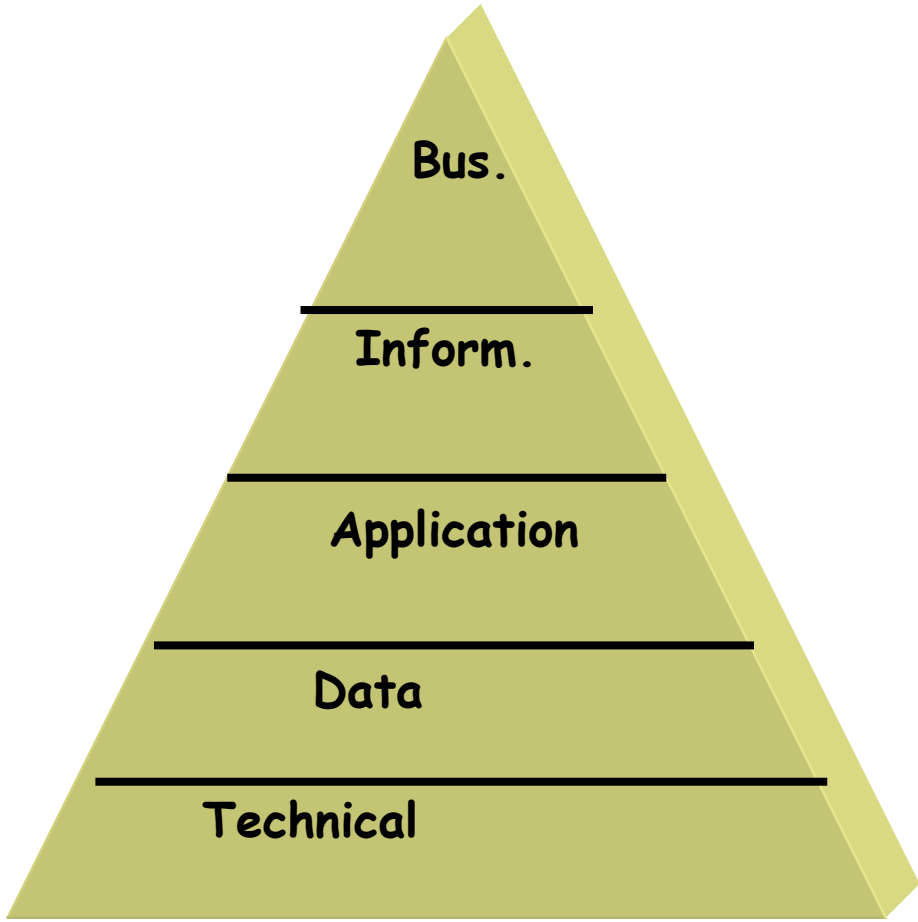
Enterprise Security as a Wicked Problem

- Difficult to define enterprise security
- Never sure when it is achieved-it's a process not a final state
- Many possible approaches--some good some bad
- Cannot be definitively tested
- Each solution is ad-hoc and iterative

Part II

Review of the Standards-based Model

Does it really support information security?



OMB EA MODEL

Derive Security Requirements From Conops

Requirement	Rationale
Identification and authentication	Secure electronic commerce
Confidentiality	**Secure electronic commerce**
Integrity	Secure electronic commerce
Non-repudiation	Secure electronic commerce
Access control	Secure electronic commerce
Availability	**24x7 operations**
Auditing	**Intrusion detection due to new outside links**
Perimeter Protection	Control unauthorized access to private WANs
Policy control	Enforce policy in global environment
Security administration	Organize security team for effective oversight
Directory services	Locate individuals anywhere, anytime, anyplace
Antivirus & malicious software	Protect against malicious agents from outside

Identifying and Projecting Risks

Risk Framework

- Physical Attempts to gain control (physical intrusion)
- Electronic Attempts to gain control(malicious hacking)
- Execution of Arbitrary Code (viruses, Trojans,Active-X,Java,…)
- Spoofing (lying about who you are--users,sites,devices)
- Eavesdropping(sniffing, wiretapping of data, passwords, etc.)
- Lack of Knowledge/ Awareness (admin., users,outside errors)
- Lack of Trust, Confidence (users, disgruntled…)
- Denial of service (down time: electronic DOS, disasters, reliability)
- Exploitation of User by Site (privacy, swindles…)
- Exploiting the data subject (privacy, confidentiality, non-user)
- Lack of Interoperability

Standards Profile

Information Processing Standards

Data Management

RDBMS	SQL

Data Interchange

EDI	FIPS 161-2 - ANSI X12 - EDIFACT - HL7
Document	HTML SGML COTS
Graphics	CGM JPEG GIF

Information Transfer Standards

Applications Support

E-mail	SMTP/MIME MIME/EDI
File Transfer	FTP
Directory/ Dir Access	X.500 LDAP(v3)
Naming	DNS

World Wide Web

HTTP	HTTP 1.1
URL	URL/URI/mailto

Transport	TCP
Networking	IP
Net/System Management	SNMP various MIBs

Information System Security Standards

Information Processing Security

Protocols	X12.58
Passwords	FIPS 112

Information Transfer Security

Protocols	SSL S/MIME IPsec EDIINT
Sign/Hash	DSS MD5 SHS
Encryption	DES/3DES RC2, RC4, RC5
Certificates	X.509v3 PKCS 1,7,9,10,11

Why Are They Inadequate?

Services

Authentication

Access

Integrity

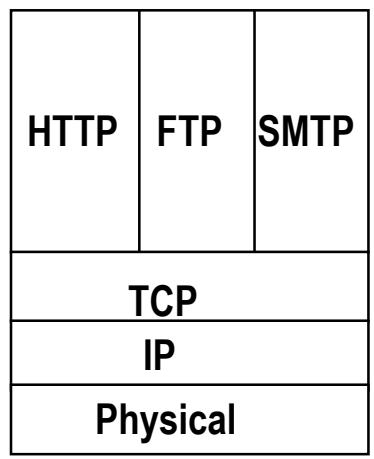
Confidentiality

Non repudiation

Mechanisms

Encipherment
Access control
Digital signature
Data integrity
Authentication exchange
Traffic padding
Routing control
Time stamping
Notarization

