Developments in Cloud and IT/Security Assurance

Mark Lundin, Partner, KPMG

Governance, Risk & Compliance – G31

2014 Fall Conference - "Think Big"

Agenda

Overview of SOC1/SSAE16 and SOC2/SOC3 reports

Trends in cloud/IT outsourcing

Effectively transitioning to the updated SOC2/SOC3 criteria effective 12/15/14

Using attestation reports to help address industry/regulatory requirements

Changing international standards and requirements

Cloud infrastructure governance, risk and controls

Overview of SOC1/SSAE16 and SOC2/SOC3 reports

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Service Organization Control (SOC) Reports Overview

Scope/Focus	Report Type	Summary
Internal Control Over Financial Reporting (ICOFR)	**SOC1** **(SSAE16, ISAE 3402)**	**Detailed report relevant to ICOFR based on control objectives defined by the service provider**
Operational Controls • **Security, Availability, Confidentiality, Processing Integrity, and/or Privacy**	**SOC2**	**Detailed report based on Trust Services Principles and Criteria**
	SOC2 Enhanced Reporting	**Detailed report with additional controls and mappings added to show alignment with other standards/frameworks such as ISO 27001, CSA-CCM, HIPAA Security, etc.**
	SOC3	**Short report that excludes the detail of controls and test procedures performed.**

- **These reports are typically Type 2 reports covering design and effectiveness for a period of time.**
- **In some cases Type 1 point in time design reports may also be useful.**

Trends in cloud/IT outsourcing

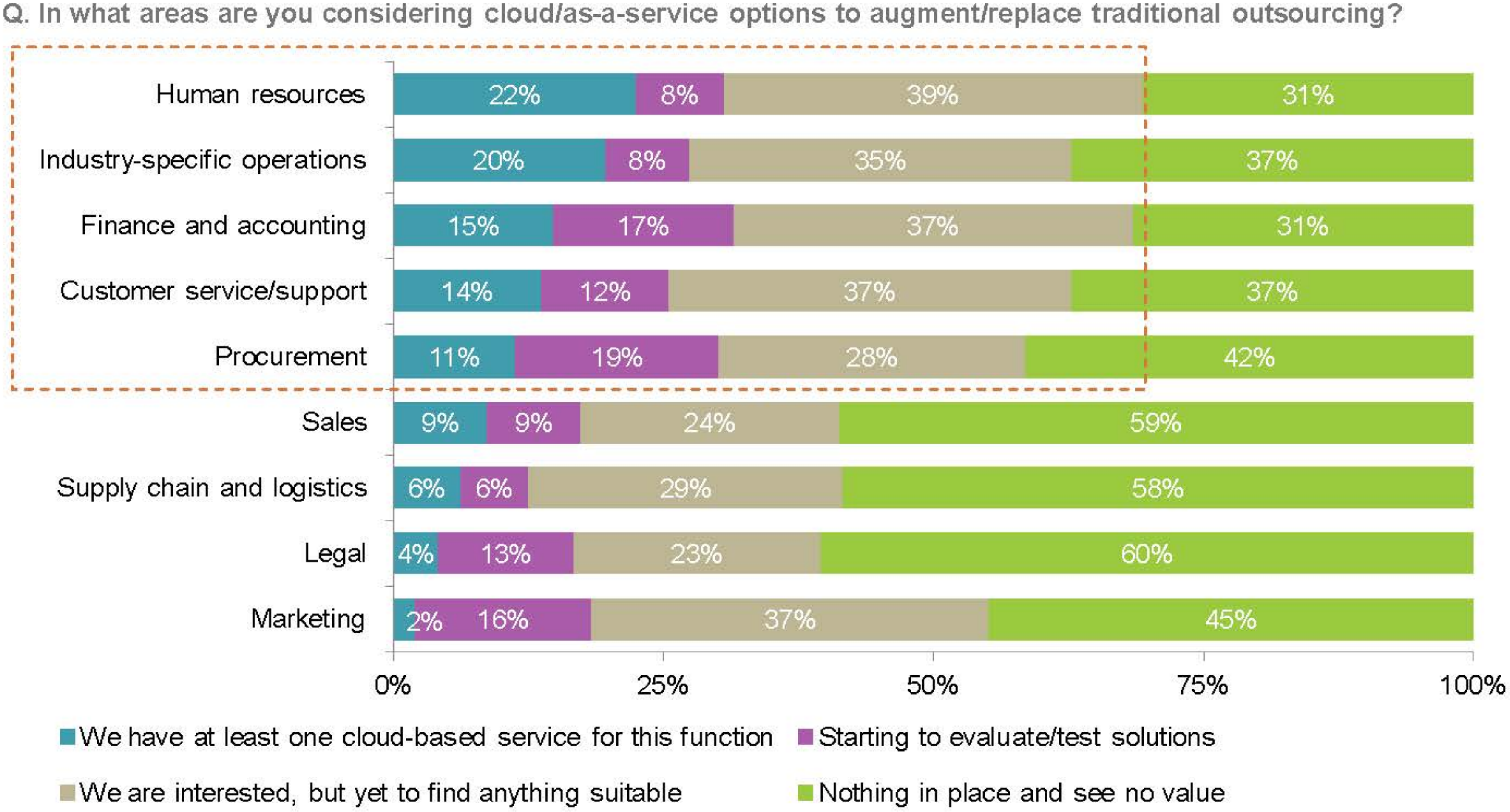
Highlights from KPMG and HfS Research, Executive report: The State of Services & Outsourcing in 2014

The conversation is moving rapidly away from process improvement and cost reduction. Anything rules-based must be automated/moved into the cloud/outsourced.

Both shared services and outsourcing are on the increase. One in four enterprise buyers are reinvesting heavily in their global shared services operations, while seven out of ten are continuing to make (largely moderate) investments in their outsourcing delivery.

