MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

CLOUD RISK AND GOVERNANCE: HANDS-ON "LITE"

Jon-Michael C. Brook
Principal, Guide Holdings
@jonmichaelbrook

Randall Brooks
Engineering Fellow, Raytheon
@randallsbrooks

WHY ARE YOU HERE?

- How do you protect your data?
- Who thinks they don’t use cloud within their organization?
- Who here uses cloud within their organization?
- How did you determine if a Cloud Service Provider you use took security precautions like you do?
- Will you pass an audit using this CSP?

AGENDA

2 Hour Preview of Cloud & Governance:

- Framework Landscapes (NIST, ISO, CSA)
- Where to integrate with other industry cloud tool sets for policies and standards compliance
- How to streamline your cloud approval and adoption processes
- Hands-on software experience with STAR Watch*, the Cloud Controls Matrix, and Open Source Tools
- Demonstrations of compliance software vendors*
- * Time Permitting

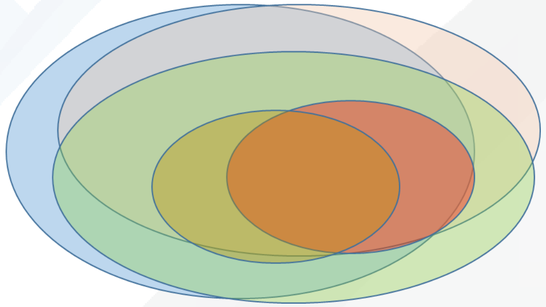
FRAMEWORK LANDSCAPES

Holistic/Descriptive

- NIST 800.53 rev 4
  - 18 families /218 controls
- ISO 27001
  - 14 groups /114 controls
- CSA CCM 3.0.1
  - 16 domains/133 controls

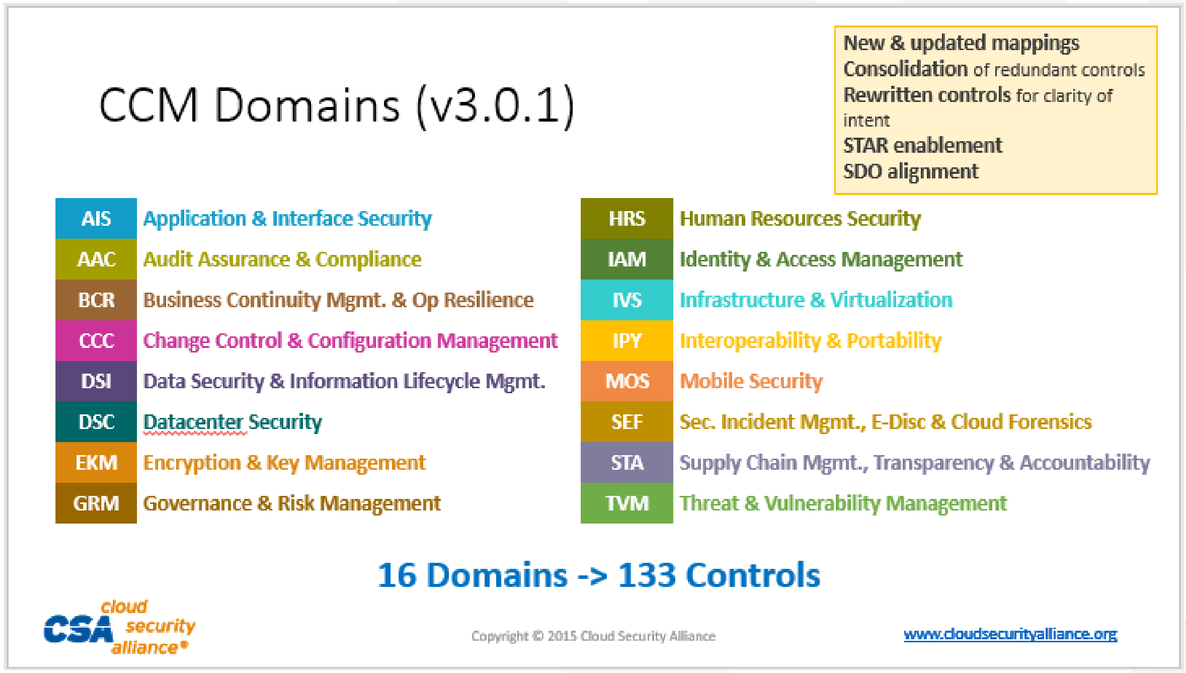
Industry Specific/Prescriptive

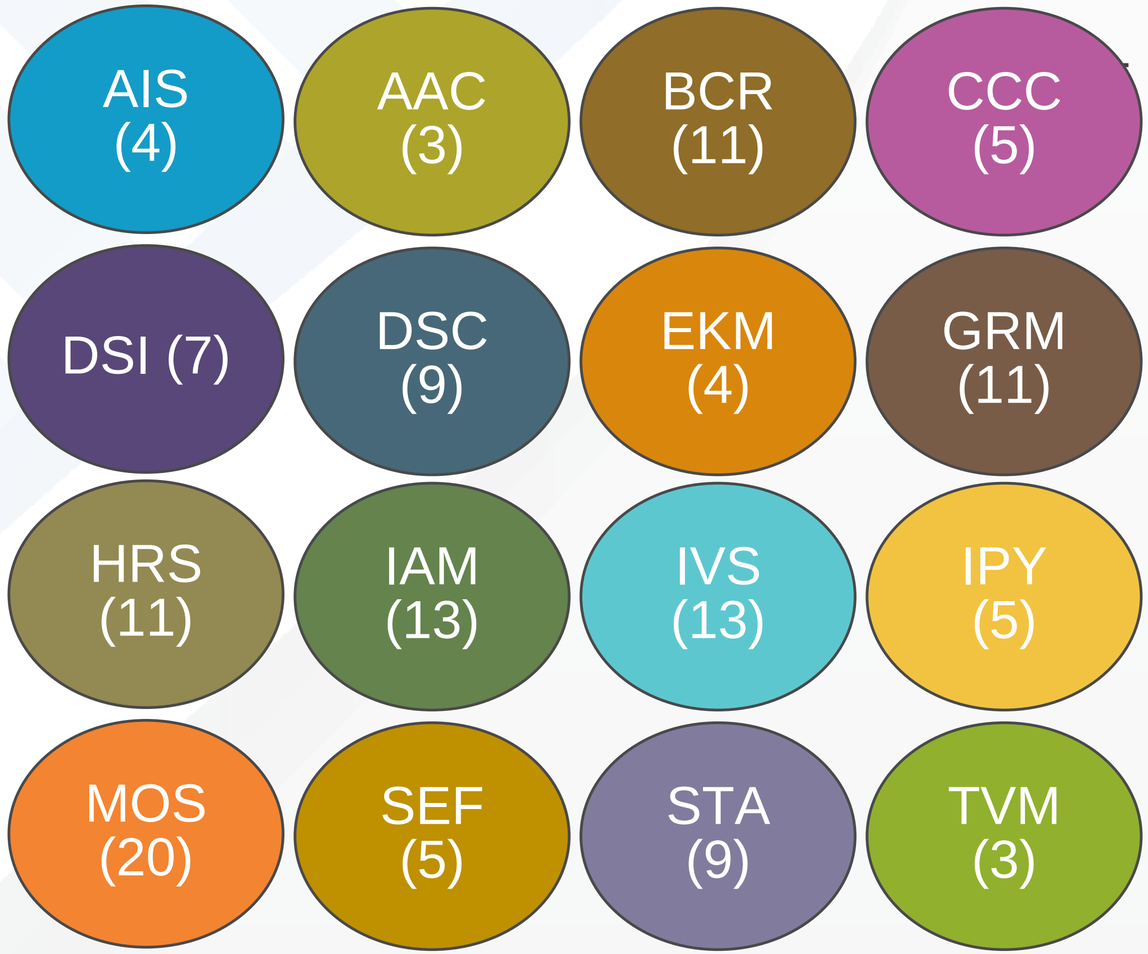
- PCI
  - 6 Goals /12 Controls
- HIPAA/HITRUST
- FERPA
- 23 NYCRR 500
- CIS AWS Benchmark