TCP/IP



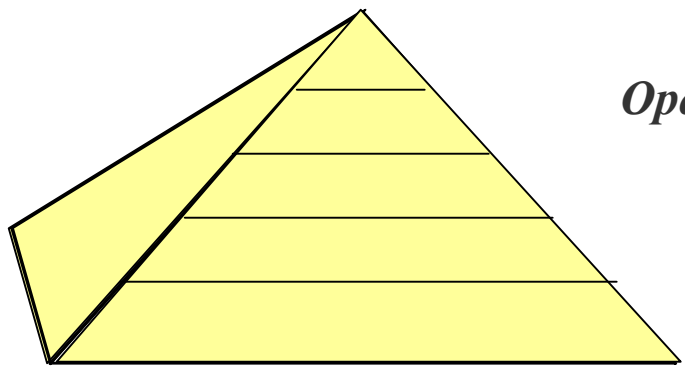
Part III

Toward the Development of a New Security Process

The world cannot be understood from a single point of view

--Eleanor Roosevelt--

Management View



Operational View

Technical View

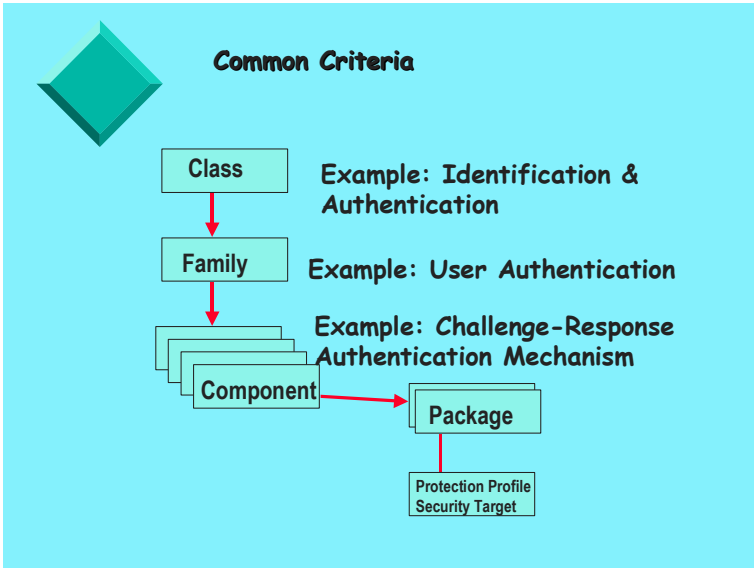
1. *Evaluating Existing Processes*
2. *A Suggested Security Process*

1. Existing Processes

Security Engineering CMM KPA Overview

	Management	Organizational	Engineering
5 *Optimizing* — *Work the Measures*		• Technology Change Management	
	• Process Change Management		• Defect Prevention
4 *Managed* — *Measure the Work*	• Quantitative Process Mgmt		• Security Validation • Security Vulnerability Analysis • Quality Management
3 *Defined* — *Work the Plan*	• Security Coordination • External Coordination • Intergroup Coordination • Integrated Project Mgmt	• Organization Process Focus • Organization Process Defn • Training Program	• Security Concept • Security Verification • Evidence Management • Peer Reviews
2 *Repeatable* — *Plan the Work*	• Requirements Management • Project Planning • Project Tracking & Oversight • Subcontract Management • Quality Assurance • Configuration Management		• Security Requirements • Security Design • Security Implementation
1 *Initial* — *Work and Work*	• Ad Hoc Processes		

Common Criteria V.2



- *Descriptive not prescriptive*
- *Uneven criteria for evalauting "maturity"*
- *Requires outside evaluation*
- *Long time to achieve*

- *Imposed only on vendors*
- *Applied after product is developed*
- *Not many success stories yet*
- *Scalability is an issue*

Security Engineering CMM KPA Overview

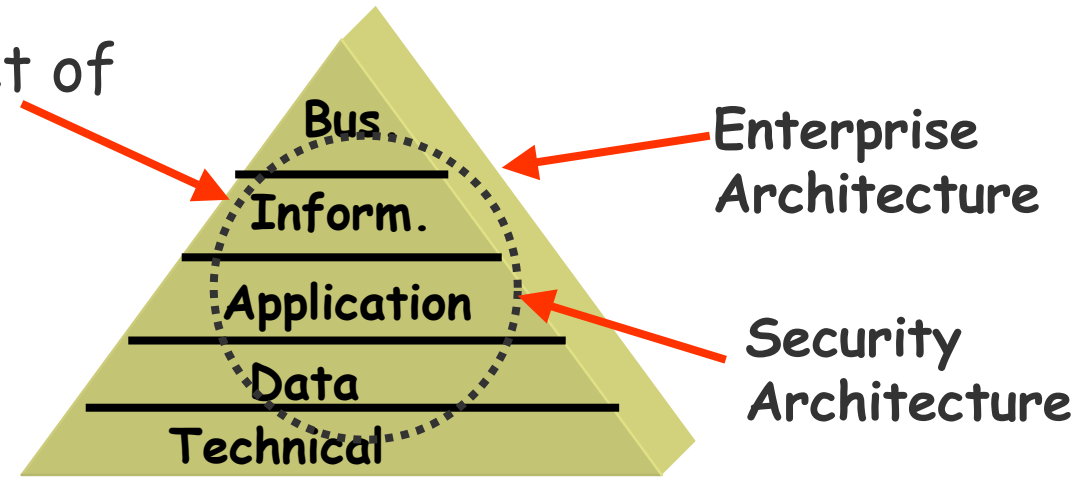
	Management	Organizational	Engineering
5 ***Optimizing*** *Work the Measures*		• Technology Change Management	
	• Process Change Management		• Defect Prevention
4 ***Managed*** *Measure the Work*	• Quantitative Process Mgmt		• Security Validation • Security Vulnerability Analysis • Quality Management
3 ***Defined*** *Work the Plan*	• Security Coordination • External Coordination • Intergroup Coordination • Integrated Project Mgmt	• Organization Process Focus • Organization Process Defn • Training Program	• Security Concept • Security Verification • Evidence Management • Peer Reviews
2 ***Repeatable*** *Plan the Work*	• Requirements Management • Project Planning • Project Tracking & Oversight • Subcontract Management • Quality Assurance • Configuration Management		• Security Requirements • Security Design • Security Implementation
1 ***Initial*** *Work and Work*	• Ad Hoc Processes		

2. A Suggested Security Process

Security may require its own process, but it must conform with the EA

Logical Security Architecture

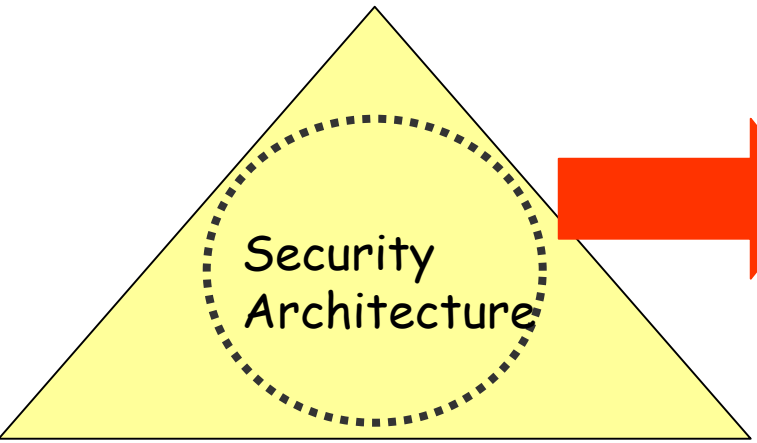
Driven by a hypothetical set of security requirements