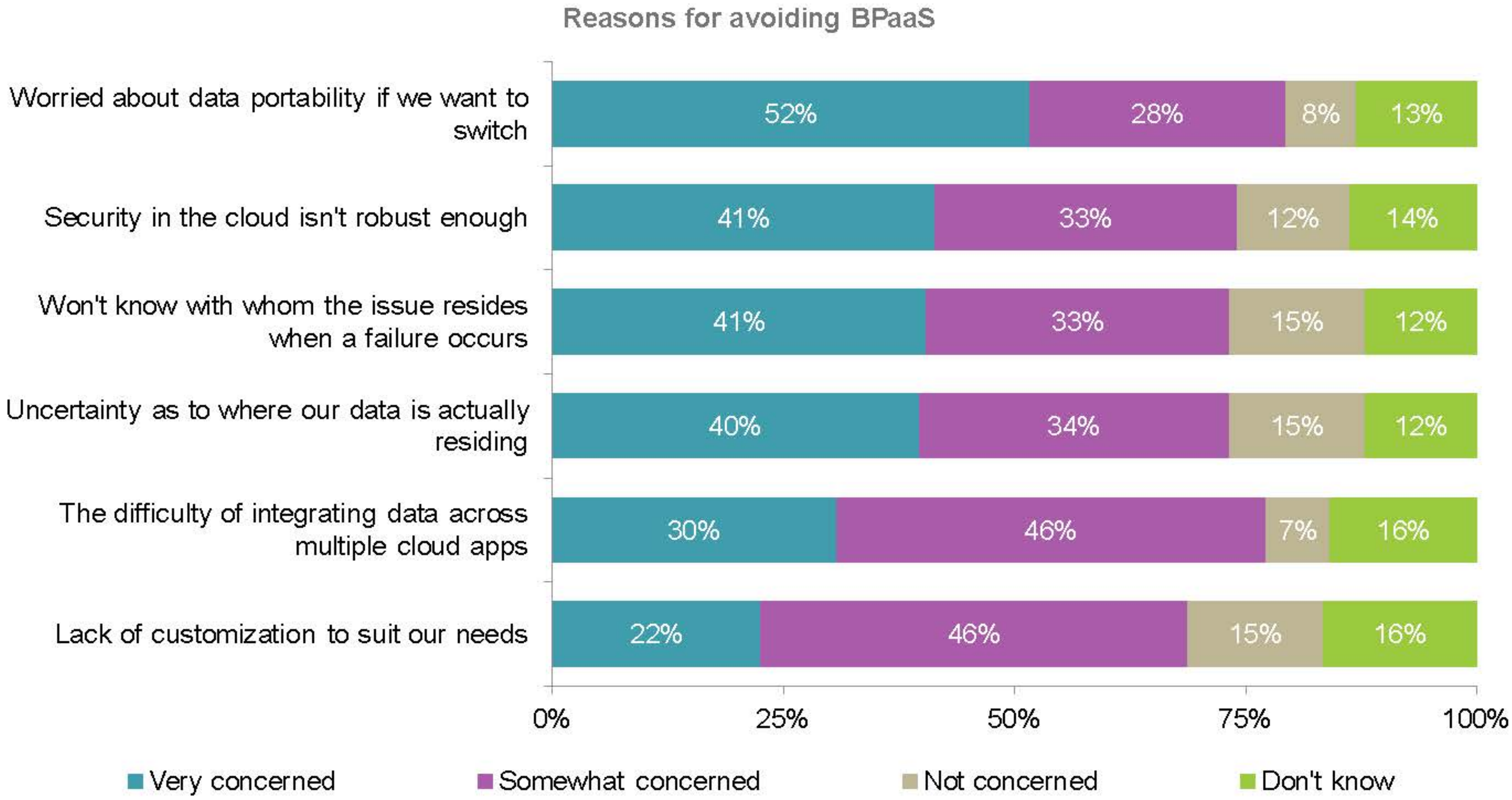
Ambitious and sophisticated clients are now seeing the huge benefits of shifting from on-premise to as-a-Service delivery and many now view BPaaS as an alternative to outsourcing. This isn't something that is occurring in a few years, it's already happening where our latest research shows close to one-in-three enterprises already using (or about to use) BPaaS/cloud as an alternative to legacy outsourcing in areas such as HR, industry-specific operations, finance and accounting, and procurement.

BPaaS is already replacing legacy outsourcing



Source: HfS Research State of Industry Study June 2014, conducted in conjunction with KPMG. (Sample 312 Enterprises)

Cloud concerns



n =740 IT Managers in Enterprises

Source: HfS Research 2014.

Effectively transitioning to the updated SOC2/SOC3 criteria effective 12/15/14

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Trust Services Criteria Summary – 2014 Update

Common Security Criteria

- Organization and management
- Communications
- Risk Management and Design and Implementation of Controls
- Monitoring of Controls
- Logical and Physical Access Controls
- System Operations
- Change Management

Availability

- Capacity management
- Environmental and backup controls
- Disaster recovery

Confidentiality

- Life cycle protection
- Access from within and outside system
- Vendor commitments and compliance
- Changes to commitments

Processing Integrity

- Error handling
- System inputs
- Data processing
- Data retention
- System output
- Data modification

- **The Trust Services Criteria (excluding Privacy) were updated in February 2014.**
- **The updated criteria are effective for periods ending on or after December 15, 2014.**
- **The updates include simplification of the structure and increased focus on risk assessment.**

