Cloud Security Certifications:
A Comparison to Improve Cloud Service Provider Security

Presenter: Carlo Di Giulio
Advisor: Masooda Bashir

10/05/2016

Context (1/2)

- 2011 Federal Cloud Computing Strategy:
  - Savings (The total IT expenditure in 2011 at a Federal level was $75.4 Billion)
  - High security level in the cloud
- Creation of the Federal Risk Authorization Management Program (FedRAMP)
  - Leveraging on NIST 800-53 requirements

FedRAMP and DISA Authorization

810 Controls/Enhancements

Impact level 5

FedRAMP Moderate + 47 controls
FedRAMP High + 12 controls (?)

- Only dedicated infrastructure
- Facility under the legal jurisdiction of the US

Impact level (3) 4

FedRAMP High, or Moderate + 38 controls

Impact level 2

Same as FedRAMP Moderate baseline

- Shared or dedicated infrastructure
- Within the US territory
- Other locations may be authorized according to mission requirements

Moderate Baseline

325 controls

Low Baseline

125 controls

- Shared or dedicated (not private cloud) infrastructure
- Location not specified

NIST

How a Control Looks Like

AC-10 - Access Control - Concurrent Session Control

The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*]. (NIST SP 800-53)

DSI-05 - Data Security & Information Lifecycle Management - Non-Production Data

Production data shall not be replicated or used in non-production environments. (CSA CCM V. 3.0.1)

A1.2 – Additional Criteria for Availability

Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. (AICPA TSC 2014)

Context (2/2)

- Cloud Computing means easy access to remote services, but also increased concern on security and privacy
- Certifications and compliance with standards are the easiest (if not only) indicator to evaluate a CSP from the outside
- To reassure users on the quality of services (IT and not), security standards are widely used by governments and industries

From a Vendor's Point of View

10+ Standards,
~1000 Control Requirements (CRs)

SOC 2 (5 Principles) – 116 CR
Service Organization Controls

ISO 27001 – 26 CRs
International Organization for Standardization

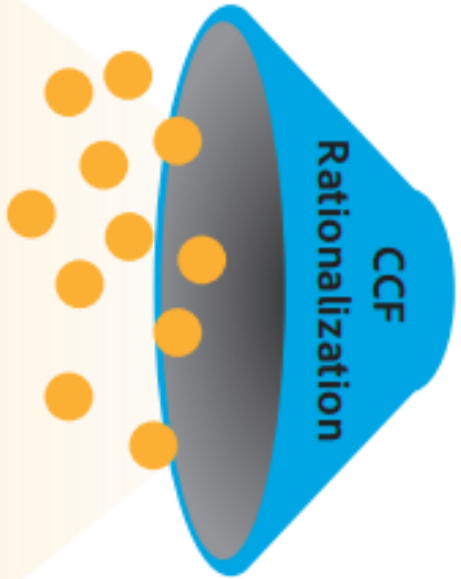
PCI DSS – 247 CRs
Payment Card Industry – Data Security Standard

FedRAMP – 325 CRs
Federal Risk and Authorization Management Program

ISO 27002 – 114 CRs
International Organization for Standardization

SAFE HARBOR – 7 CRs
Safe Harbor

SOX 404 (IT) – 63 CRs
Sarbanes Oxley 404



~ 200 common controls
across 11 control domains

- Asset Management – 12 Controls
- Access Control – 30 Controls
- BCM – 10 Controls
- Cryptography – 11 Controls
- Data Privacy – 10 Controls
- Incident Response – 6 Controls
- Operations Management – 70 Controls
- Physical and Env. Security – 16 Controls
- People Resources – 11 Controls
- SDLC – 11 Controls
- Security Governance – 31 Controls

Source : http://www.adobe.com/content/dam/Adobe/en/security/pdfs/adobe-ccf-012015.pdf
Additional resources: https://commoncontrolshub.com/

FedRAMP (Moderate) and Others

	VENDORS	AUDITORS	COST
	#/**compliant** vendors in the US	Pre-requisites **for** Auditors	**Initial cost** for average company
FedRAMP Federal Risk Authorization Management Program	• **73 (Sep 2016)**	• **ISO 17020** (Conformity assessment: inspections)	**$250K +/- 85K (165-335K)***
Information Security Management System ISO 27001 Certified	• **664 (2014)**	• **ISO 17021** (Conformity assessment for auditors) • **ISO 27006** (IT Security techniques for auditors)	**$48K +/- 32K (16-80K)***
AICPA Service Organization Control Reports SOC 2 Formerly SAS 70 Reports	• **N/A**	• **Certified Public Accountant**	**$55K +/- 15K (40-70K)***