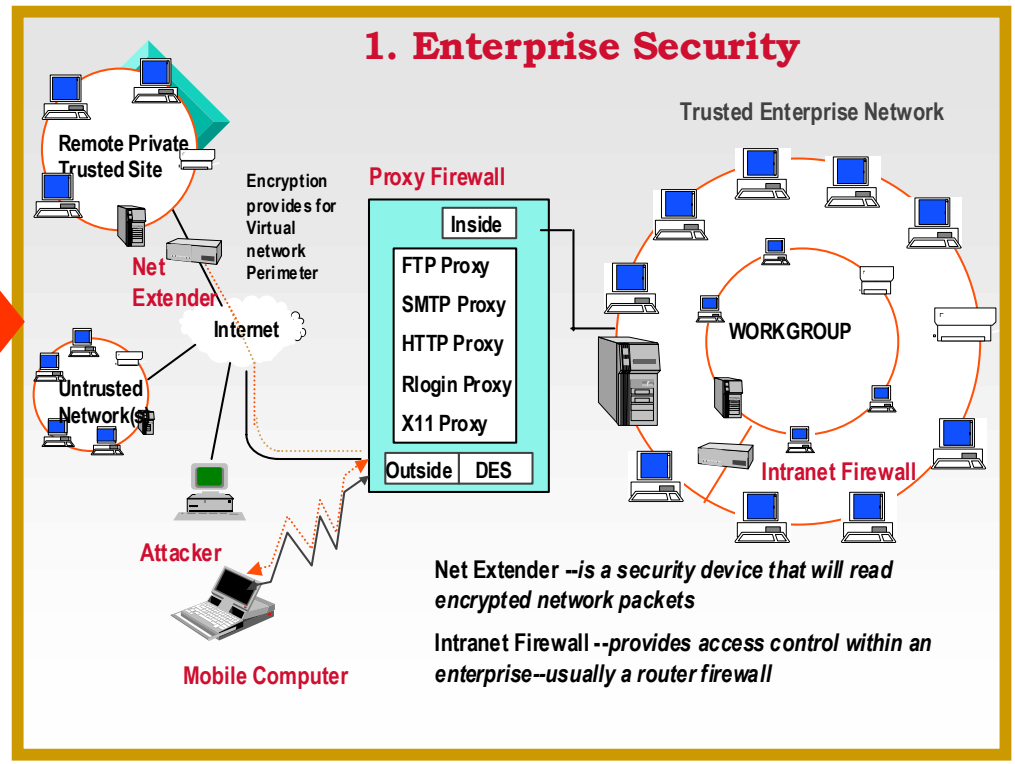


- Is a design that meets a hypothetical set of requirements
- Not intended to be implemented
- Requires no cost analysis
- Should describe the security analysis to be performed

Specific Security Architectures

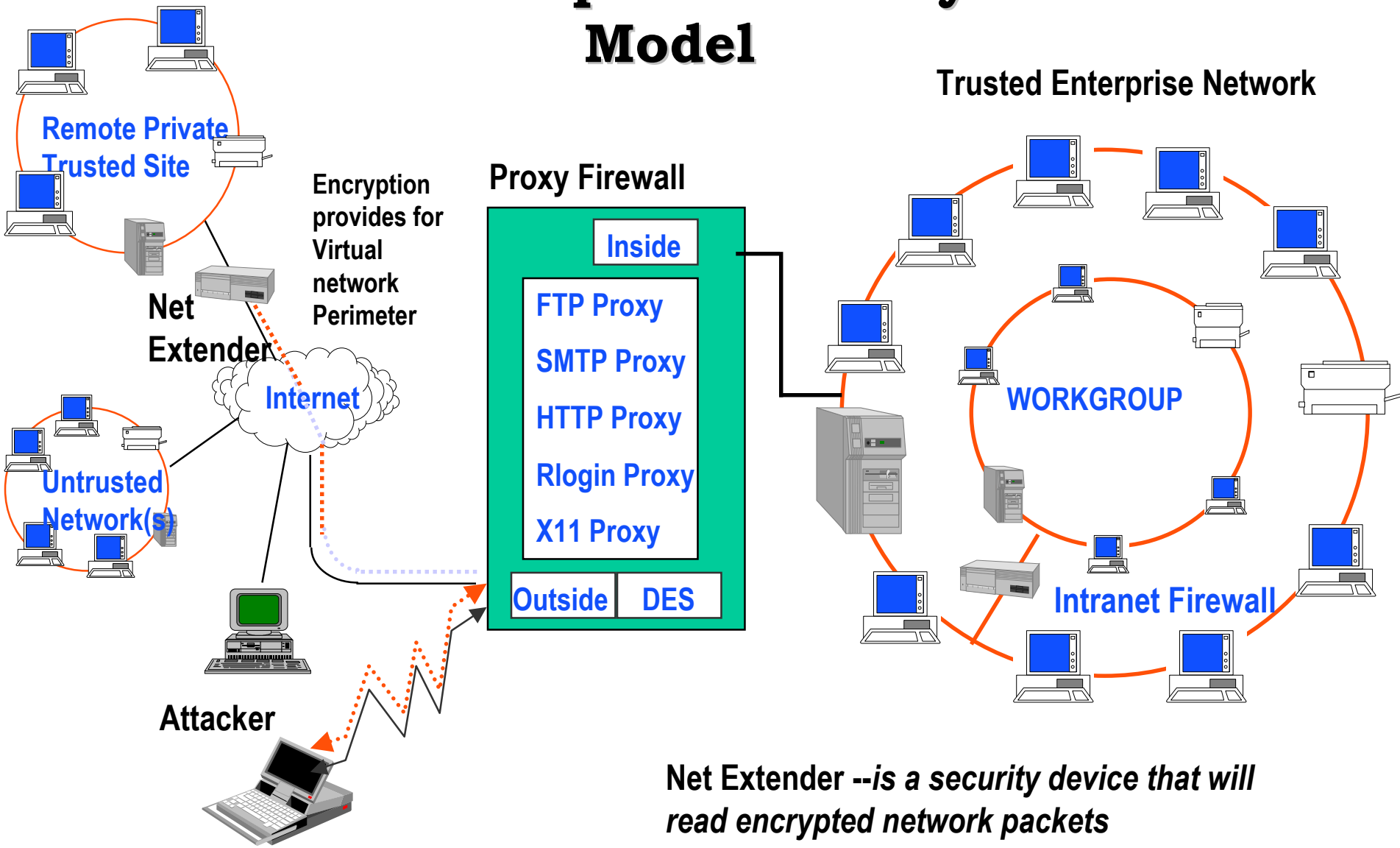
How do we instantiate?