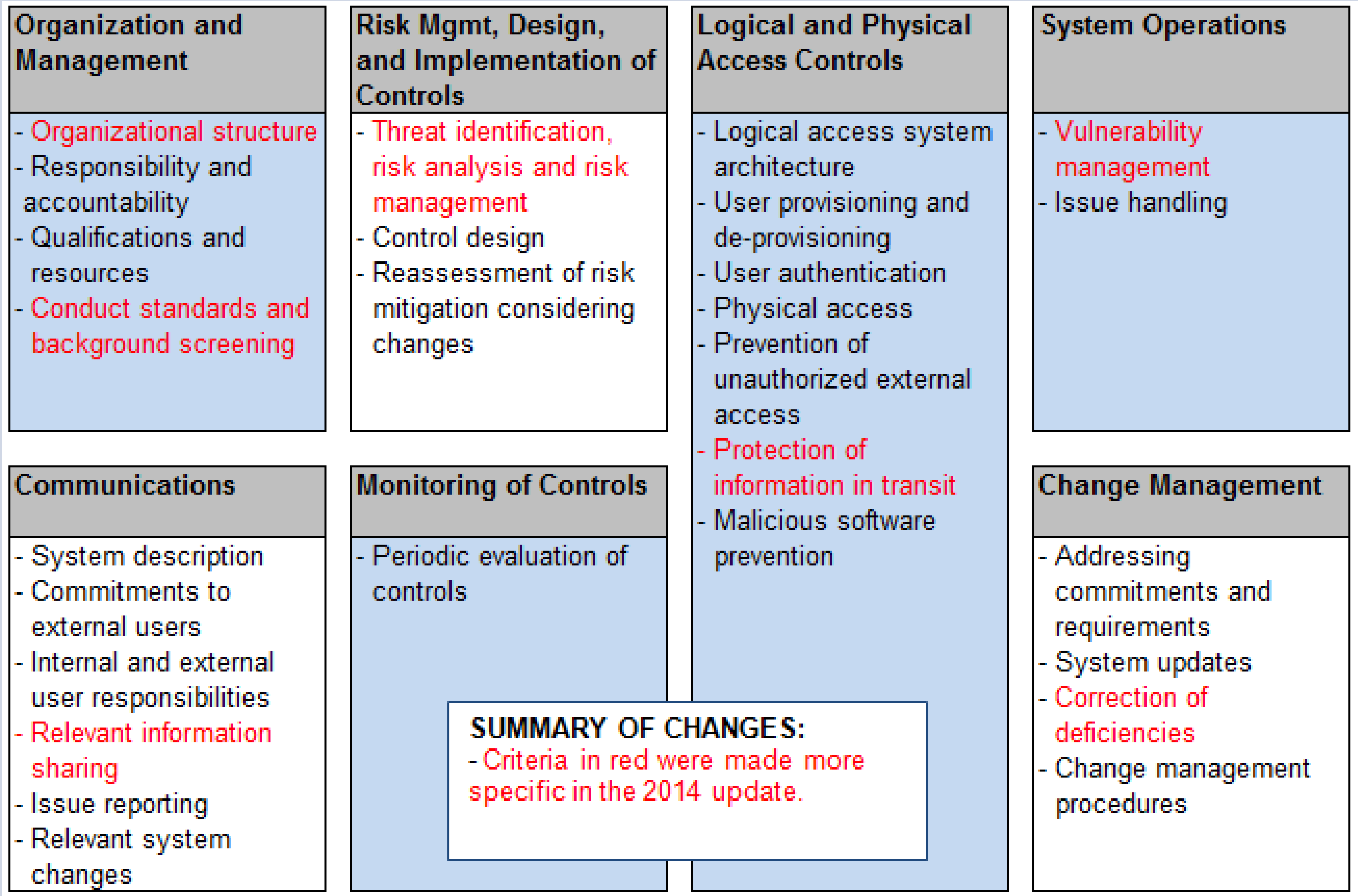
Basic steps to complete preparations for the updated criteria

Realign controls based on new criteria structure

Link risk assessment to Trust Services Criteria

Verify controls are in place to address new criteria

Summary of Changes
Common Criteria – Security



Organization and Management

- Organizational structure
- Responsibility and accountability
- Qualifications and resources
- Conduct standards and background screening

Risk Mgmt, Design, and Implementation of Controls

- Threat identification, risk analysis and risk management
- Control design
- Reassessment of risk mitigation considering changes

Logical and Physical Access Controls

- Logical access system architecture
- User provisioning and de-provisioning
- User authentication
- Physical access
- Prevention of unauthorized external access
- Protection of information in transit
- Malicious software prevention

System Operations

- Vulnerability management
- Issue handling

Communications

- System description
- Commitments to external users
- Internal and external user responsibilities
- Relevant information sharing
- Issue reporting
- Relevant system changes