*Information retrieved from www.pivotpointsecurity.com

ISO 27001 Certifications (and percentage varation)

ISO/IEC 27001									
Year	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**
Russian Federation*	5	9	17	53	72	31	27	48	50
		44.44%	88.89%	211.76%	35.85%	-56.94%	-12.90%	77.78%	4.17%
Bulgaria	0	8	23	60	116	132	208	278	330
		N/A	187.50%	160.87%	93.33%	13.79%	57.58%	33.65%	18.71%
Germany	95	135	239	253	357	424	488	581	640
		29.63%	77.04%	5.86%	41.11%	18.77%	15.09%	19.06%	10.15%
USA	69	94	168	252	247	315	415	566	664
		26.60%	78.72%	50.00%	-1.98%	27.53%	31.75%	36.39%	17.31%
Spain	23	93	203	483	711	642	805	799	701
		75.27%	118.28%	137.93%	47.20%	-9.70%	25.39%	-0.75%	-12.27%
Taipei, Chinese	159	256	702	934	1028	791	855	918	781
		37.89%	174.22%	33.05%	10.06%	-23.05%	8.09%	7.37%	-14.92%
Romania	4	16	44	303	350	575	866	840	893
		75.00%	175.00%	588.64%	15.51%	64.29%	50.61%	-3.00%	6.31%
Italy	175	148	233	297	374	425	495	901	970
		-18.24%	57.43%	27.47%	25.93%	13.64%	16.47%	82.02%	7.66%
China	75	146	236	459	957	1219	1490	1710	2002
		48.63%	61.64%	94.49%	108.50%	27.38%	22.23%	14.77%	17.08%
India	369	508	813	1240	1281	1427	1611	1931	2170
		27.36%	60.04%	52.52%	3.31%	11.40%	12.89%	19.86%	12.38%
United Kingdom	486	519	738	946	1157	1464	1701	1923	2261
		6.36%	42.20%	28.18%	22.30%	26.53%	16.19%	13.05%	17.58%
Japan	3790	4896	4425	5508	6237	6914	7199	7140	7181
		22.59%	-9.62%	24.47%	13.24%	10.85%	4.12%	-0.82%	0.57%