Specific security architectures show how all the selected information security components and mechanisms, including doctrine and supporting security management components, combine to meet the security requirements of the specific system under consideration.

Enterprise Security Model

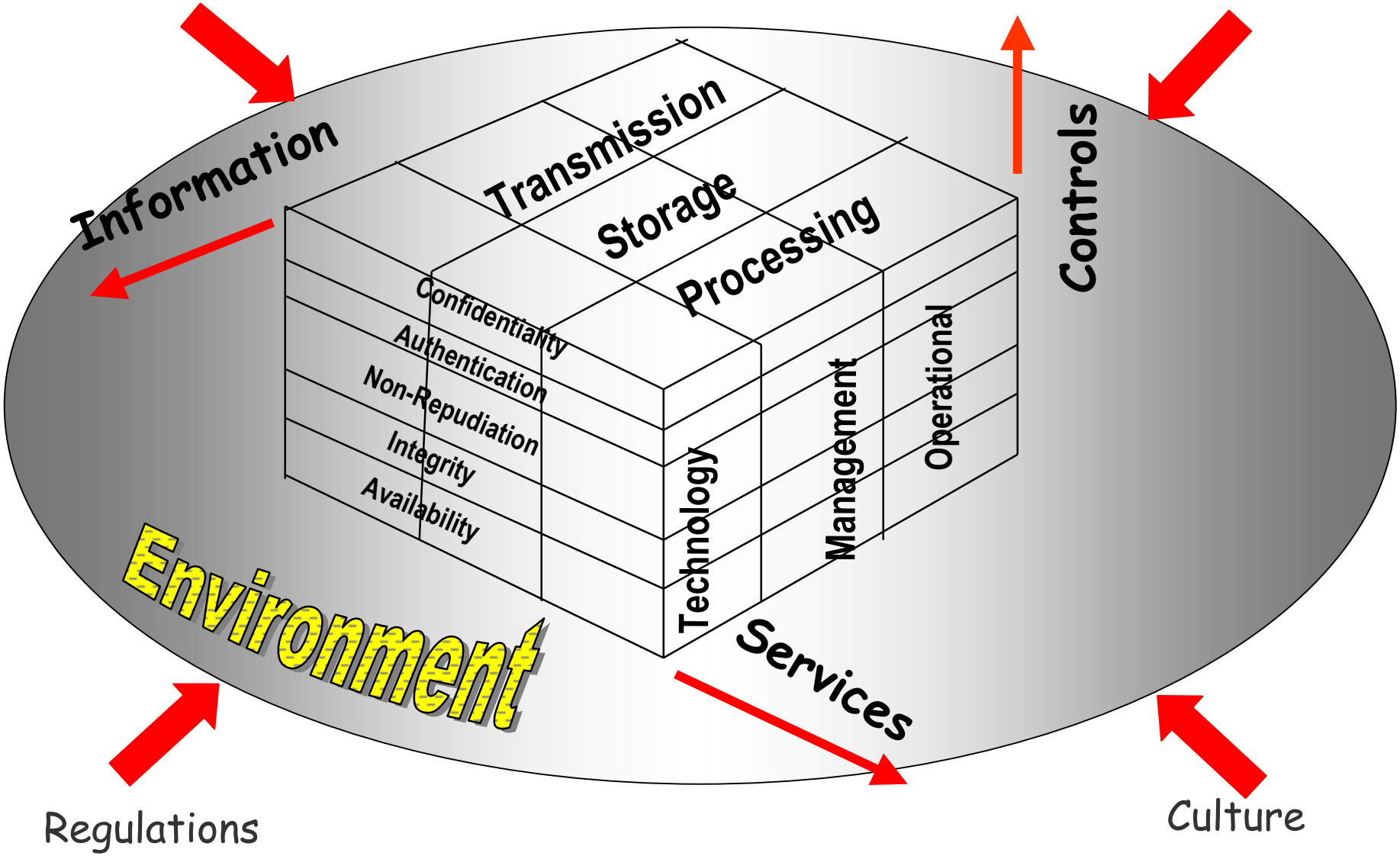


Net Extender --*is a security device that will read encrypted network packets*

Intranet Firewall --*provides access control within an enterprise--usually a router firewall*

An INFOSEC Model

(Adapted from McCumber)