Monitoring of Controls

- Periodic evaluation of controls

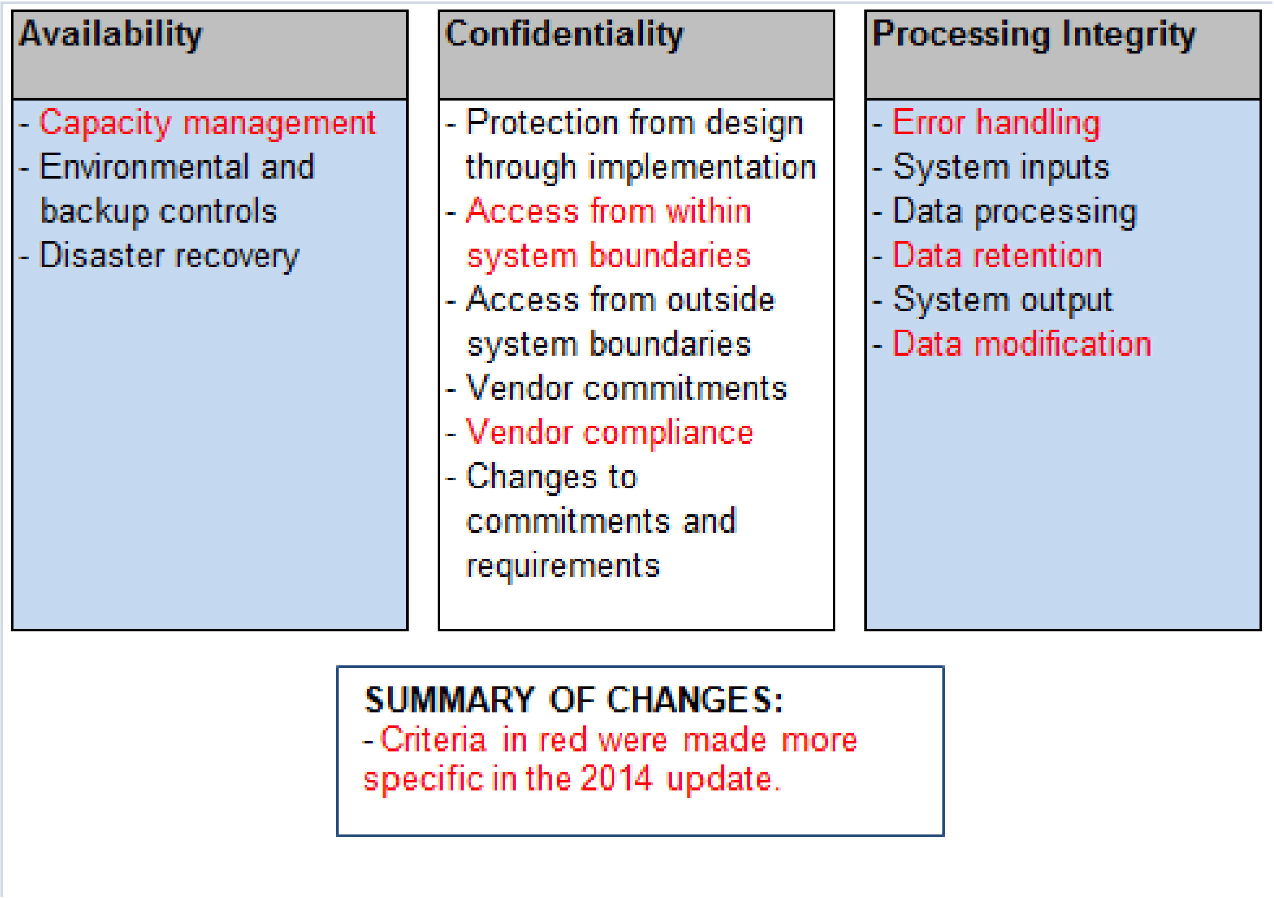
Change Management

- Addressing commitments and requirements
- System updates
- Correction of deficiencies
- Change management procedures

SUMMARY OF CHANGES:

- Criteria in red were made more specific in the 2014 update.

Summary of Changes – Availability, Confidentiality, Processing Integrity



Availability	Confidentiality	Processing Integrity
- Capacity management - Environmental and backup controls - Disaster recovery	- Protection from design through implementation - Access from within system boundaries - Access from outside system boundaries - Vendor commitments - Vendor compliance - Changes to commitments and requirements	- Error handling - System inputs - Data processing - Data retention - System output - Data modification

SUMMARY OF CHANGES:

- Criteria in red were made more specific in the 2014 update.

Changes to Common Criteria – Security

Ref.	Criteria Topic	Change Summary
CC1	**Organization and Management**	
CC1.1	**Organizational structure**	■ **Made more specific – called out as a separate topic**
CC1.2	**Responsibility and accountability**	
CC1.3	**Qualifications and resources**	
CC1.4	**Conduct standards and background screening**	■ **Made more specific – calling out background screening**
CC2	**Communications**	
CC2.1	**System description**	
CC2.2	**Commitments to external users**	
CC2.3	**Internal and external user responsibilities**	
CC2.4	**Relevant information sharing**	■ **Made more specific – called out as a separate topic**
CC2.5	**Issue reporting**	
CC2.6	**Relevant system changes**	

Changes to Common Criteria – Security (continued)

Ref.	Criteria Topic	Change Summary
CC3	**Risk Management and Design and Implementation of Controls**	
CC3.1	**Threat identification, risk analysis and risk management**	■ **Made more specific – tying risk analysis to controls**
CC3.2	**Control design**	
CC3.3	**Reassessment of risk mitigation considering changes**	■ **Made more specific – focusing on actions taken**
CC4	**Monitoring of Controls**	
CC4.1	**Periodic evaluation of controls**	■ **Made more specific – focusing on design and operating effectiveness, and actions taken**

Changes to Common Criteria – Security (continued)

Ref.	Criteria Topic	Change Summary
CC5	**Logical and Physical Access Controls**	
CC5.1	**Logical access system architecture**	
CC5.2	**User provisioning and de-provisioning**	
CC5.3	**User authentication**	
CC5.4	**Access privilege management**	
CC5.5	**Physical access**	
CC5.6	**Prevention of unauthorized external access**	
CC5.7	**Protection of information in transit**	■ **Made more specific – calling out transmission, movement and removal**
CC5.8	**Malicious software prevention**	

Changes to Common Criteria – Security (continued)

Ref.	Criteria Topic	Change Summary
CC6	**System Operations**	
CC6.1	**Vulnerability management**	**Made more specific – adding emphasis to evaluation and counter-measures**
CC6.2	**Issue handling**	
CC7	**Change Management**	
CC7.1	**Addressing commitments and requirements**	
CC7.2	**System updates**	
CC7.3	**Correction of deficiencies**	**Made more specific – called out as a separate topic**
CC7.4	**Change management procedures**	

Changes to Common Criteria – Security (continued)

Ref.	Criteria Topic	Change Summary
CC6	**System Operations**	
CC6.1	**Vulnerability management**	■ **Made more specific – adding emphasis to evaluation and counter-measures**
CC6.2	**Issue handling**	
CC7	**Change Management**	
CC7.1	**Addressing commitments and requirements**	
CC7.2	**System updates**	
CC7.3	**Correction of deficiencies**	■ **Made more specific – called out as a separate topic**
CC7.4	**Change management procedures**	

Changes to Criteria – Availability and Confidentiality

Ref.	Criteria Topic	Change Summary
A	**Availability**	
A1.1	**Capacity management**	■ Made more specific – calling out capacity management
A1.1	**Environmental and backup controls**	
A1.2	**Disaster recovery**	
C	**Confidentiality**	
C1.1	**Protection from design through implementation**	
C1.2	**Access from within system boundaries**	■ Made more specific – called out as a separate topic
C1.3	**Access from outside system boundaries**	
C1.4	**Vendor commitments**	
C1.5	**Vendor compliance**	■ Made more specific – adding focus on monitoring and action taken
C1.6	**Changes to commitments and requirements**	

Changes to Criteria – Processing Integrity

Ref.	Criteria Topic	Change Summary
PI	**Processing Integrity**	
PI1.1	**Error handling**	▪ Made more specific – now called out as a separate topic
PI1.2	**System inputs**	
PI1.3	**Data processing**	
PI1.4	**Data retention**	▪ Made more specific – calling out data retention requirements
PI1.5	**System output**	
PI1.6	**Data modification**	▪ Made more specific – focusing on authorization rather than just database management

Privacy Criteria – 2015 Anticipated Updates

Current structure

Privacy (approximately 75 criteria including different security criteria)

- Management
- Notice
- Choice and consent
- Collection
- Use and retention
- Access
- Disclosure to third parties
- Security for privacy
- Quality
- Monitoring and enforcement

Anticipated new structure

Common Security Criteria

- Organization and Management
- Communications
- Risk Management and Design and Implementation of Controls
- Monitoring of Controls
- Logical and Physical Access Controls
- System Operations
- Change Management

Privacy (approximately 20 criteria)

- Notice
- Choice and Consent
- Collection
- Use, Retention and Disposal
- Access
- Disclosure and notification
- Quality
- Monitoring and Enforcement

Using attestation reports to help address industry/regulatory requirements

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

SOC2 Enhanced Reporting Overview

SOC2 Enhanced Reporting can potentially be used as a single framework to address multiple security-focused external compliance requirements.