Gaps in the Literature

Industry/Non Academic Work

- Threats
- Compliance
  - Controls
  - Adoption of current standards

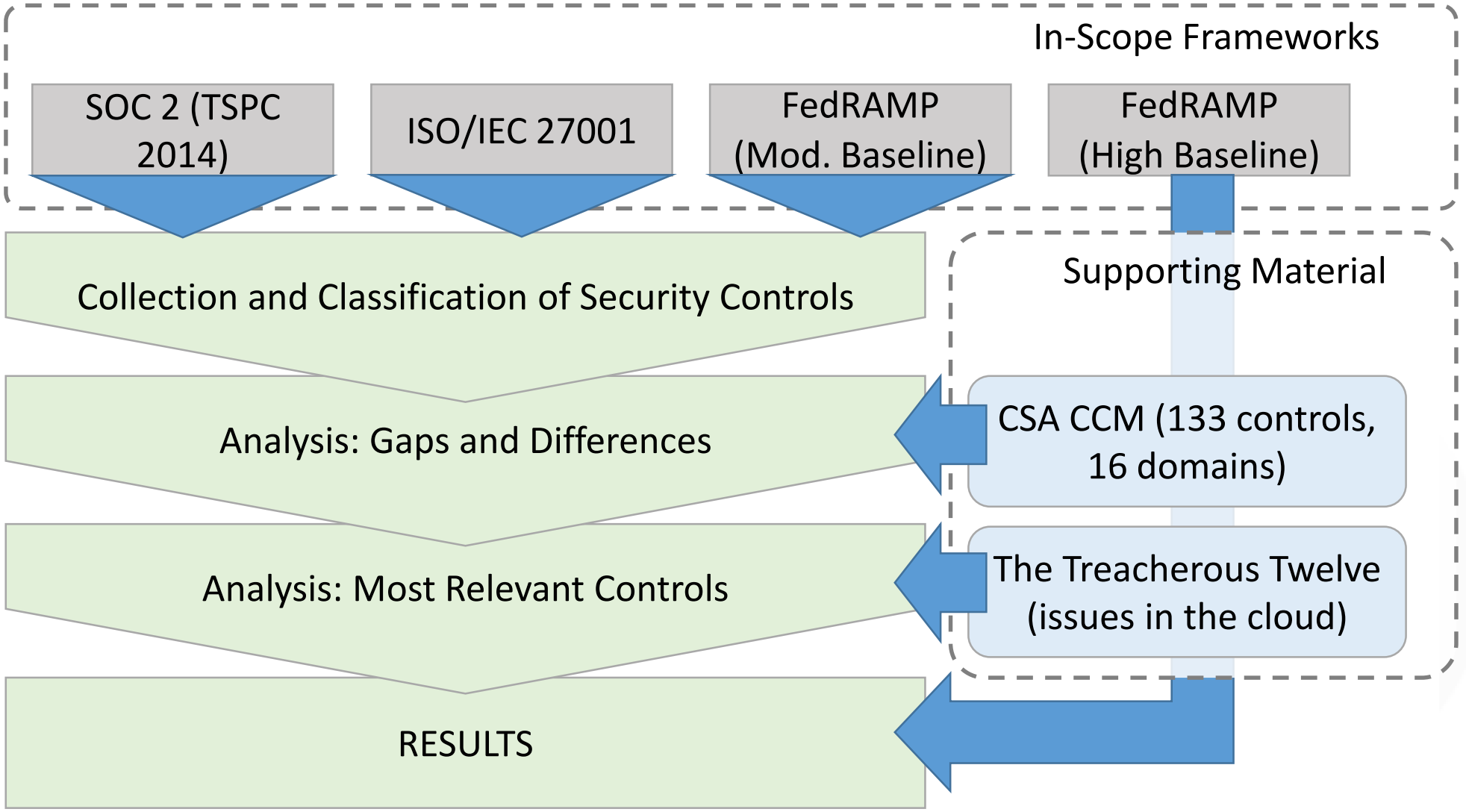
Academic Work

- Threats
- Standards
  - Outdated material
  - Limited scope
  - New approaches

Research Questions

- How effective are current IT security measures and frameworks at addressing cloud security?
- Is FedRAMP better than other security frameworks at protecting information assurance in cloud environments, and if so, how?
- Is it ultimately worth it to invest in new cloud security standards like FedRAMP?
- What can be done to improve current cloud security standards?