FRAMEWORKS: CCM

CSA Cloud Controls Matrix Open, Community Contributed Cross Mappings





https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

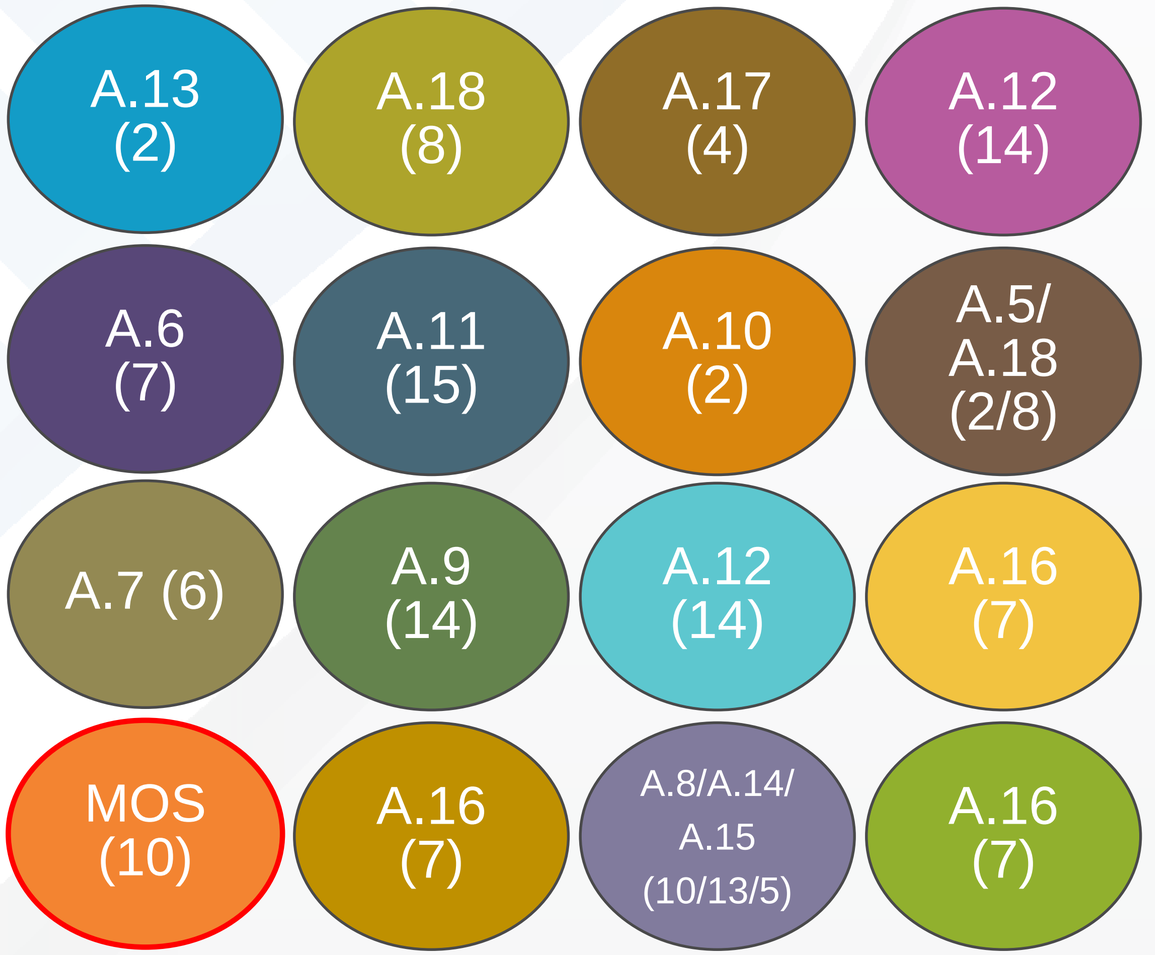
OVERLAP: NIST 800.53

NIST FAMILY NAMES AND SECURITY CONTROL (SC) IDs

ID	FAMILY
AC	Access Control = IAM
MP	Media Protection = EKM
AT	Awareness and Training = HRS
PE	Physical and Environmental Protection = DCS
AU	Audit and Accountability = AAC
PL	Planning = CCC
CA	Security Assessment and Authorization = GRM
PS	Personnel Security = HRS
CM	Configuration Management = CCC
RA	Risk Assessment = TVM
CP	Contingency Planning = BCR
SA	System and Services Acquisition = STA
IA	Identification and Authentication = IAM
SC	System and Communications Protection = IVS/AIS
IR	Incident Response = SEF
SI	System and Information Integrity = DSI
MA	Maintenance = IVS
PM	Program Management

OVERLAP: ISO 27001:2013

ISO Framework overlap
v2013: 114 controls/14 groups
35 control objectives
v2005: 133 controls/11 groups



- A.5: Information security policies (2 controls) = GRM
- A.6: Organization of information security (7 controls) = DSI
- A.7: Human resource security - 6 controls that are applied before, during, or after employment = HRS
- A.8: Asset management (10 controls) = STA
- A.9: Access control (14 controls) = IAM
- A.10: Cryptography (2 controls) = EKM
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls) = CCC/IVS
- A.13: Communications security (7 controls) = AIS
- A.14: System acquisition, development and maintenance (13 controls) = STA
- A.15: Supplier relationships (5 controls) = STA
- A.16: Information security incident management (7 controls) = IPY/SEF/TVM
- A.17: Information security aspects of business continuity management (4 controls) = BCR
- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls) = AAC/GRM

OVERLAP: PCI-DSS R 3.0

Payment Card Industry Data Security Standard 6 Goals/12 Requirements

Build and maintain a secure network
1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

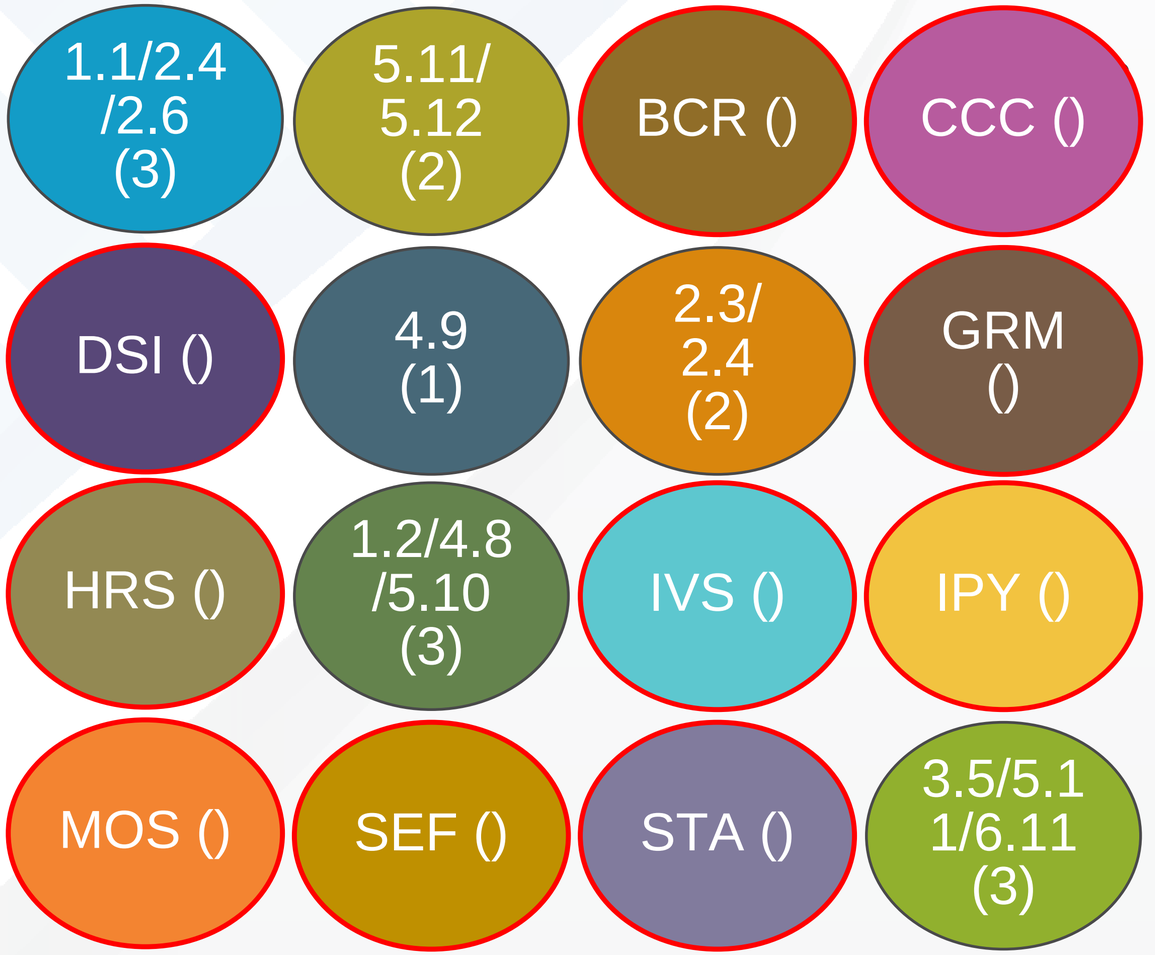
Protect cardholder data
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program
5. Use and regularly update anti-virus software on all systems commonly affected by malware
6. Develop and maintain secure systems and applications

Implement strong access control measures
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