Additional detail can be added to the SOC2 report to help address the needs of customers who have requirements related to other industry standards and frameworks

In most cases, the SOC2 Enhanced Report would cover the Trust Services Security and Availability criteria with additional controls and testing added to enable mapping to the relevant standards.

SOC2 Enhanced Reporting Examples

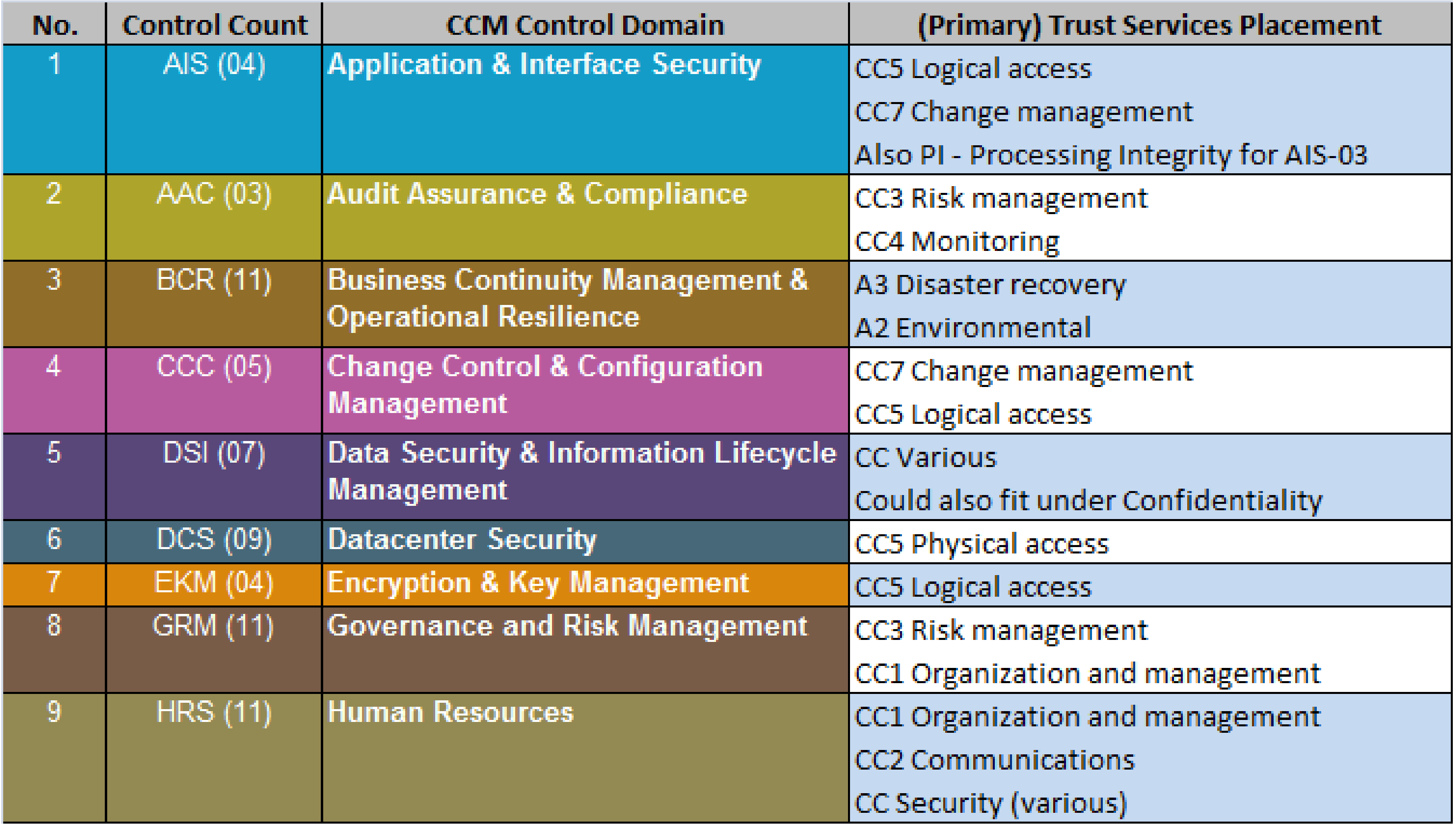
Standard/Framework	Potential Benefit
ISO 27001	Address security requirements of global customers Could serve as a replacement for, or interim step toward ISO certification
HIPAA Security Rule	Provide information on how the service provider’s controls align with the requirements of the rule
PCI DSS	Relevant to customers who may operate systems that process or store credit card account information
Cloud Security Alliance Cloud Controls Matrix	Addresses a framework for cloud providers that many customers are familiar with
NIST 800-53	Highly relevant standard to public sector customers
NIST Cybersecurity Framework	Relevant to third parties who are interested in the service provider’s cybersecurity efforts
Other Industry Specific Standards	Provides a mechanism to show alignment of controls with the particular industry standard

Typical format

Specific topics/ requirements from specified framework	Reference to Related Service Provider Controls	Reference to related SOC2 Criteria
Sec 1.1	<Include control description>	#.#
Sec 1.2	<Include control description>	#.#
Sec 1.3	<Include control description>	#.#
Sec 1.4	<Include control description>	#.#
Sec 1.5	<Include control description>	#.#
etc.	etc.	etc.