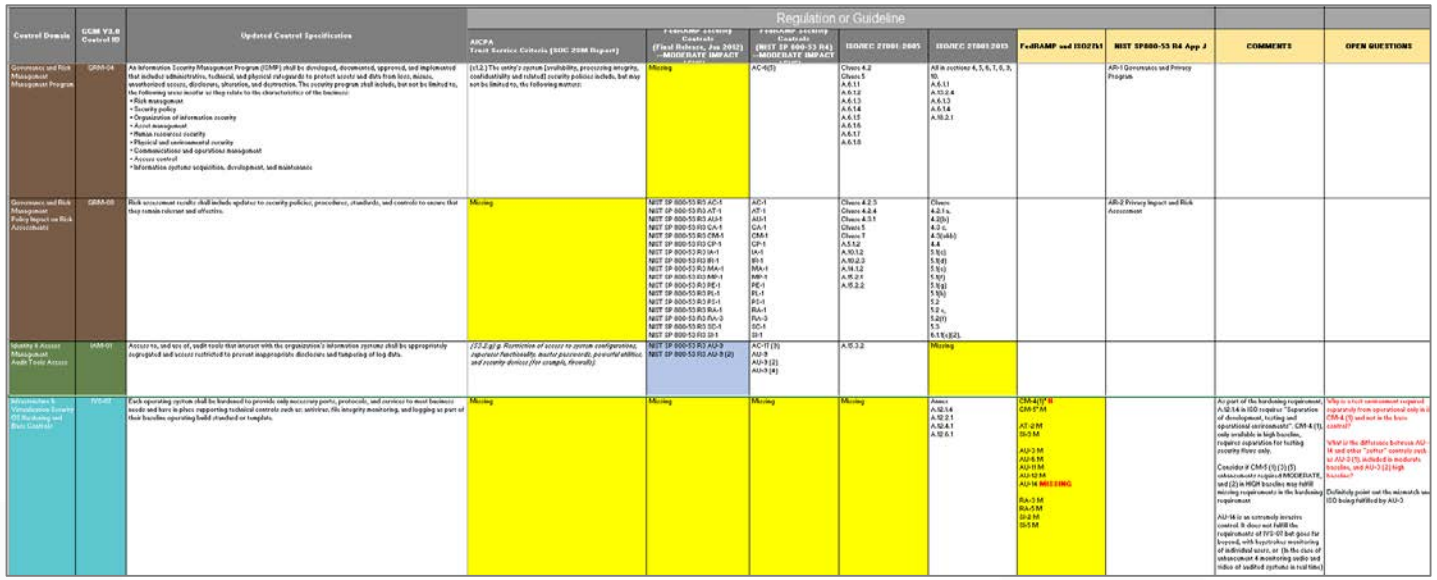
Methodology



The CSA CCM and the T12

Step 1:

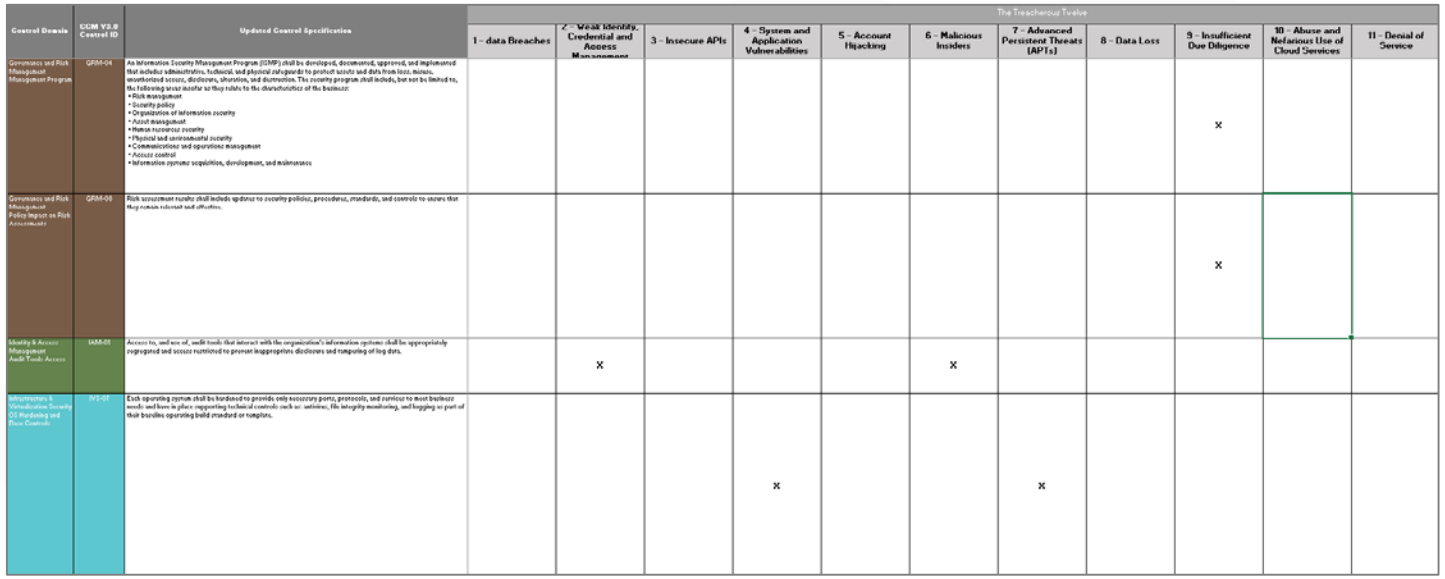
- Matching of guidelines
- Analysis of missing controls



