RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SEM-M04D

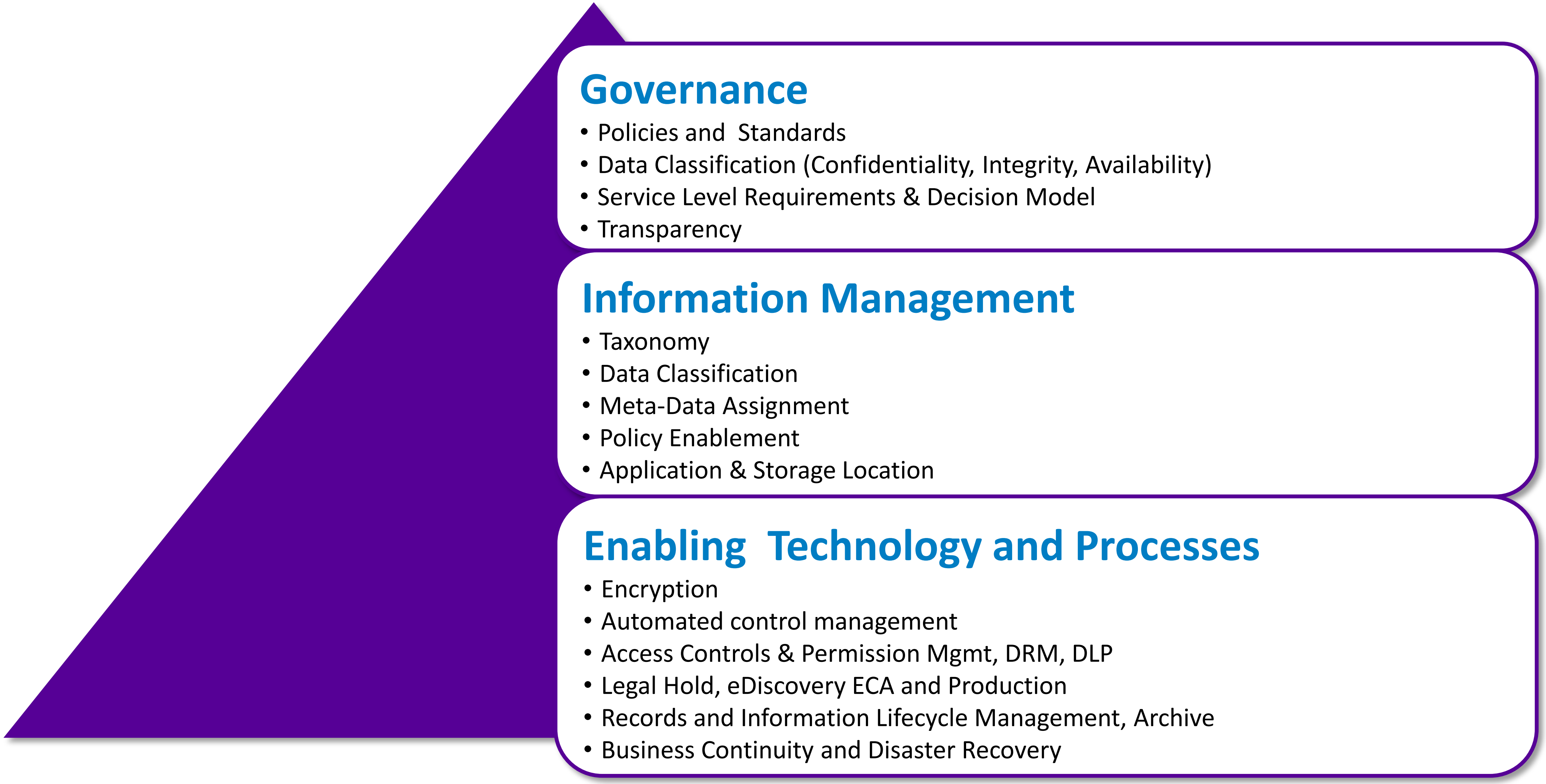
Common Security Frameworks

Kathleen M. Moriarty

Global Lead Security Architect
Dell EMC Office of the CTO
@KathleeMoriarty

Frameworks in Context of Business and Risk Tolerance

Frameworks to manage policy considering risk



Governance

- Policies and Standards
- Data Classification (Confidentiality, Integrity, Availability)
- Service Level Requirements & Decision Model
- Transparency