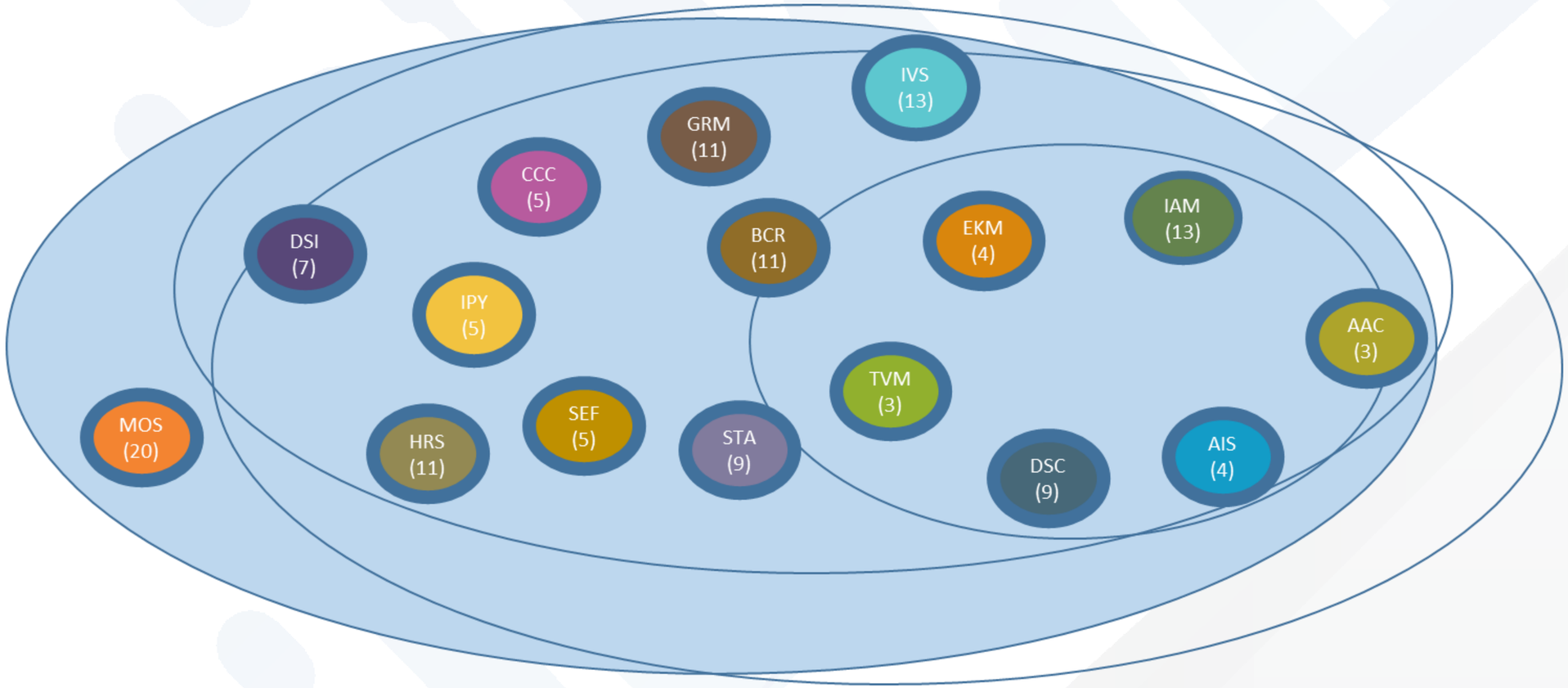
Regularly monitor and test networks
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an information security policy
12. Maintain a policy that addresses information security