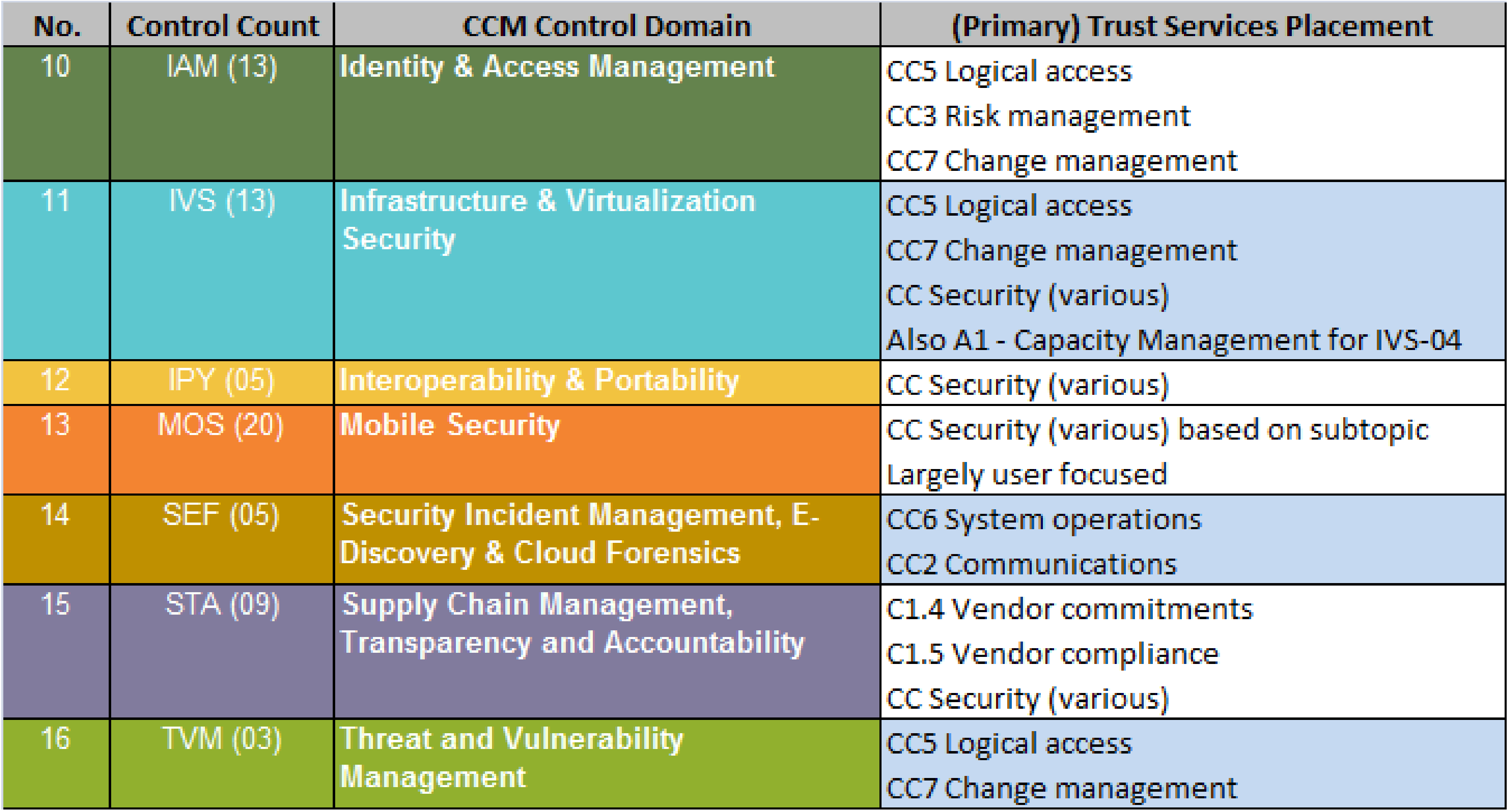
- This format can be used to map the service provider's SOC2 controls to the relevant parts of other applicable frameworks/standards.
- This information can be extremely helpful to customers whose vendor risk and compliance management programs or requirements include these other standards/frameworks.
- This information would normally be included in the Other Information portion of the SOC2 report.

Alignment of CCM 3.0.1 with the Trust Services Criteria



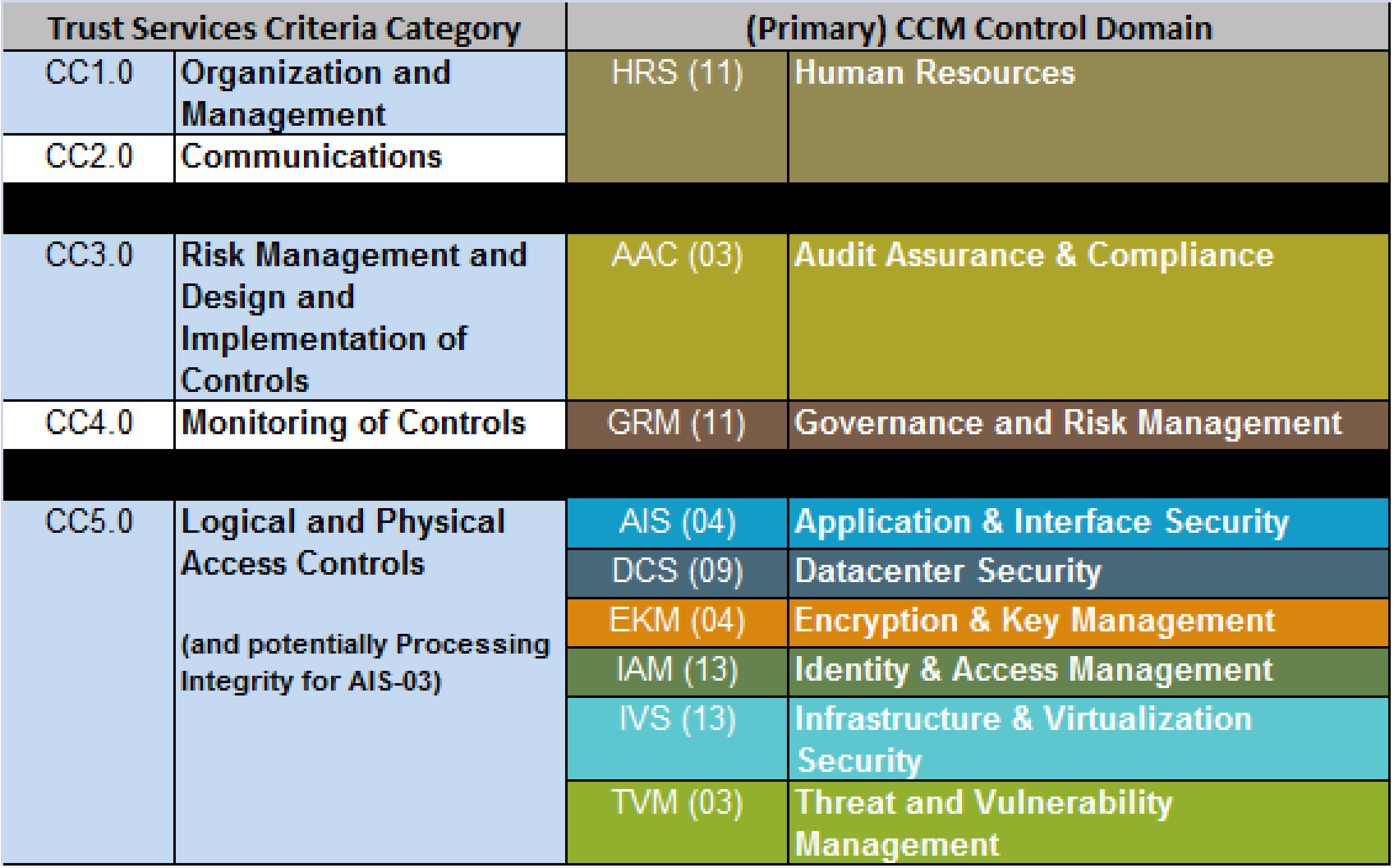
No.	Control Count	CCM Control Domain	(Primary) Trust Services Placement
1	AIS (04)	Application & Interface Security	CC5 Logical access CC7 Change management Also PI - Processing Integrity for AIS-03
2	AAC (03)	Audit Assurance & Compliance	CC3 Risk management CC4 Monitoring
3	BCR (11)	Business Continuity Management & Operational Resilience	A3 Disaster recovery A2 Environmental
4	CCC (05)	Change Control & Configuration Management	CC7 Change management CC5 Logical access
5	DSI (07)	Data Security & Information Lifecycle Management	CC Various Could also fit under Confidentiality
6	DCS (09)	Datacenter Security	CC5 Physical access
7	EKM (04)	Encryption & Key Management	CC5 Logical access
8	GRM (11)	Governance and Risk Management	CC3 Risk management CC1 Organization and management
9	HRS (11)	Human Resources	CC1 Organization and management CC2 Communications CC Security (various)