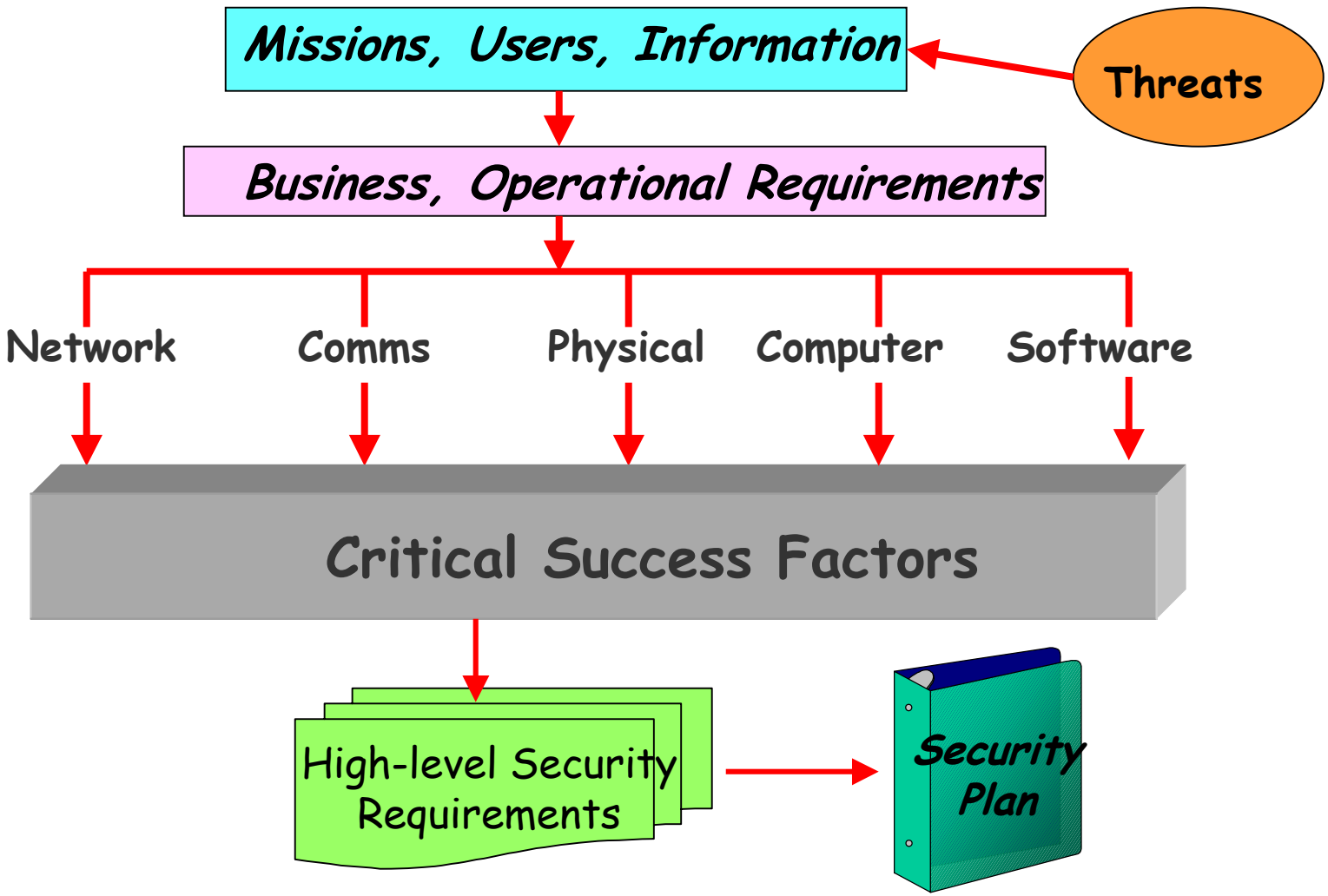
Identify Critical Success Factors

(Ballpark and Owners View)

Definition of "Future" State

What security will the enterprise need?

What are the critical success factors



Separating Applications from Infrastructures

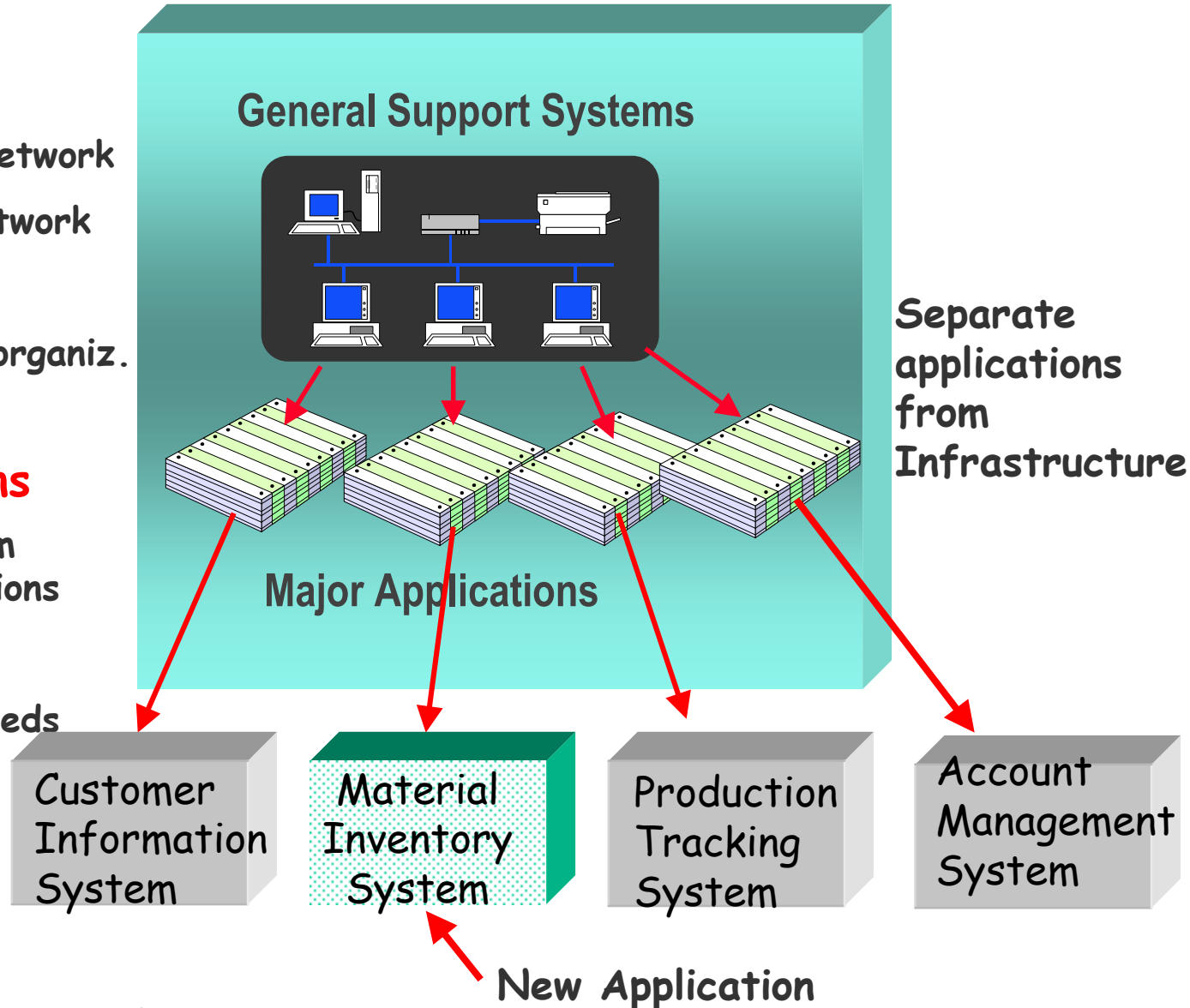
General Support Systems

- LANs
- Backbones
- Communications network
- Tactical radio network
- DP centers
- Shared services organiz.