https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

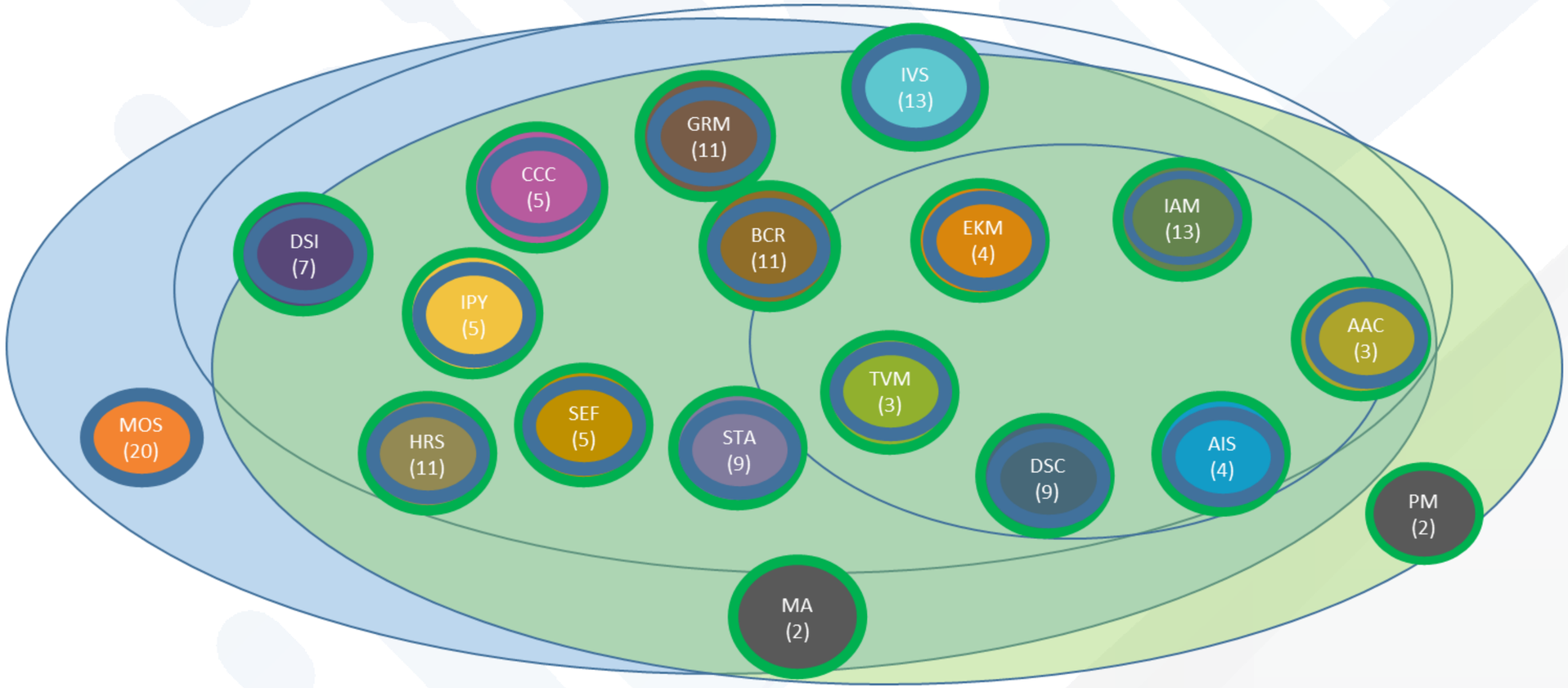
FRAMEWORK COVERAGE: CCM



- CCM 3.0.1
  - 16/132
- NIST 800-53
  - 18/650
- ISO 27001
  - 14/133
- PCI-DSS
  - 6/12

https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

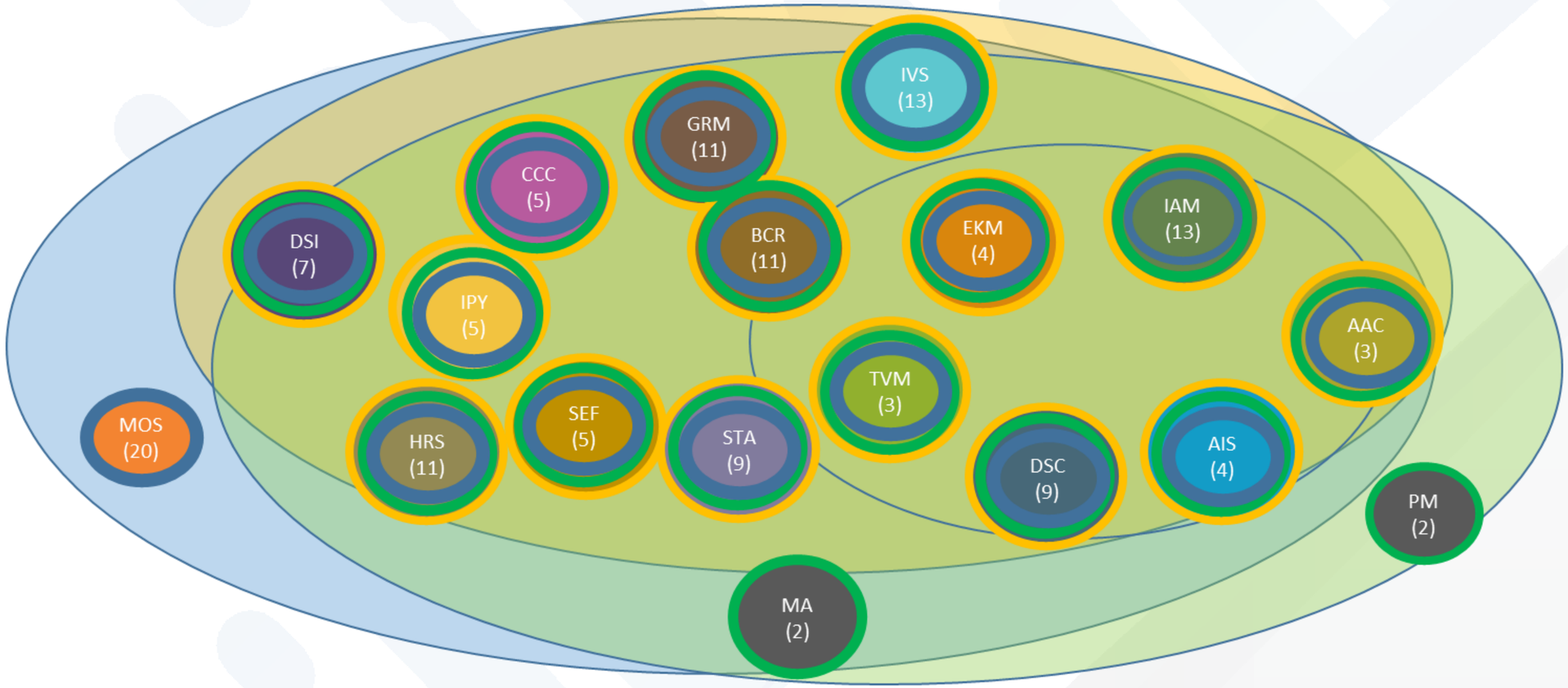
OVERLAP: +NIST 800.53



- CCM 3.0.1
  - 16/133
- NIST 800-53
  - 18/650
- ISO 27001
  - 14/133
- PCI-DSS
  - 6/12

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

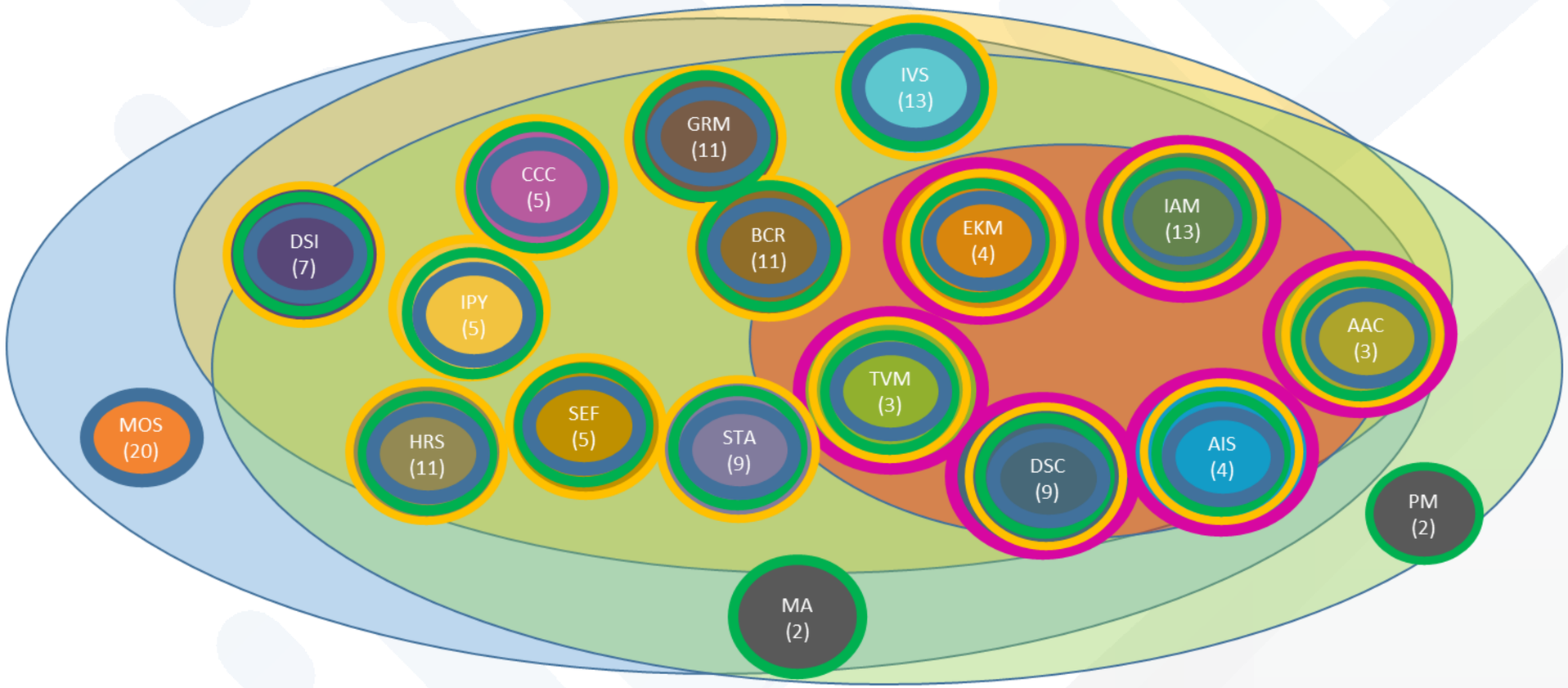
OVERLAP: +ISO 27001



- CCM 3.0.1
  - 16/133
- NIST 800-53
  - 18/650
- ISO 27001
  - 14/133
- PCI-DSS
  - 6/12

https://en.wikipedia.org/wiki/ISO/IEC_27001:2013

OVERLAP: +PCI DSS



- CCM 3.0.1
  - 16/133
- NIST 800-53
  - 18/650
- ISO 27001
  - 14/133
- PCI-DSS
  - 6/12

https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

CSA TOOLS

- Hands-on software experience with
  - Cloud Controls Matrix (CCM)
    - 16 domains, 133 controls
  - Consensus Assessment Initiative Questionnaire (CAIQ)
    - 295 question survey for assessment of CCM
  - Security, Trust and Assurance Registry (STAR)
    - Self Assessment
    - 3rd Party Assessment
    - Continuous Assessment
  - STARWatch

CROSS FRAMEWORK MAPPINGS

- Where to integrate with other industry cloud tool sets for policies and standards compliance?
  - Cloud
    - SIEM, CASB, Splunk
  - Internal Enterprise Tracking
    - Risk & Compliance Databases - Archer
  - Do you separate cloud items from enterprise items?
  - How do you get between them?

OPEN THE CCM SHEET (FILE -> MAKE A COPY)

Examine the NIST 800.53 column (AV)

- Why is there a one to many mapping?
- What does the one to many mapping imply?

Examine the HIPAA/HI-TECH column (AL)

- Why are there gaps in the entries?

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		AICPA 2009 TSC Map	AICPA Trust Service Criteria
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer		
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.			X	X	X	X		X	X	X	X		S3.10.0 S3.10.0	(S3.10.0) Design, acqu modification, and mana are consistent with defi authorized access and (S3.10.0) Design, acqu modification, and mana are consistent with defi security policies.
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	X	X	X	X	X	X	X	X	X	X	X	X	S3.2.a	(S3.2.a) a. Logical acc to information resource
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.		X	X	X	X	X		X	X	X	X	X	I3.2.0 I3.3.0	(I3.2.0) The procedures timeliness, and authoriz documented system pro (I3.3.0) The procedures timeliness, and authoriz error correction and da documented system pro
Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.		X	X	X	X	X	X	X	X	X	X		S3.4	(S3.4) Procedures exis to system resources.

CCM/NIST/ISO Mapping Exercise - 5 Min

EXAMPLE

- EKM-02: Who Creates Keys? Who Controls Keys?
  - AWS: HSM Service, BYOK API check
  - Azure: Key Vault Premium, Azure Information Protection
  - GCE: Customer Supplied Encryption

- Tools for checks –
  - Evident.io, Dome9, CloudCheckr
- Aggregation
  - Allgress, Splunk, SIEM

https://aws.amazon.com/blogs/aws/new-bring-your-own-keys-with-aws-key-management-service/

https://docs.microsoft.com/en-us/information-protection/plan-design/byok-price-restrictions