Control Domain	CCM V3.0 Control ID	Updated Control Specification	Regulation or Guideline								
			AICPA Trust Service Criteria (SOC 2SM Report)	FedRAMP Security Controls (Final Release, Jan 2012) -MODERATE IMPACT	FedRAMP Security Controls (NIST SP 800-53 R4) -MODERATE IMPACT	ISO/IEC 27001:2005	ISO/IEC 27001:2013	FedRAMP and ISO27k1	NIST SP800-53 R4 App J	COMMENTS	OPEN QUESTIONS
Governance and Risk Management Program	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance		Missing	AC-6(5)	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	All in sections 4, 5, 6, 7, 8, 9, 10 A.6.1.1 A.10.2.4 A.6.1.3 A.6.1.4 A.18.2.1		AR-1 Governance and Privacy Program		
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Missing	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-3 SC-1 SI-1	Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2	Clause 4.2.1 a, 4.2(b) 4.2 c, 4.3(a&b) 8.4 5 b) 5 d) 5 e) 5 g) 5 g) 5 h) 5.2 5.2 c, 5.2 f) 5.3 6.1.1(c),(2).			AR-2 Privacy Impact and Risk Assessment		
Identity & Access Management Audit Tools Access	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	*(12.2.g) e.g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).*	NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-9 (2)	AC-17 (3) AU-9 AU-9 (2) AU-9 (4)	A.15.3.2	Missing				
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-01	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Missing	Missing	Missing	Missing	Annex A.12.5.1 A.12.2.1 A.12.6.1 A.12.6.1	CM-4(1)* S CM-5* M AT-2 M SI-5 M AU-3 M AU-6 M AU-11 M AU-12 M AU-14 MISSING RA-3 M RA-5 M SI-2 M SI-5 M		As part of the hardening requirement, A.12.1.4 in ISO requires "Separation of development, testing and operational environments". CM-4 (1), only available in high baseline, requires separation for testing security flaws only. Consider if CM-5 (1) (2) (3) subsequently required MODERATE, and (2) in HIGH baseline may fulfill missing requirements in the hardening requirement. AU-14 is an extremely invasive control. It does not fulfill the requirements of IVS-01 but good for beyond, with keystrokes monitoring of individual users, or (in the case of unsupervised 4 monitoring audio and video of audited systems in real time).	Why is a root environment required separately from operational only as in CM-4 (1) and not in the base control? What if the differences between AU-14 and other "active" controls such as AU-2 (3), included in moderate baseline, and AU-3 (2) high baseline? Definitely point out the mismatch as ISO being fulfilled by AU-3

Step 2

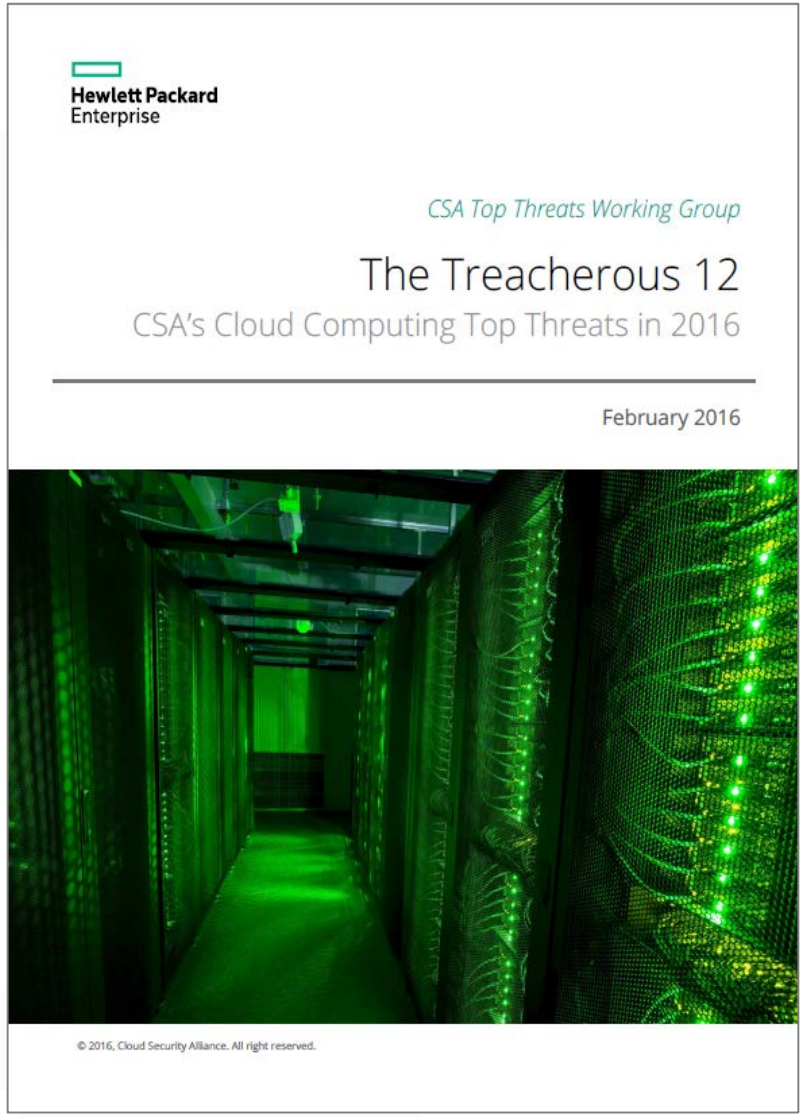
- Collection of Threats
- Matching on missing controls