Information Management

- Taxonomy
- Data Classification
- Meta-Data Assignment
- Policy Enablement
- Application & Storage Location

Enabling Technology and Processes

- Encryption
- Automated control management
- Access Controls & Permission Mgmt, DRM, DLP
- Legal Hold, eDiscovery ECA and Production
- Records and Information Lifecycle Management, Archive
- Business Continuity and Disaster Recovery

NIST SP800-37 Risk Management Framework

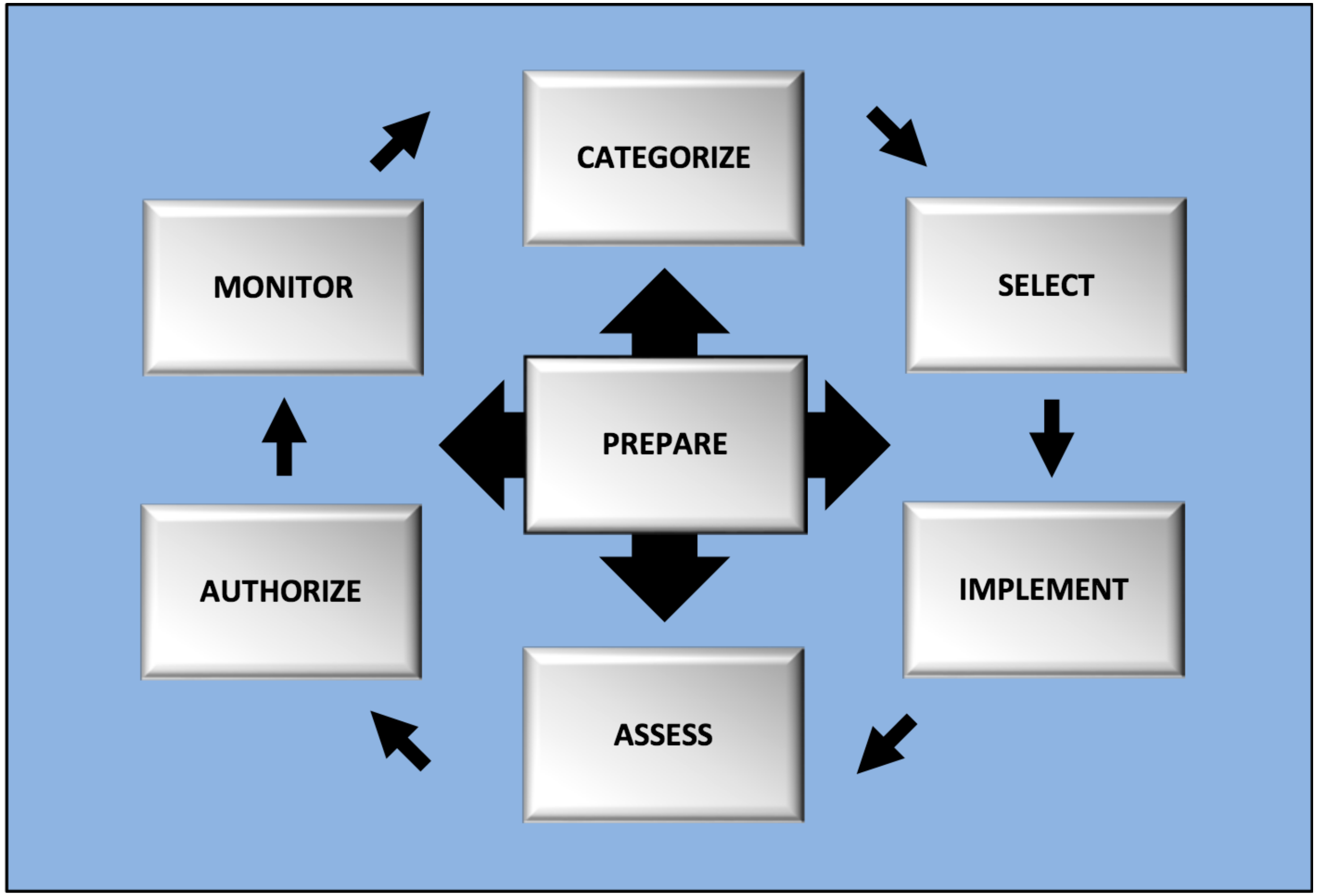


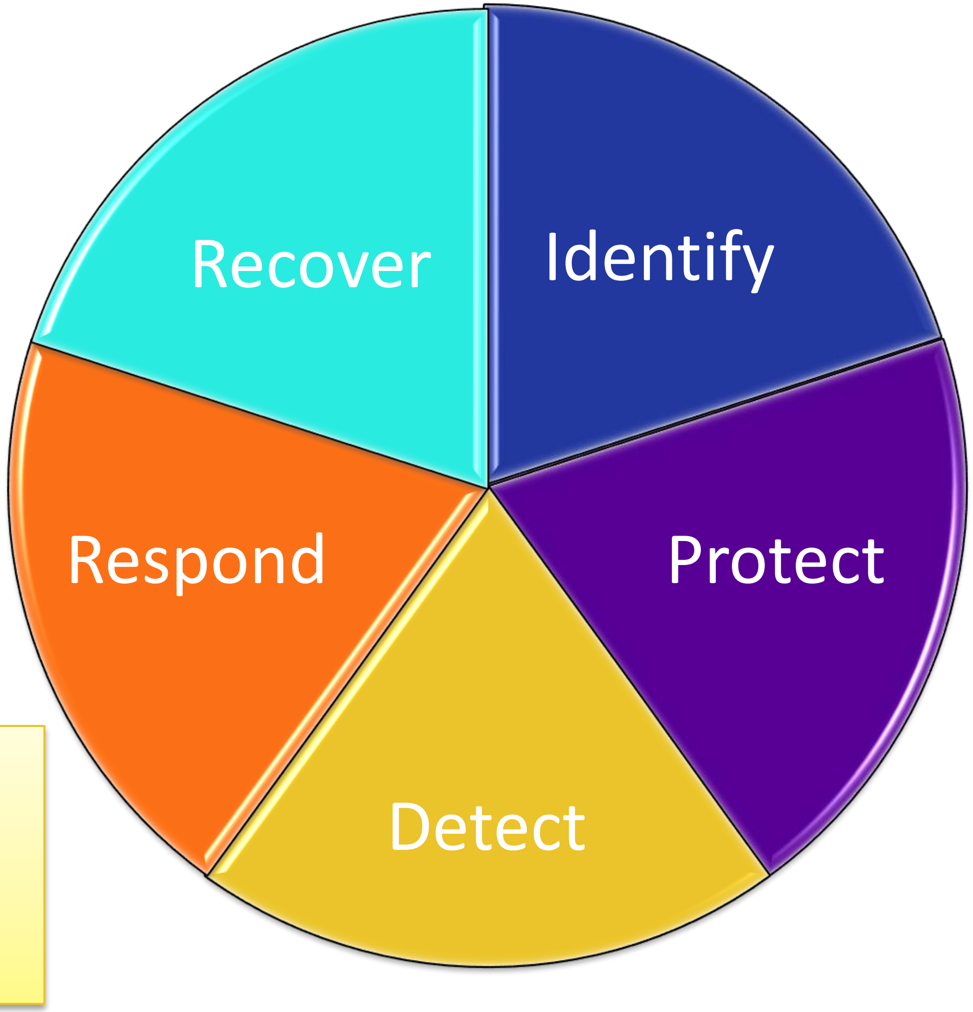
FIGURE 2: RISK MANAGEMENT FRAMEWORK

NIST CyberSecurity Framework version 1.1

- Recovery Planning
- Improvements

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes



- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Security and Privacy Controls for Federal Information Systems and Organizations: NIST SP 800-53