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-hsm-protected-keys

https://cloud.google.com/compute/docs/disks/customer-supplied-encryption

PROCESS INTEGRATION

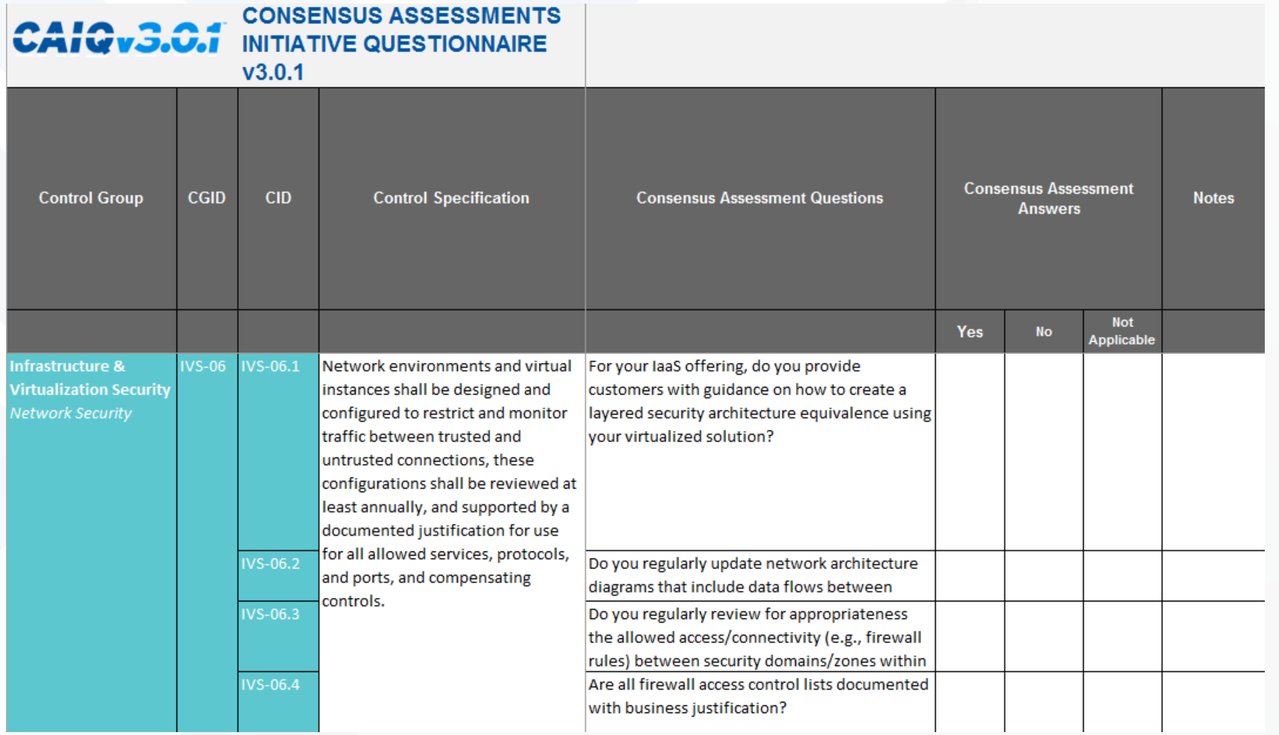
- How to streamline your cloud approval and adoption processes
  - Where are decisions made?
  - What's the coverage goal?
    - Coverage, 2 week turnaround, 80%
  - How might compensating controls be used?
  - Where would mitigations fit in?

PROCESS INTEGRATION

- What does your organization look like?
  - Enterprise
  - Corporation
  - Small Business
- Decision Makers Titles/Roles
  - Risk & Compliance
  - Legal
  - Info Sec Officer
  - IT Director

“COLLECTING RISK” RISKS?

- CAIQ 3.0.1
  - Yes/No/Not Applicable
    - Quantitative?
- Purpose of the CAIQ?
  - A measure of CCM Risk?
  - Detractors/Benefits?
  - Identify Gaps



CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?				
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between				
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within				
		IVS-06.4		Are all firewall access control lists documented with business justification?				

- WHAT ADDITIONAL RISKS INTRODUCED BY USING CAIQ ?

EXERCISE: EVALUATING CAIQ RESPONSE CONFIDENCE

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
		IAM-07.2	likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you monitor service continuity with upstream providers in the event of provider failure?	X			Dependent on the provider
		IAM-07.3		Do you have more than one provider for each service you depend on?				
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including		X	X	
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?	X			See SOC II report
		IAM-07.6		Do you provided a tenant-triggered failover option?		X		Not currently (feature is in development)
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?			x	attached is the Global DRBCP Overview.pdf

HOW MANY MISTAKES CAN YOU FIND IN 3 MINUTES?

HOW MANY DID YOU FIND?

6 REAL WORLD EXAMPLES IN ORDER OF FREQUENCY

MISTAKEN CONFIDENCE

6 REAL WORLD EXAMPLES IN ORDER OF FREQUENCY

1. Blank answer
2. 2 answers (never 3)
   - Yes/No/Not Applicable
3. NA – Cleary in scope
4. No = always good?
5. Blank justification
6. Doesn't answer Q

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
		IAM-07.2	likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you monitor service continuity with upstream providers in the event of provider failure?	X			Dependent on the provider
		IAM-07.3		Do you have more than one provider for each service you depend on?				
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including		X	X	
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?	X			See SOC II report
		IAM-07.6		Do you provided a tenant-triggered failover option?		X		Not currently (feature is in development)
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?			x	attached is the Global DRBCP Overview.pdf

EXERCISE: CONFIDENCE COLUMN

Three ways of doing this in practice:

1. Insert column on CAIQ – quickest
2. Copy & Paste CAIQ responses into a calculations page – doesn't allow for continuous updates
3. Use a reference and move the CAIQ info into separate tab – most repeatable

Let's use the Calculations Exercise tab

5 MINUTES TO COMPLETE – BREAK FOLLOWING

CONFIDENCE CHECKS

- RECAP: WHO FINISHED
- ANYONE WITH CONFIDENCE CHECKING?

IF(SUM(Yes/No/NA)=1
- Test for one, two, blank answer

IF(NOT(No))
- Respondent doesn't do. They admit it.

IF(ISBLANK(Explanation)
- Respondent wrote nothing

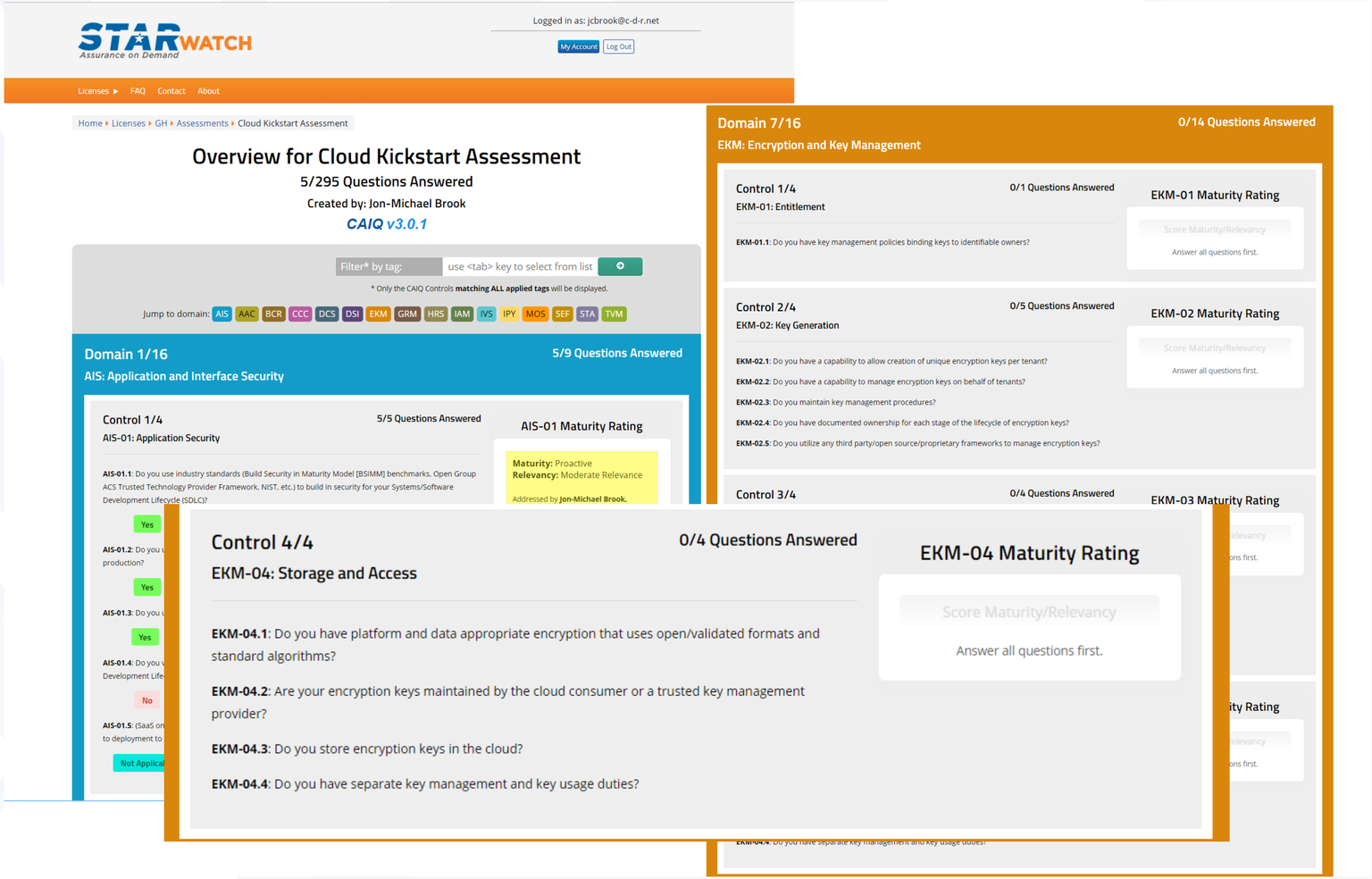
IF(FIND(http:// or https://)
- Confidence in extended explanation?