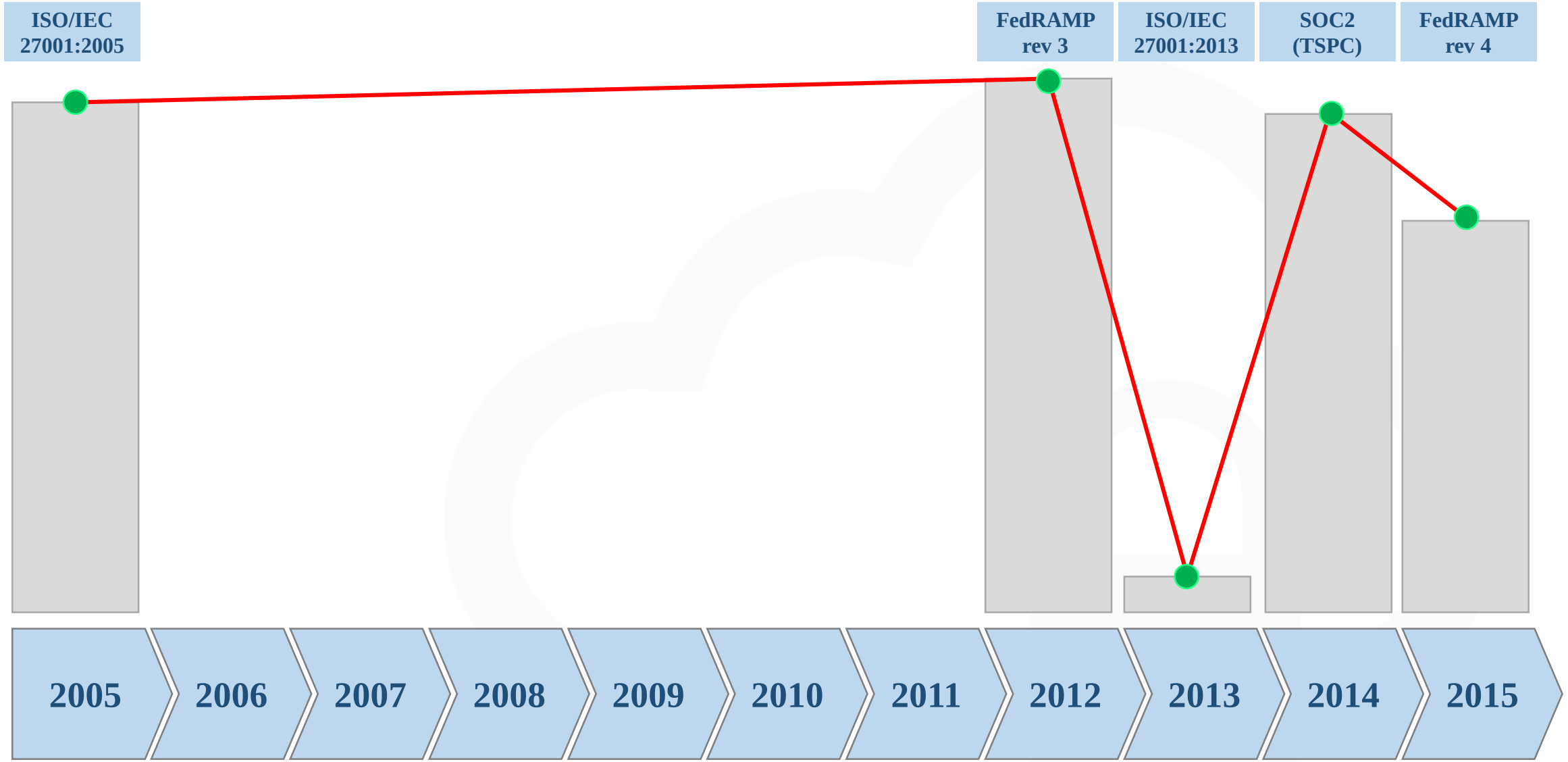
Control Domain	CCM V3.0 Control ID	Updated Control Specification	The Treacherous Twelve										
			1 - data Breaches	2 - Weak Identity, Credential and Access Management	3 - Insecure APIs	4 - System and Application Vulnerabilities	5 - Account Hijacking	6 - Malicious Insiders	7 - Advanced Persistent Threats (APTs)	8 - Data Loss	9 - Insufficient Due Diligence	10 - Abuse and Nefarious Use of Cloud Services	11 - Denial of Service
Governance and Risk Management Program	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance									x		
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.									x		
Identity & Access Management Audit Tools Access	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.		x				x					
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-01	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.				x			x				