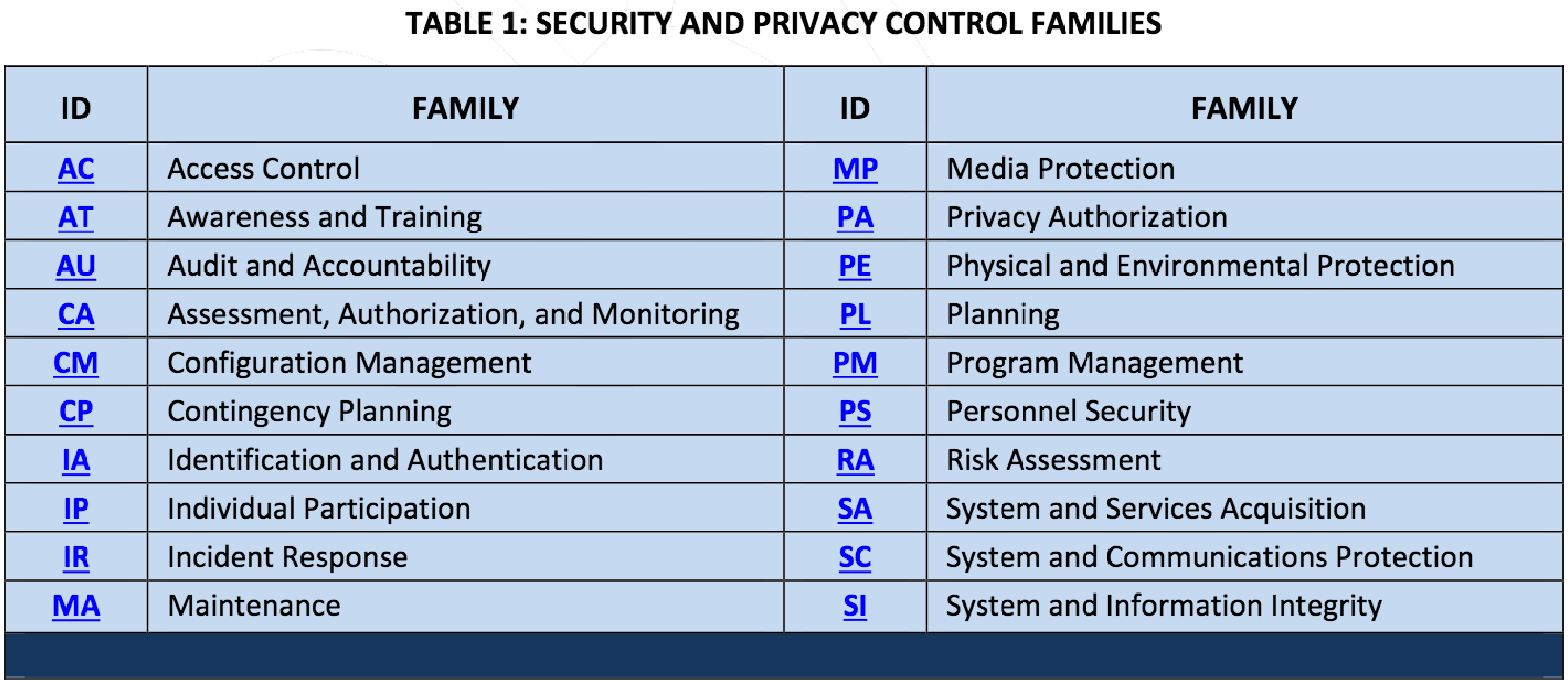


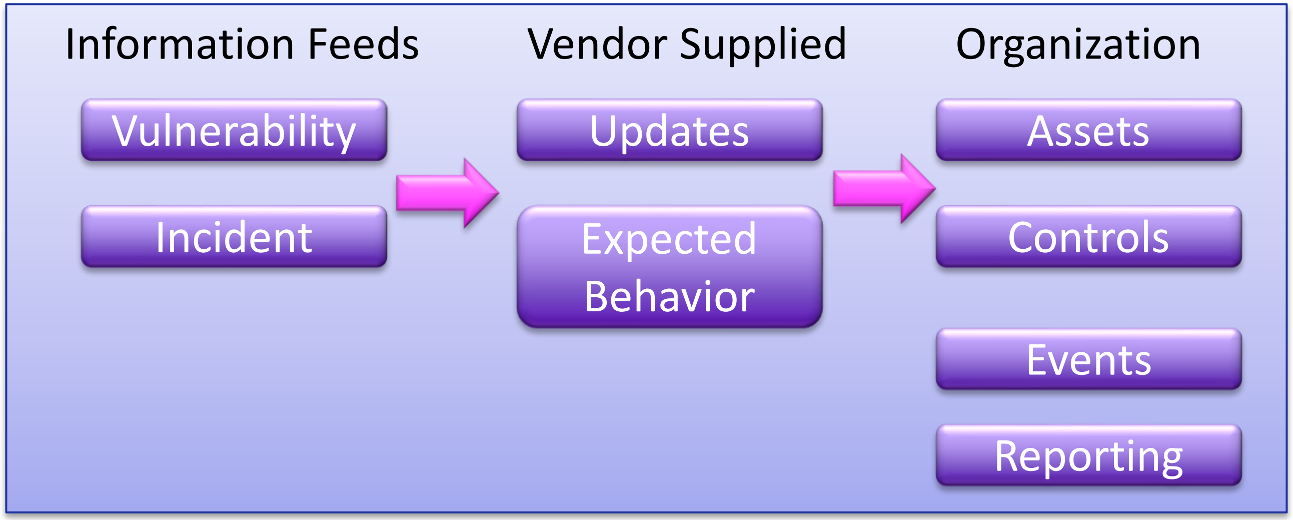
TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

ISO 27000 and Control Automation

	ISO 27002 Control Domains
4	Risk Assessment and Treatment
5	Security Policy
6	Organization of Information Security
7	Asset Management
8	Human Resources Management
9	Physical and Environmental Security
10	Communications and Operations Management
11	Access Control
12	Information Systems Acquisition, Development and Maintenance
13	Incident Management
14	Business Continuity
15	Compliance