CCM Domain Detail	CID	Yes	No	NA	Q Count	AVG	Conf 1ans	Conf Exp	Conf ???	Average (-1 to 1)
Application & Interface Security Application Security	AIS-01	0	0	0	5	0	-5	-5		-0.666666667
Application & Interface Security Customer Access Requirements	AIS-02	0	0	0	2	0	-2	-2		-0.666666667
Application & Interface Security Data Integrity	AIS-03	0	0	0	1	0	-1	-1		-0.666666667
Application & Interface Security Data Security / Integrity	AIS-04	0	0	0	1	0	-1	-1		-0.666666667
Audit Assurance & Compliance Audit Planning	AAC-01	0	0	0	1	0	-1	-1		-0.666666667
Audit Assurance & Compliance Independent Audits	AAC-02	0	0	0	8	0	-8	-8		-0.666666667
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	0	0	0	4	0	-4	-4		-0.666666667
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	0	0	0	2	0	-2	-2		-0.666666667
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	0	0	0	1	0	-1	-1		-0.666666667
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental	BCR-03	0	0	0	2	0	-2	-2		-0.666666667
Business Continuity Management & Operational Resilience Documentation	BCR-04	0	0	0	1	0	-1	-1		-0.666666667
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	0	0	0	1	0	-1	-1		-0.666666667
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	0	0	0	1	0	-1	-1		-0.666666667
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	0	0	0	5	0	-5	-5		-0.666666667
Business Continuity Management &	BCR-08									

https://docs.google.com/spreadsheets/d/117Mupiz80UhOoNjyBR6oSFvMdBfG65fKiPnmO44W9-w/edit#gid=333101758

STARWATCH

- Hands-on or Demo of software experience with STAR Watch, the Cloud Controls Matrix, and Open Source Tools



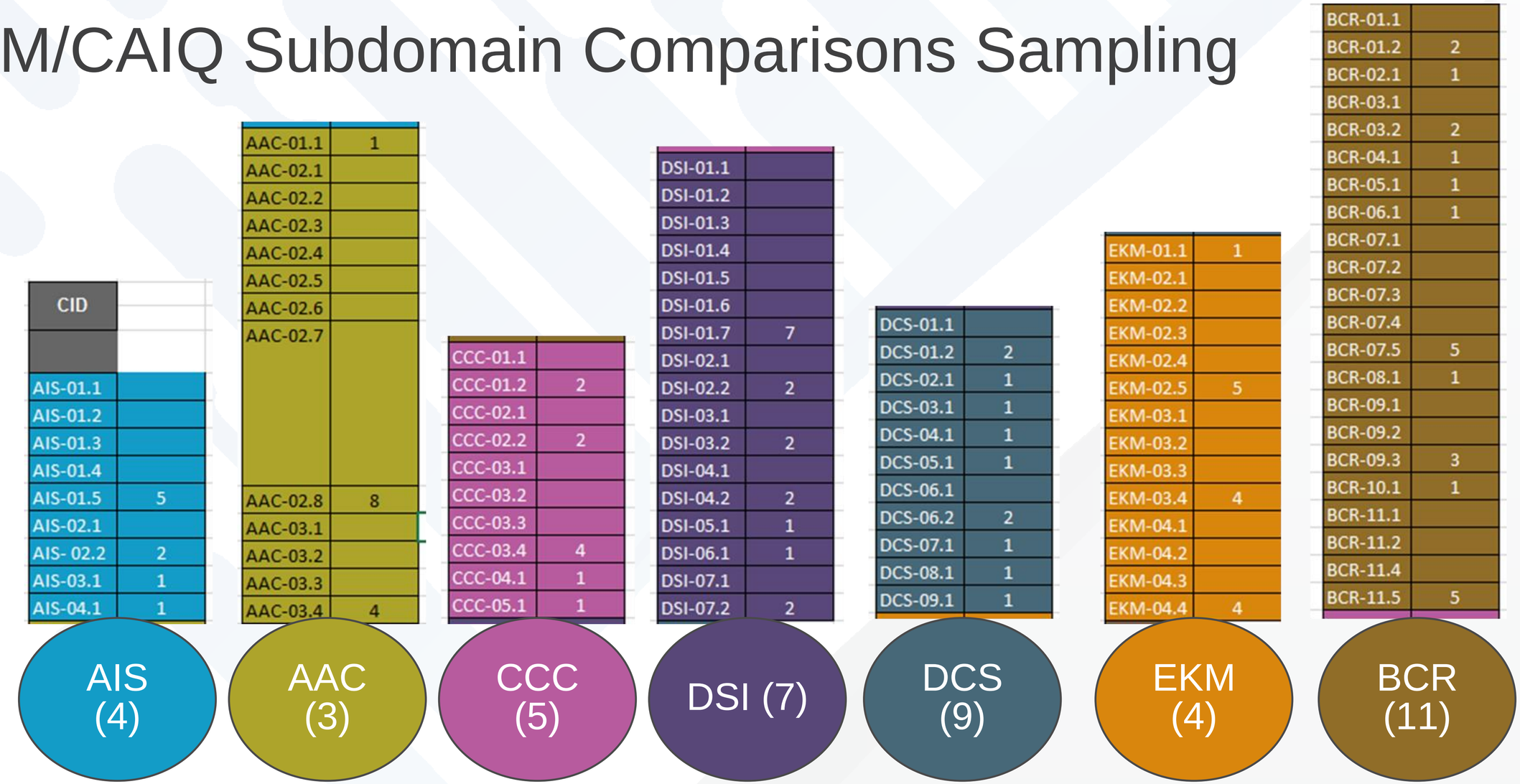
https://star.watch/en

QUESTION COMPARISON

HRS-01.1: Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?
HRS-02.1: Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?
HRS-03.5: Are personnel trained and provided with awareness programs at least once a year?

SUBDOMAIN COMPARISON

CCM/CAIQ Subdomain Comparisons Sampling



CATEGORY TOPIC COMPARISON

- EKM-01 – Entitlement:
  - Who owns keys? What are management policies?
- EKM-02 – Key Generation:
  - Keys per tenant, Key Management, Documented ownership
- EKM-03 – Encryption:
  - Encrypt data at rest, data in motion, tenant keys, Documentation
- EKM-04 – Storage and Access:
  - Where stored, separation of duties

Encryption & Key Management *Entitlement*	EKM-01.1	1
Encryption & Key Management *Key Generation*	EKM-02.1	
	EKM-02.2	
	EKM-02.3	
	EKM-02.4	
	EKM-02.5	5
Encryption & Key Management *Encryption*	EKM-03.1	
	EKM-03.2	
	EKM-03.3	
	EKM-03.4	4
Encryption & Key Management *Storage and Access*	EKM-04.1	
	EKM-04.2	
	EKM-04.3	
	EKM-04.4	4

SUMMARIZATION CALCULATIONS

- Summarization during confidence scoring
  - Easy Average = Sum(Confidence) / Count (Confidence)
- Risk Summarization
  - Direct average = Yes / (Yes + No - NA)
    - Benefits – Speed, Easy to Implement, No arguments (In or Out)
  - Sub-category average
    - Benefits – Fits w/ CSA methodology explanation, only slightly more calculation
  - Weighted average
    - Organization decision some topics are more important?

EXERCISE: RISK SUMMARY

- Insert column next to previous Confidence Column
- Average CAIQ across the control group
  - Avg = SUM(YES) – SUM(NO) / (Q Count – NA)
- Normalize values from 1-5
- ROUND(Avg * 5)
- Contextualize with Vlookup for VL/L/M/H/VH
- Color with Conditional Formatting (Format Painter)

- Why not a true Risk Calculation in Google Sheets example?

CID	Dom Avg	Dom Avg Q	Dom Norm 1-5	Likelihood	Conf 1ans	Conf Exp	Conf ???	Average (-1 to 1)
AIS-01	0.222222	0.5555556	3	Likely	5	-3		0.133333333
AIS-02			2	Not likely	2	-2		0
AIS-03					1	1		0.666666667
AIS-04					-1	-1		-0.666666667
AAC-01	0.153846	0.5384615	3	Likely	1	-1		0
AAC-02			2	Not likely	8	-4		0.166666667
AAC-03					4	-4		0
BCR-01	0.045455	0.2272727	3	Likely	2	2		0.666666667
BCR-02			3	Likely	1	1		0.666666667
BCR-03					2	-2		0
BCR-04					1	-1		0
BCR-05					1	-1		0
BCR-06					1	-1		0
BCR-07					5	-5		0
BCR-08					1	1		0.666666667

5 MINUTES TO COMPLETE

RISK CALCULATIONS

- Risk Summarization
  - Direct average per Domain = Yes / (Yes + No - NA)
    - (SUM(J5:J9)-SUM(K5:K9))/(Count(L5:L9)-SUM(L5:L9)) - [Google Sheets]
    - Benefits – Speed, Easy to Implement, No arguments (In or Out)
  - Sub-category average per CID
    - Benefits – Fits w/ CSA methodology explanation, only slightly more calculation
    - SUM(N5:N13)/COUNT(N5:N13) - [Google Sheets]
  - Weighted average
    - Organization decision some topics are more important?

https://docs.google.com/spreadsheets/d/117Mupiz80UhOoNjyBR6oSFvMdBfG65fKiPnmO44W9-w/edit#gid=129000287

OPEN CLOUD RISK FRAMEWORK - MICROSOFT

- Breaks Risk into Four Categories:
  - Compliance, Strategic, Operational, Market & Finance