Alignment of CCM 3.0.1 with the Trust Services Criteria (continued)



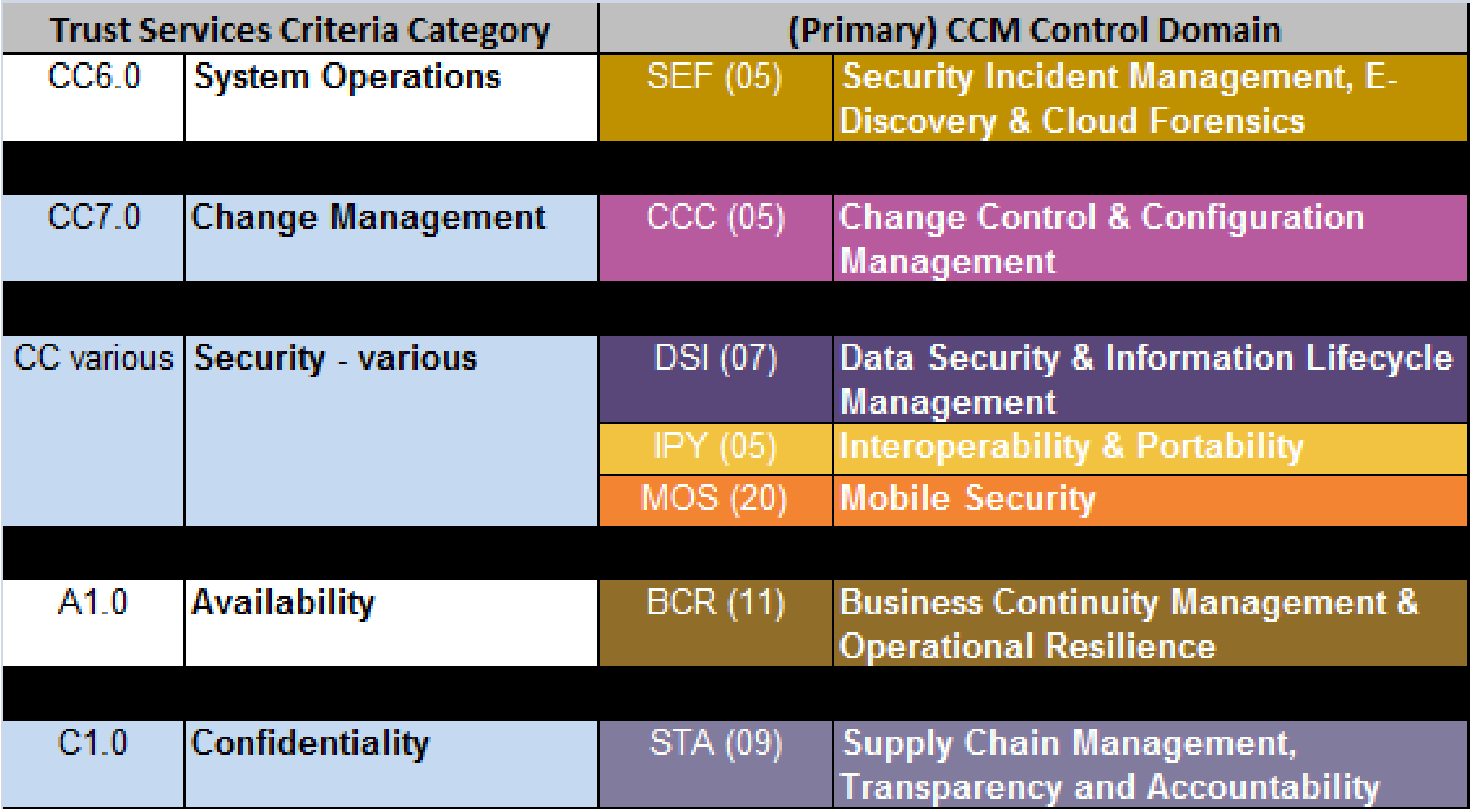
No.	Control Count	CCM Control Domain	(Primary) Trust Services Placement
10	IAM (13)	Identity & Access Management	CC5 Logical access CC3 Risk management CC7 Change management
11	IVS (13)	Infrastructure & Virtualization Security	CC5 Logical access CC7 Change management CC Security (various) Also A1 - Capacity Management for IVS-04
12	IPY (05)	Interoperability & Portability	CC Security (various)
13	MOS (20)	Mobile Security	CC Security (various) based on subtopic Largely user focused
14	SEF (05)	Security Incident Management, E-Discovery & Cloud Forensics	CC6 System operations CC2 Communications
15	STA (09)	Supply Chain Management, Transparency and Accountability	C1.4 Vendor commitments C1.5 Vendor compliance CC Security (various)
16	TVM (03)	Threat and Vulnerability Management	CC5 Logical access CC7 Change management