Security Automation



Information Feeds

Vulnerability

Incident

Vendor Supplied

Updates

Expected Behavior

Organization

Assets

Controls

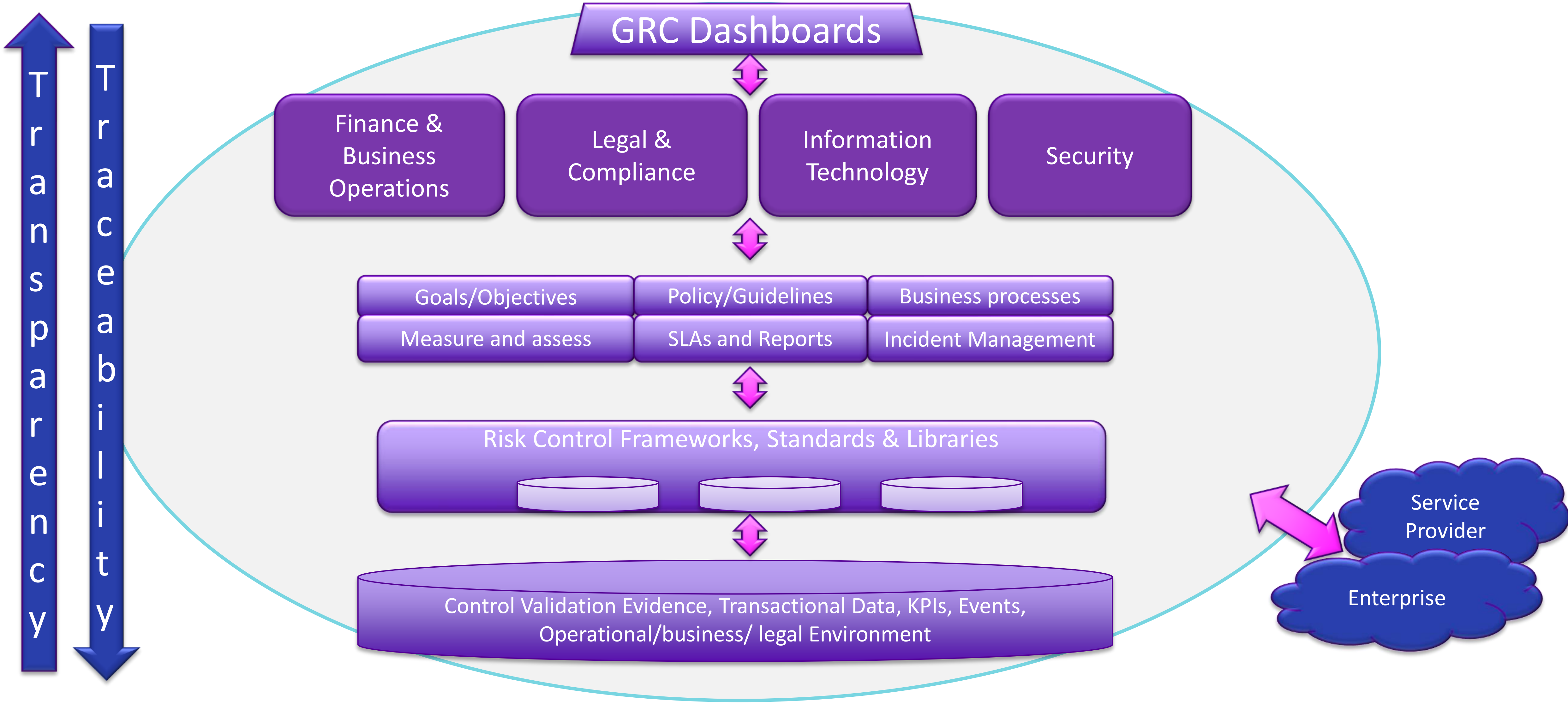
Events

Reporting

- Security Assessments mapped to holistic controls in framework enables:
  - Transparency of IT and security posture
  - Risk understanding and prioritization
  - Comparison of security for multiple environments
  - Regulatory and policy compliance reporting

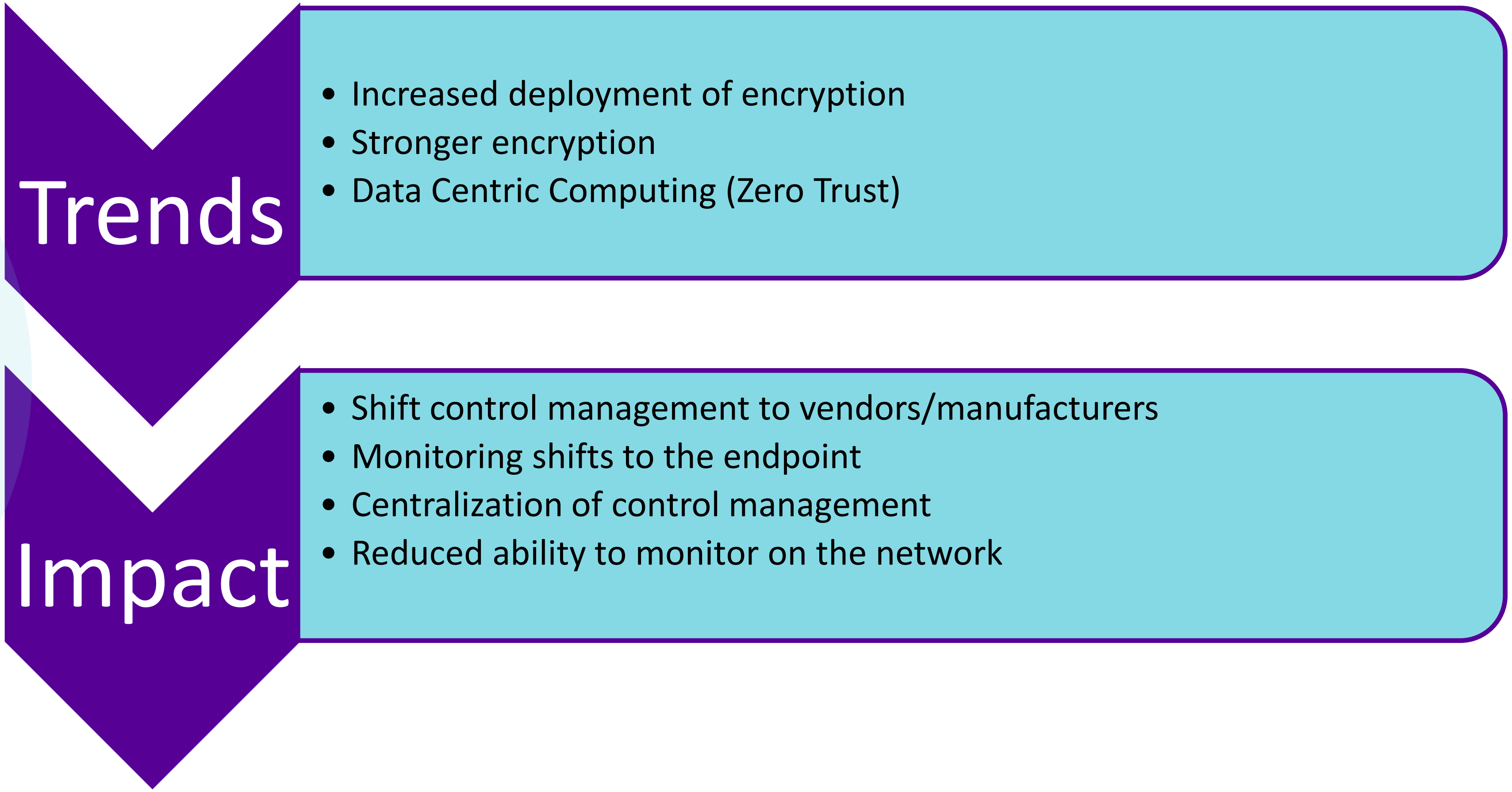
Note: Framework interchangeable with other frameworks or regulations