	Risk Control Area
Compliance Risks	Governance & Entreprise Risk Management
	Legal Issues : Contracts and Electronic Discovery
	Incident Response
	Storage of data in multiple jurisdictions and lack of transparency
	Compliance and Audit Management
	Data Protection Risks
	Sensitive Media Sanitization
	Audit or Certification unavailable
	Compliance Degradation
	Governance Degradation
Strategic Risks	Information Management and Data Security
	Interoperability and Portability
	Poor Provider Selection
	Organizational Readiness
	Lack of Supplier Redundancy
	Lock-In
	Data classification on DoCE side
	Data migration from on-premise into the cloud (regardless whether public, private or hybrid)

Operational Risks	Data Center Operations
	Log & Tracing failure
	Backup Failure
	Information Management and Data Security
	Impact on current internal operational procedures
	Integration into existing business solutions
	Malicious Activities from an Insider
	Sensitive Information Leakage
	Operations management
	Subpoena and e-discovery
	Unauthorized access to premises
	Theft of Computer Equipment
	Security of the endpoint (e.g. laptop, pc, smartphone, slate) from which the cloud service is consumed.
	Human Resource Constraints
	Natural Disasters
	Licensing Risks
	Traditional Security, Business Continuity and Disaster Recovery

Market & Finance Risks	Loss of reputation
	Service Termination or Failure
	Isolation Failure
	Capacity Management
	Environment Agility / Time to Market
	Incident Response

Disclaimer

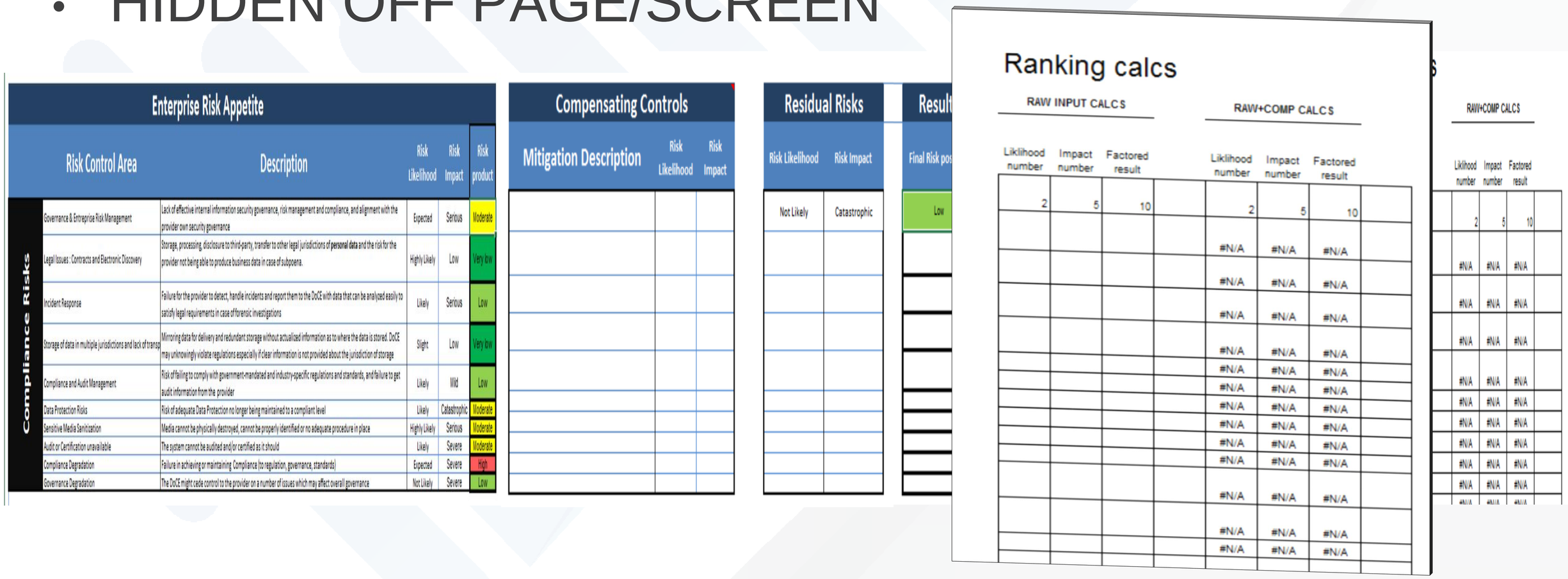
This document has been prepared by Microsoft to provide an overarching risk-management framework to allow organisations to conduct a risk-based assessment of a move to the cloud.

This document is provided on an "as is" basis and to the maximum extent permitted by law Microsoft disclaims all conditions, warranties and guarantees, express or implied, including but not limited to any warranty or guarantee that the use of the framework set out in this document will not infringe any rights or any warranty or guarantee of merchantability or fitness for a particular purpose. Before using the framework set out in this document, you should evaluate its suitability for your organisation. In particular, if you choose to act upon the output of the framework, then you do so at your own risk.

Authors:
Greg Stone - Chief Technology Officer, Microsoft Austrtalia
Pierre Noel - Chief Security Advisor, Microsoft Asia
James Kavanagh - Chief Security Advisor, Microsoft Australia

CALCULATING RISKS IN FRAMEWORK

- RISK = LIKELIHOOD x IMPACT x MITIGATION
  - HIDDEN OFF PAGE/SCREEN



Enterprise Risk Appetite

	Risk Control Area	Description	Risk Likelihood	Risk Impact	Risk product
Compliance Risks	Governance & Entreprise Risk Management	Lack of effective internal information security governance, risk management and compliance, and alignment with the provider own security governance	Expected	Serious	Moderate
	Legal Issues : Contracts and Electronic Discovery	Storage, processing, disclosure to third-party, transfer to other legal jurisdictions of personal data and the risk for the provider not being able to produce business data in case of subpoena.	Highly Likely	Low	Very low
	Incident Response	Failure for the provider to detect, handle incidents and report them to the DoCE with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations	Likely	Serious	Low
	Storage of data in multiple jurisdictions and lack of transp	Mirroring data for delivery and redundant storage without actualized information as to where the data is stored. DoCE may unknowingly violate regulations especially if clear information is not provided about the jurisdiction of storage	Slight	Low	Very low
	Compliance and Audit Management	Risk of failing to comply with government-mandated and industry-specific regulations and standards, and failure to get audit information from the provider	Likely	Mid	Low
	Data Protection Risks	Risk of adequate Data Protection no longer being maintained to a compliant level	Likely	Catastrophic	Moderate
	Sensitive Media Sanitization	Media cannot be physically destroyed, cannot be properly identified or no adequate procedure in place	Highly Likely	Serious	Moderate
	Audit or Certification unavailable	The system cannot be audited and/or certified as it should	Likely	Severe	Moderate
	Compliance Degradation	Failure in achieving or maintaining Compliance (to regulation, governance, standards)	Expected	Severe	High
	Governance Degradation	The DoCE might cede control to the provider on a number of issues which may affect overall governance	Not Likely	Severe	Low

Compensating Controls

Mitigation Description	Risk Likelihood	Risk Impact

Residual Risks

Risk Likelihood	Risk Impact
Not Likely	Catastrophic

Result

Final Risk pos
Low

Ranking calcs

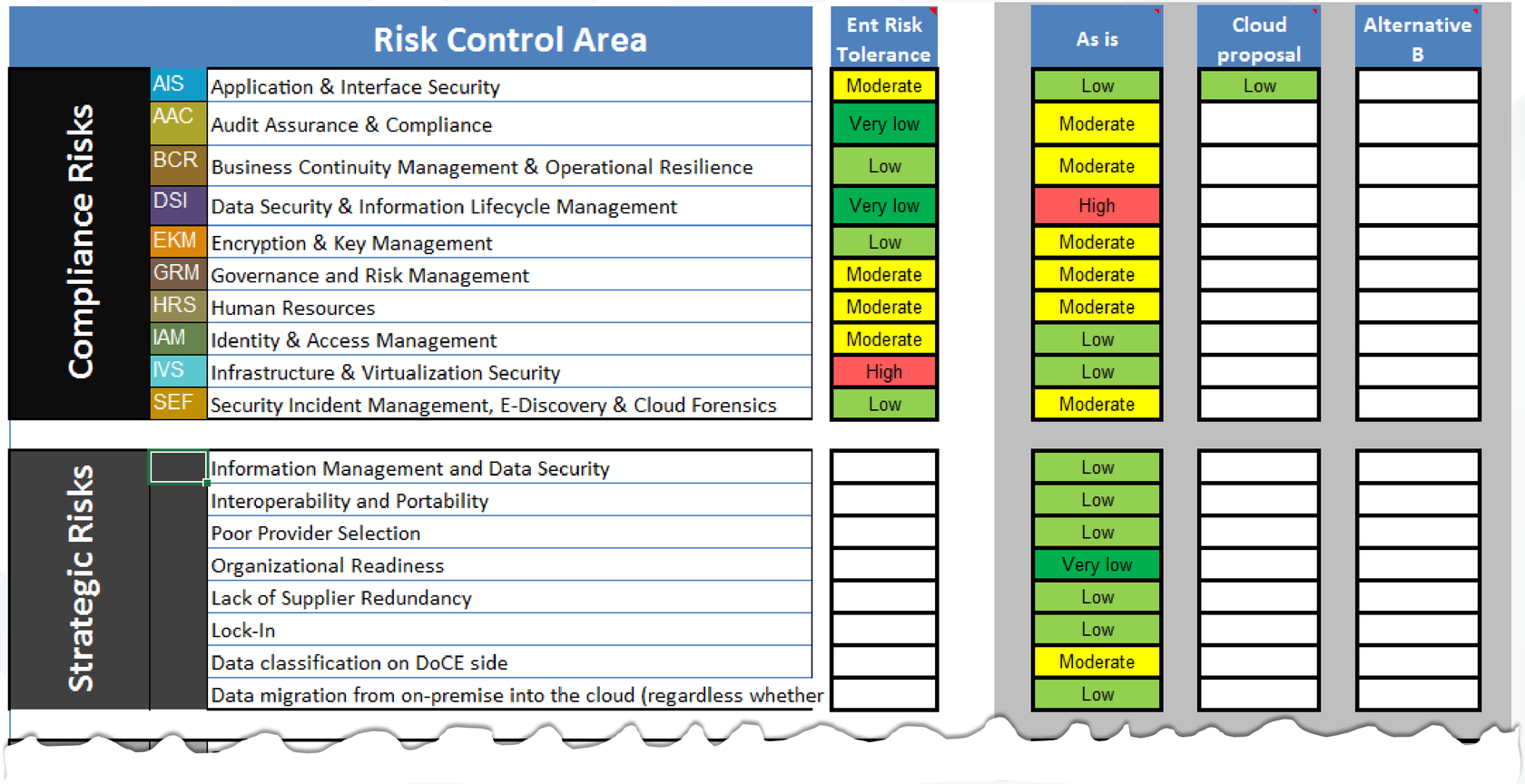
RAW INPUT CALCS				RAW+COMP CALCS			
Liklihood number	Impact number	Factored result		Liklihood number	Impact number	Factored result	
2	5	10		2	5	10	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	
				#N/A	#N/A	#N/A	