Major Applications

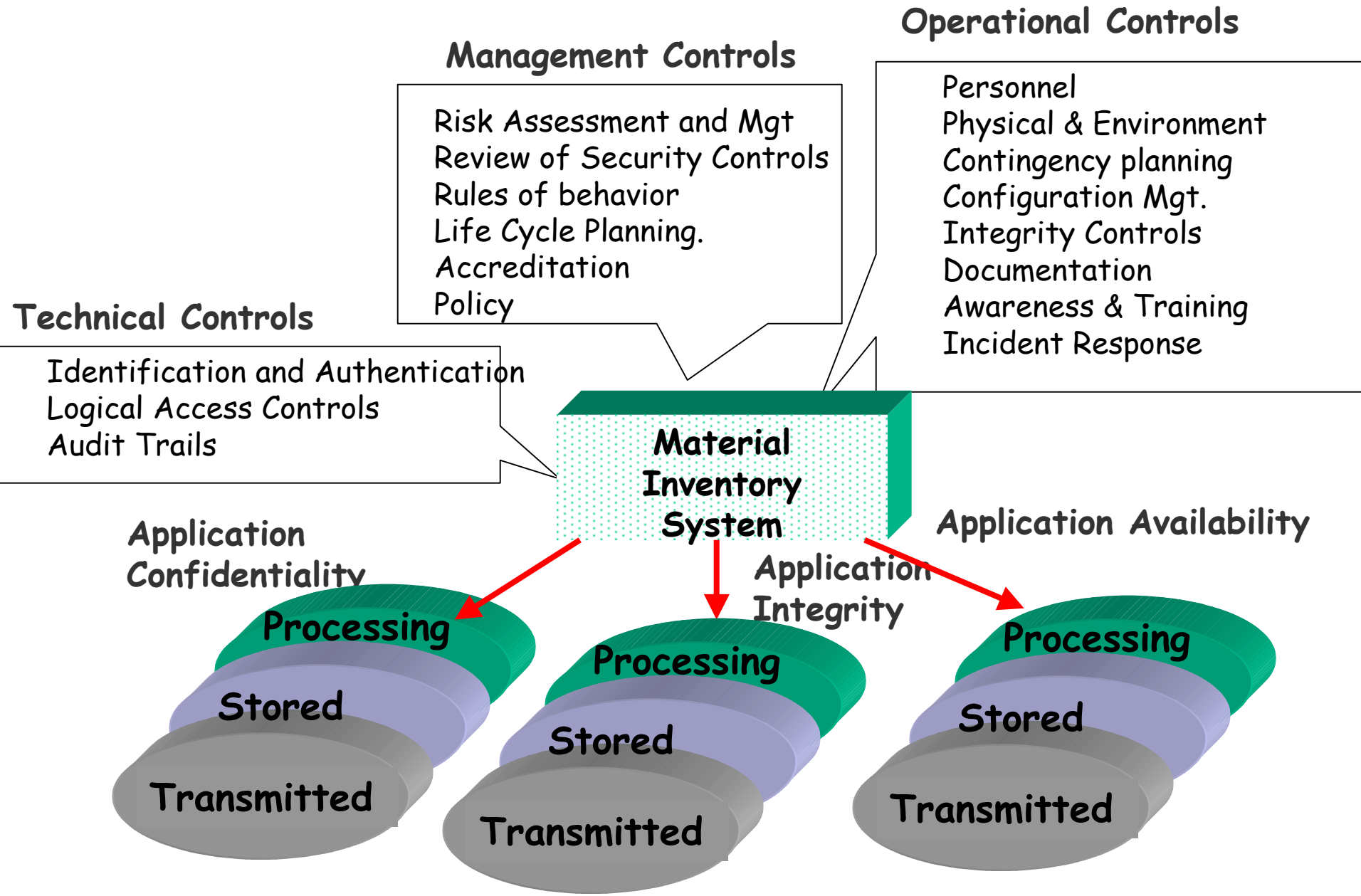
Systems that perform clearly defined functions for which there are identifiable security considerations and needs

(Designers & Builder's View)