Addressing CCM 3.0.1 within a SOC2 Report



Trust Services Criteria Category		(Primary) CCM Control Domain	
CC1.0	Organization and Management	HRS (11)	Human Resources
CC2.0	Communications		
CC3.0	Risk Management and Design and Implementation of Controls	AAC (03)	Audit Assurance & Compliance
CC4.0	Monitoring of Controls	GRM (11)	Governance and Risk Management
CC5.0	Logical and Physical Access Controls (and potentially Processing Integrity for AIS-03)	AIS (04)	Application & Interface Security
		DCS (09)	Datacenter Security
		EKM (04)	Encryption & Key Management
		IAM (13)	Identity & Access Management
		IVS (13)	Infrastructure & Virtualization Security
		TVM (03)	Threat and Vulnerability Management

Addressing CCM 3.0.1 within a SOC2 Report (continued)



Trust Services Criteria Category		(Primary) CCM Control Domain	
CC6.0	System Operations	SEF (05)	Security Incident Management, E-Discovery & Cloud Forensics
CC7.0	Change Management	CCC (05)	Change Control & Configuration Management
CC various	Security - various	DSI (07)	Data Security & Information Lifecycle Management
		IPY (05)	Interoperability & Portability
		MOS (20)	Mobile Security
A1.0	Availability	BCR (11)	Business Continuity Management & Operational Resilience
C1.0	Confidentiality	STA (09)	Supply Chain Management, Transparency and Accountability

Changing international standards and requirements

ISO 27001:2013 control objectives & controls

Ref.	Approx. # of Requirements	Domain
General - Information Security Management System (ISMS)	-	ISMS Documentation Risk Assessment and Risk Treatment Statement of Applicability Internal Audit of ISMS Corrective Action/Continuous Improvement
A.5	2	Security policy
A.6	7	Organization of information security
A.7	6	Human resources security
A.8	10	Asset management
A.9	14	Access control
A.10	2	Cryptography
A.11	15	Physical and environmental security
A.12	14	Operations security
A.13	7	Communications security
A.14	13	Information systems acquisition, development and maintenance
A.15	5	Supplier relationships
A.16	7	Information security incident management
A.17	4	Information security aspects of business continuity management
A.18	8	Compliance
Total	114	

ISO 27018

- ISO/IEC 27018 (2014) – Information technology – Security techniques -- Code of practice for PII protection in public clouds acting as PII processors
- Builds on ISO 27001/27002 and ISO/IEC 29100 Information technology – Security techniques – Privacy framework
- Provides guidance for selecting PII protection controls within the process of implementing a cloud computing information security management system

ISO 27018 Summary

Additional Guidance to Supplement ISO 27001/27002

- Information security policies*
- Organization of information security*
- Human resource security*
- Asset management
- Access control*
- Cryptography
- Physical and environmental security*
- Operations security*
- Communications security*
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management*
- Information security aspects of business continuity management
- Compliance*

* Includes additional cloud guidance

ISO 27018 Summary (continued)

Public cloud PII processor extended control set for PII protection
Building on eleven privacy principles of ISO/IEC 29100

A.1 Consent and choice

- A.1.1 Obligation to co-operate regarding PII principals' rights

A.2 Purpose legitimacy and specification

- A.2.1 Cloud PII processor's purpose
- A.2.2 Cloud PII processor's commercial use

A.3 Collection limitation*

A.4 Data minimization

- A.4.1 Secure erasure of temporary files

A.5 Use, retention and disclosure limitation

- A.5.1 PII disclosure notification
- A.5.2 Recording of PII disclosures

A.6 Accuracy and quality*

* No specific cloud provisions included

A.7 Openness, transparency and notice

- A.7.1 Disclosure of sub-contracted PII processing

A.8 Individual participation and access*

- A.9 AccountabilityA.9.1 Notification of a data breach involving PII
- A.9.2 Retention period for administrative security policies and guidelines
- A.9.3 PII return, transfer and disposal

A.10 Information security

- A.10.1 Confidentiality or non-disclosure agreements
- A.10.2 Restriction of the creation of hardcopy material
- A.10.3 Control and logging of data restoration
- A.10.4 Protecting data on storage media leaving the premises
- A.10.5 Use of unencrypted portable storage media and devices
- A.10.6 Encryption of PII transmitted over public data-transmission networks
- A.10.7 Secure disposal of hardcopy materials
- A.10.8 Unique use of user IDs
- A.10.9 Records of authorized users
- A.10.10 User ID management
- A.10.11 Data processing contract measures
- A.10.12 Sub-contracted PII processing
- A.10.13 Access to data on pre-used data storage space

A.11 Privacy compliance

- A.11.1 Geographical location of PII
- A.11.2 Intended destination of PII

ISO 27017 (under development)

- Information Technology — Security Techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Cloud infrastructure governance, risk and controls

Common cloud provider challenges

Rising expectations of customers

New contractual requirements

Multiple audit requirements

Increasing customer audit requests

Demands for more detailed information

Increasing number and depth of questionnaires

Common cloud provider challenges (continued)

- Inconsistencies across services/ environments
- Lack of a unified control set
- Rapidly growing and changing environments
- Launching of new services
- Complexities of managing user access
- Rapid agile development
- Pressure to adopt Dev Ops model and relax segregation of duties
- Managing risks for multi-provider solutions

Key takeaways for service providers

Establish a governance function over cloud initiatives

Make it a priority internally to critically analyze and restrict privileged user access on an ongoing basis

Ensure that strong monitoring controls are in place

Move toward an integrated control set and consolidated set of audit activities, where feasible

Prioritize and quantify emerging requirements, assess readiness for incremental requirements, fix gaps, then add to control set and audit scope

Consider available assurance tools such as SOC2 Enhanced Reporting to provide additional detail where appropriate

Conclusion

Additional Q&A

?

Contact Information

For more information, please contact:

Mark Lundin
KPMG LLP
Partner, Cloud and Security Assurance
mlundin@kpmg.com
415-963-5493

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.