RAW+COMP CALCS

Liklihood number	Impact number	Factored result	
2	5	10	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	
#N/A	#N/A	#N/A	

RISK & COMPLIANCE DASHBOARD

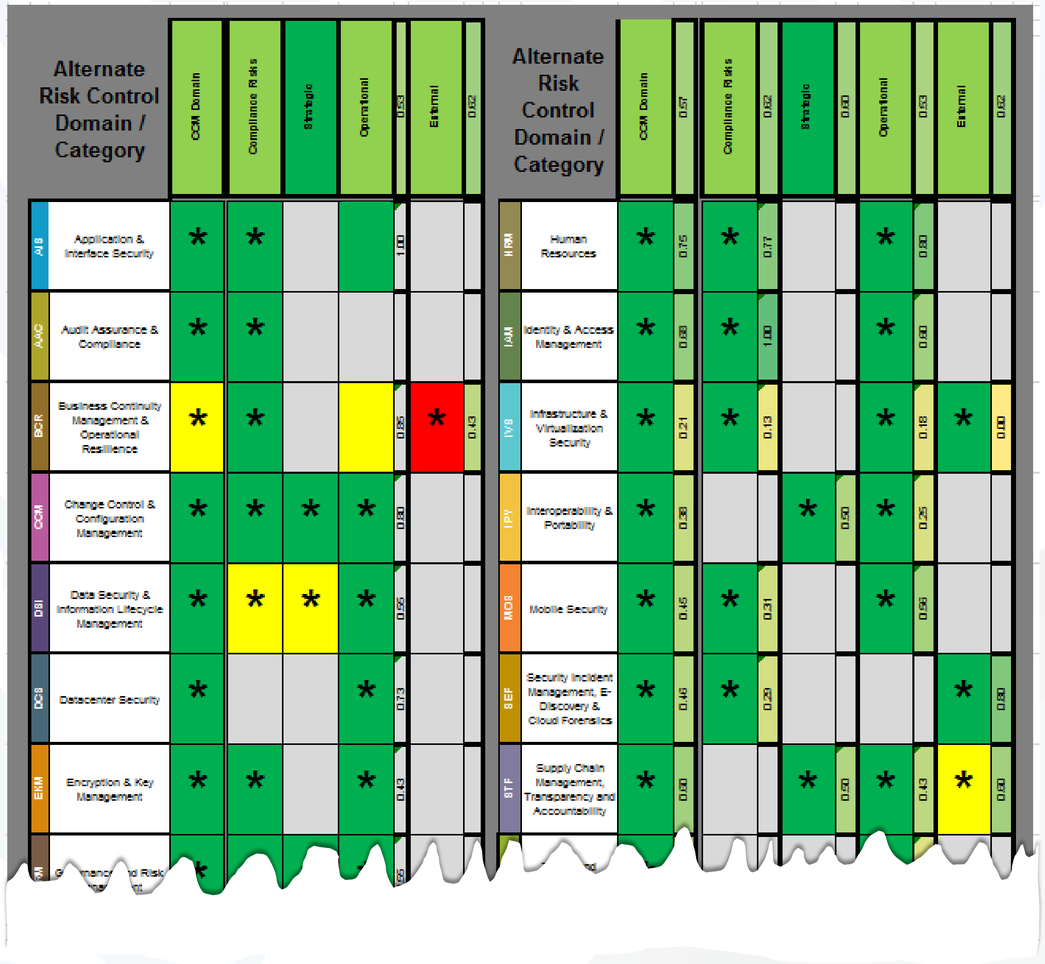
- Combination of CCM, CAIQ and Risk Framework



		Risk Control Area	Ent Risk Tolerance	As is	Cloud proposal	Alternative B
Compliance Risks	AIS	Application & Interface Security	Moderate	Low	Low	
	AAC	Audit Assurance & Compliance	Very low	Moderate		
	BCR	Business Continuity Management & Operational Resilience	Low	Moderate		
	DSI	Data Security & Information Lifecycle Management	Very low	High		
	EKM	Encryption & Key Management	Low	Moderate		
	GRM	Governance and Risk Management	Moderate	Moderate		
	HRS	Human Resources	Moderate	Moderate		
	IAM	Identity & Access Management	Moderate	Low		
	IVS	Infrastructure & Virtualization Security	High	Low		
	SEF	Security Incident Management, E-Discovery & Cloud Forensics	Low	Moderate		
Strategic Risks		Information Management and Data Security		Low		
		Interoperability and Portability		Low		
		Poor Provider Selection		Low		
		Organizational Readiness		Very low		
		Lack of Supplier Redundancy		Low		
		Lock-In		Low		
		Data classification on DoCE side		Moderate		
		Data migration from on-premise into the cloud (regardless whether		Low		

RISK & COMPLIANCE DASHBOARD

- Combination of CCM, CAIQ and Risk Framework



CLOUD COMPLIANCE TOOLS

- Demonstrations of compliance software vendors

REFERENCE LINKS FOR EXERCISES

Cloud Controls Matrix 3.0.1 for workshop
https://docs.google.com/spreadsheets/d/1XX9mWqjFHTwKlZQ3neNNthJfcqH9Re3IKBbOZIw6pYg/edit?usp=sharing

CAIQ for workshop
https://docs.google.com/spreadsheets/d/117Mupiz80UhOoNjyBR6oSFvMdBfG65fKiPnmO44W9-w/edit?usp=sharing

CSA CAIQ
https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/

STAR Registry
https://cloudsecurityalliance.org/star/#_registry

Microsoft Open Cloud Risk Framework
http://download.microsoft.com/documents/australia/enterprise/smic1545_pdf_v7_pdf.pdf

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Jon-Michael Brook
Principal, Guide Holdings
@jonmichaelbrook

Randall Brooks
Engineering Fellow, Raytheon
@randallsbrooks

BIO

Mr. Randall Brooks is an Engineering Fellow for Raytheon Company (NYSE: RTN), representing the company within the U.S. International Committee for Information Technology Standards Cyber Security 1 (CS1). Brooks has more than 20 years of experience in Cybersecurity with a recognized expertise in Software Assurance (SwA) and secure development life cycles (SDLC). In addition to holding eight patents, Mr. Brooks is a CCSK, CISSP, CSSLP, ISSEP, ISSAP, and ISSMP. Brooks graduated from Purdue University with a Bachelors of Science from the School of Computer Science.

BIO

Jon-Michael C. Brook is a certified, 20-year practitioner of information security, cloud and privacy. He is the principal contributor to certification sites for privacy and cloud security, and published books on privacy. He received numerous awards and recognitions during his time with Raytheon, Northrop Grumman and Symantec, and holds patents and trade secrets in intrusion detection, GUI design and semantic data redaction. Mr. Brook is recognized as a Research Fellow and Knolde Service Award recipient with the Cloud Security Alliance, and currently co-chairs the CSA's Top Threats to Cloud Security Working Group. He contributes to several CSA publications including the Enterprise Architecture. He is a certified trainer for the CSA's Certificate of Cloud Security Knowledge (CCSK), teaching the CCSK+ training at the BlackHat conference. Mr. Brook is currently co-developing training for the Cloud Controls Matrix (CCM), the cloud security standard and internationally-accepted GRC framework.