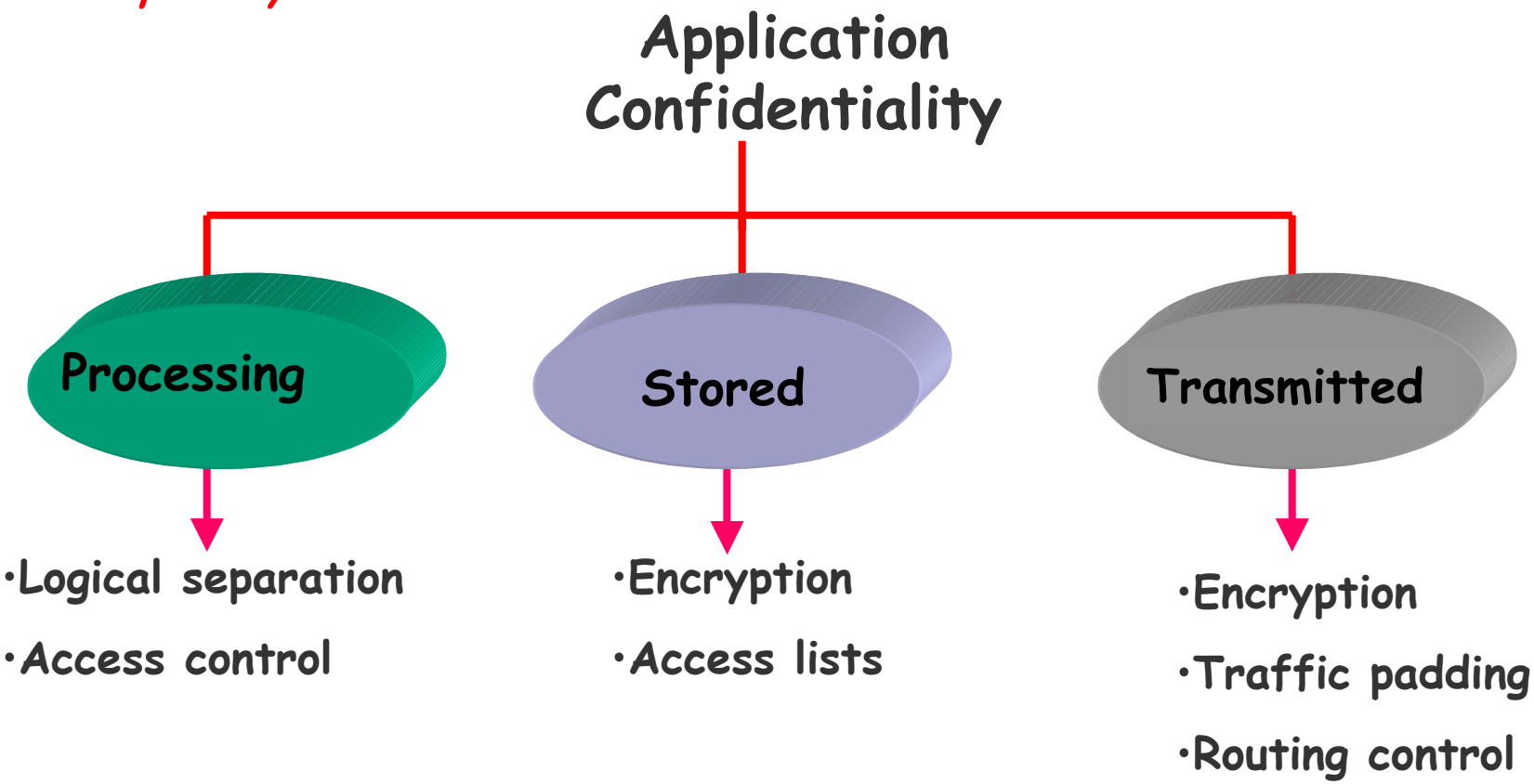
From OMB A-130 Appendix III

Application Security



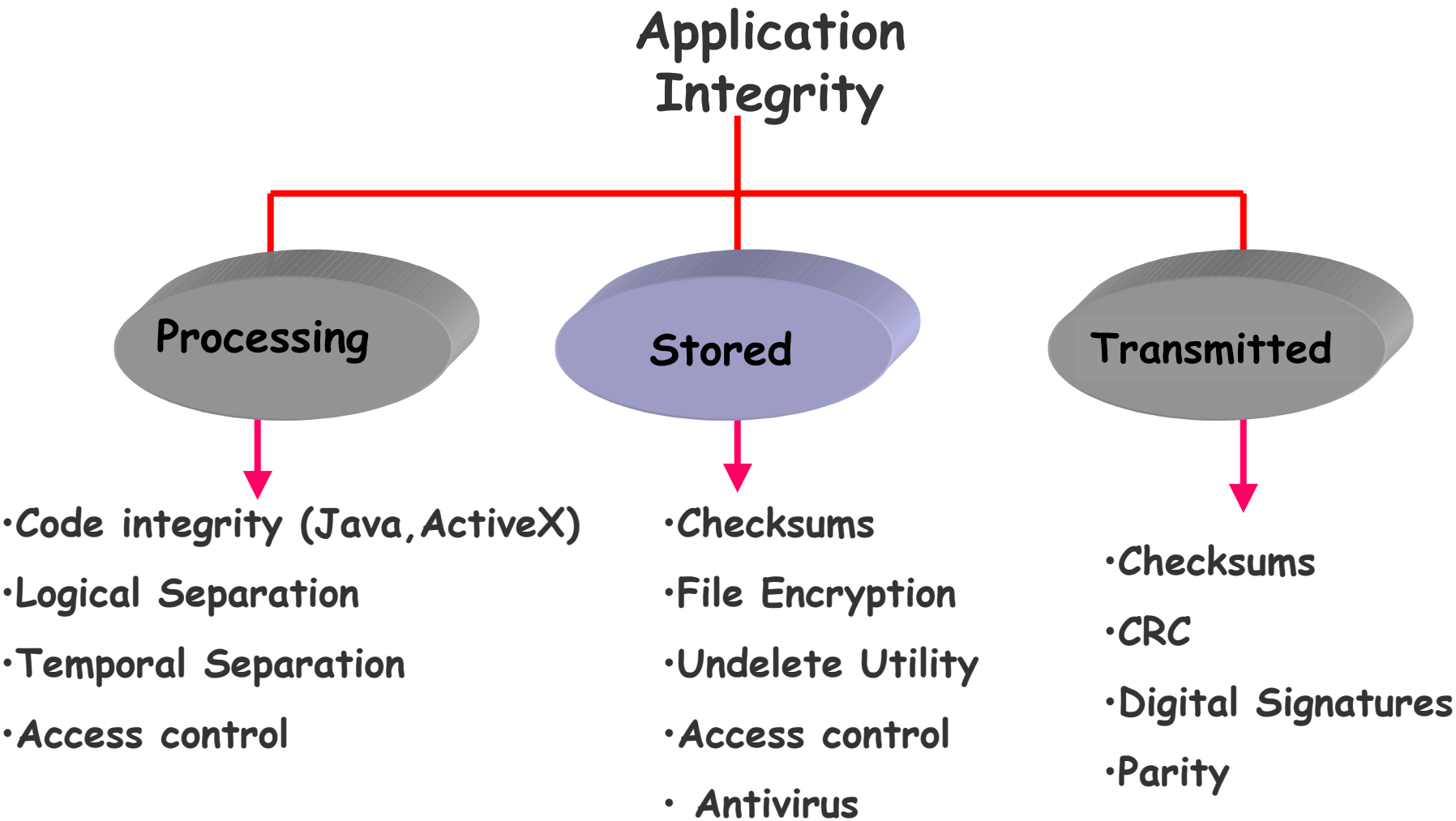
Application Confidentiality

Confidentiality in a computing or networked system means that information is disclosed only in accordance with policy