GRC Automation



Protocol evolution driving change

5 year outlook



Trends

- Increased deployment of encryption
- Stronger encryption
- Data Centric Computing (Zero Trust)

Impact

- Shift control management to vendors/manufacturers
- Monitoring shifts to the endpoint
- Centralization of control management
- Reduced ability to monitor on the network

Transport Encryption Evolving

TLSv1.3

IMPROVED PROTECTION AGAINST INTERCEPTION

- Public-key exchange mechanisms provide forward secrecy
- More secure key exchange based on the Elliptic Curve Diffie-Hellman algorithm
- Static RSA and Diffie-Hellman cipher suites deprecated
- Supported symmetric algorithms are Authenticated Encryption with Associated Data (AEAD)

QUICK UDP INTERNET CONNECTIONS (QUIC) ↗

- QUIC ↗ protocol is UDP-based
- Provides stream-multiplexing
- encrypted transport protocol
- Uses TLSv1.3 used by default

TCPcrypt

- Opportunistic security applied to TCP
- Header in clear text
- Eases configuration automation
- Used with TCP Encryption Negotiation Option (TCP-ENO)

Reducing Risk Considering Scale

Control management must scale to be effective

- Automate control management according to policy
- Automate security functions where possible
  - Automated Certificate Management Environment (ACME)
  - Manufacturer Usage Description (MUD)
  - Software Updates for Internet of Things (SUIT)
  - YANG
  - Security Content Automation Protocol (SCAP)
  - Common Information Model (CIM)
- Hybrid computing models
  - Organization’s Data Center
  - Zero Trust
    - Outsources control management and
    - Centralizes analysts assisting with scale

Apply

- Immediate
  - Evaluate current policies, procedures, and guidelines look for automation possibilities
  - Research automation options for your environment (YANG, SNMP, OVAL, NETCONF/RESTCONF)
- Three months to two years
  - Implement automated controls where possible – (SCAP, MUD, etc.)
  - Move to continuous audit cycles (automated and manual)
- One to two year progression
  - Migrate to more secure transport encryption options
  - Implement strong authentication for data centric security models
  - Reduce overall risk posture and management

RSAConference2019

Thank you!

Kathleen.Moriarty <at> dell.com

@KathleeMoriarty