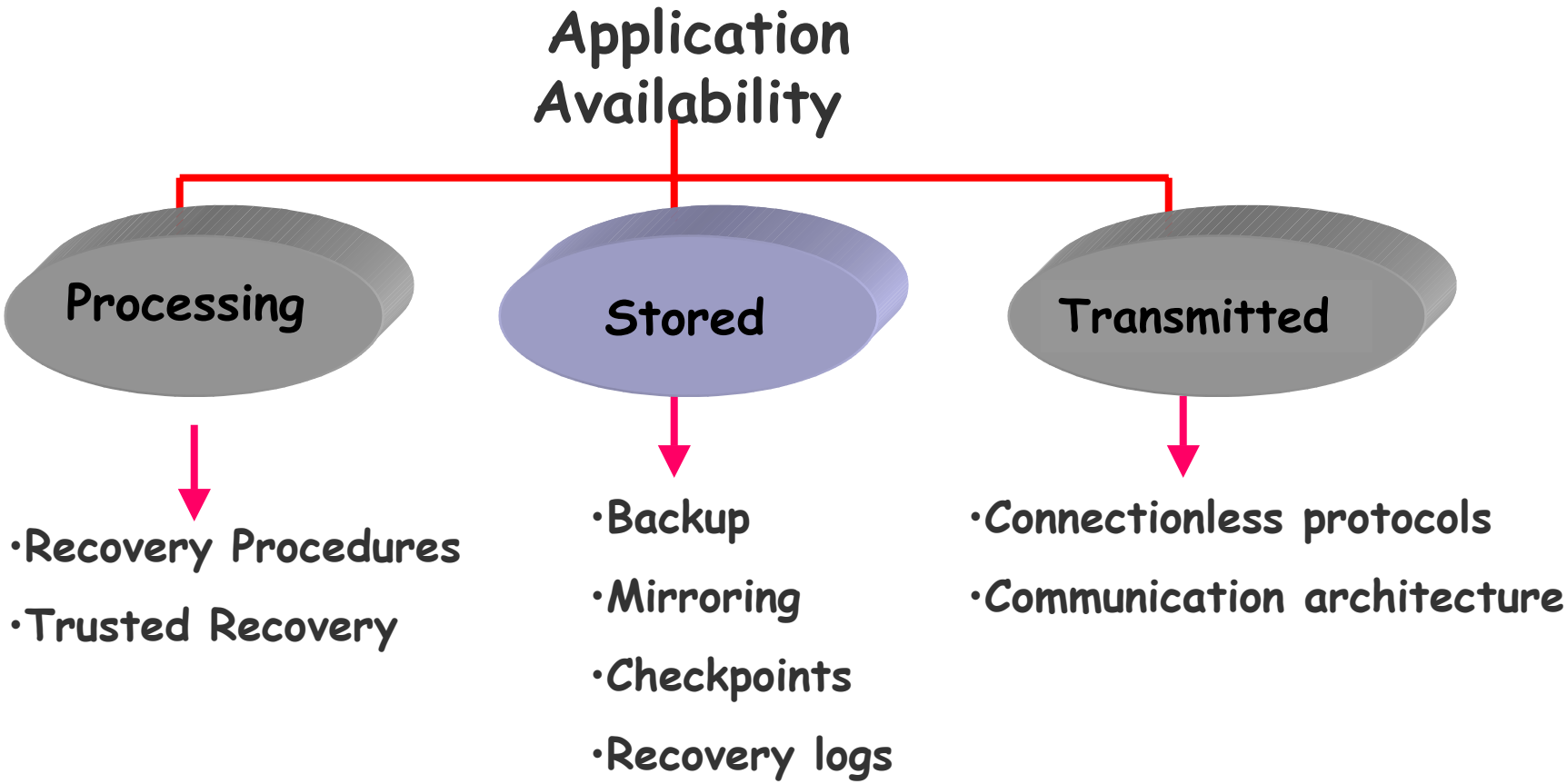
Application Integrity

Integrity means that data is not destroyed or corrupted and that the system performs correctly.



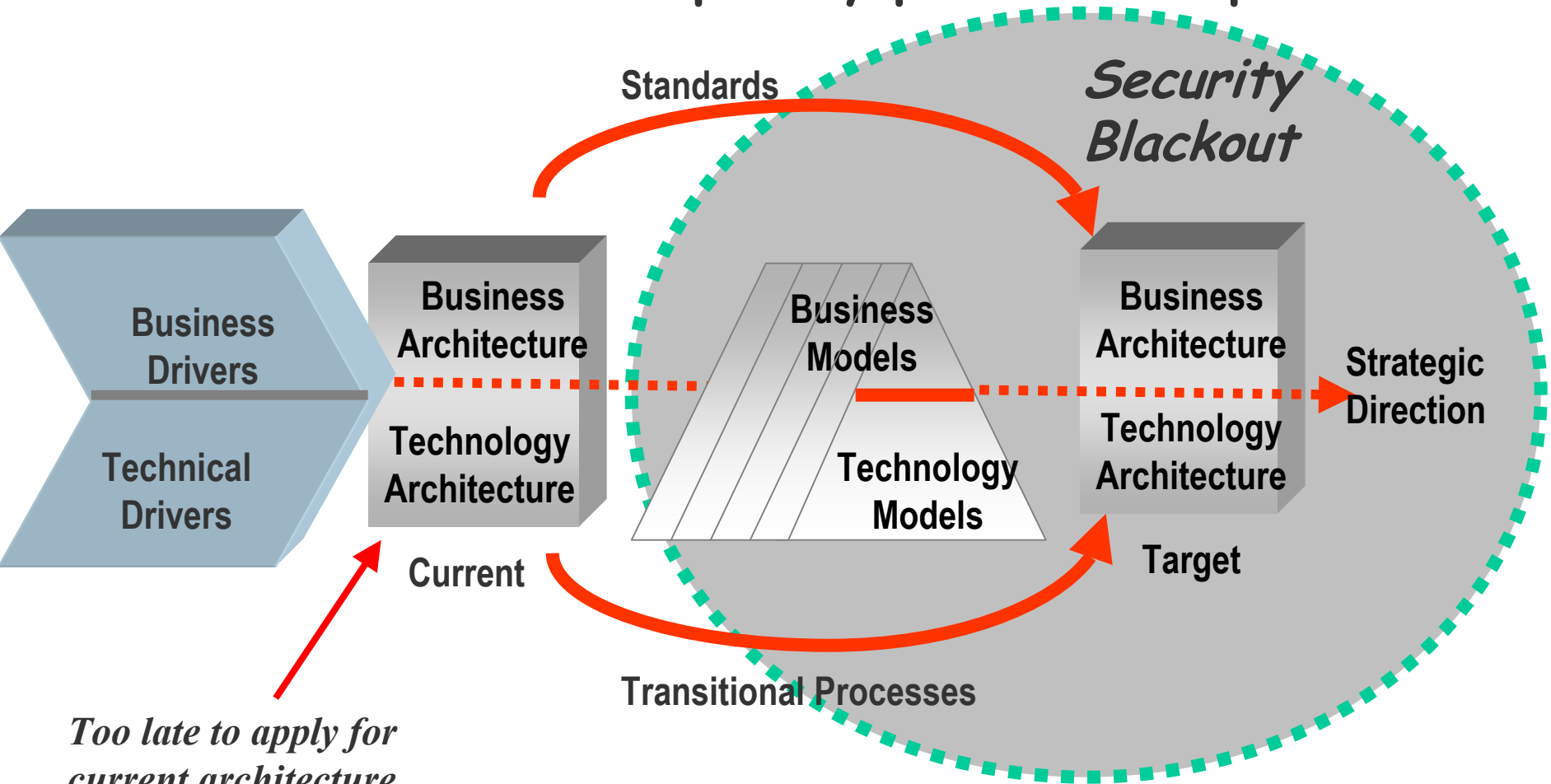
Application Availability

Addresses how systems restart after failure and preserve security and how systems protect the integrity of system and user objects against failure



Information Security Superstructure

That which is not expressly permitted is prohibited



All transitions are initially turned off

Negotiated Security

- All transitions are initially prohibited
- Designers negotiate with CIO's centralized security group for transition approval
- EDP auditors ensure security testability in design
- Transitions are introduced one-by-one after justification
- The security blackout envelope disappears after complete negotiation at all architectural levels

In this manner security becomes an overarching consideration which ensures integration at all levels

Conclusions

- Existing frameworks do not necessarily support security
- Security should be given the highest priority
- Security may need its own process
- High-level management support is crucial
- Security governance is a hot issue
- Enterprise security technologies are still maturing