The Treacherous Twelve (Issues)

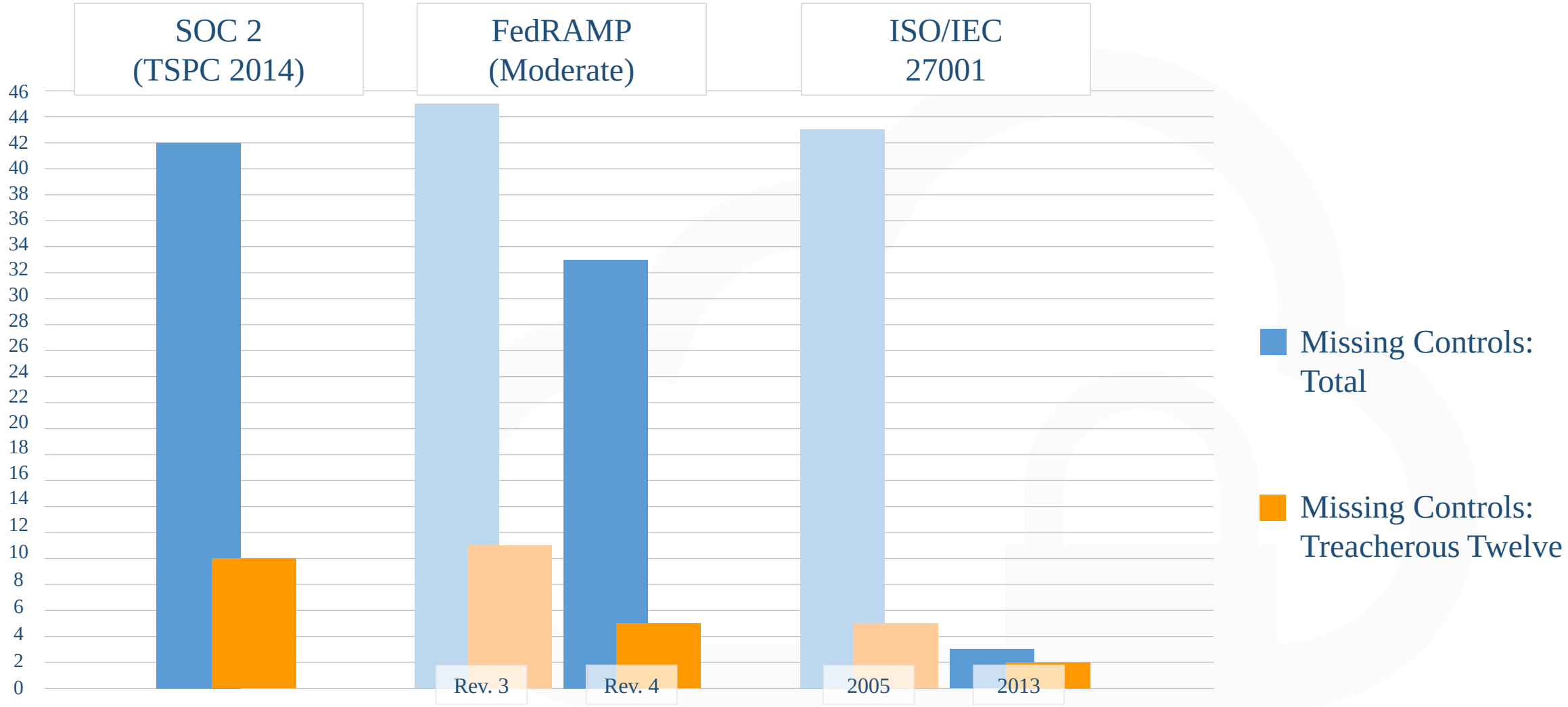
1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues



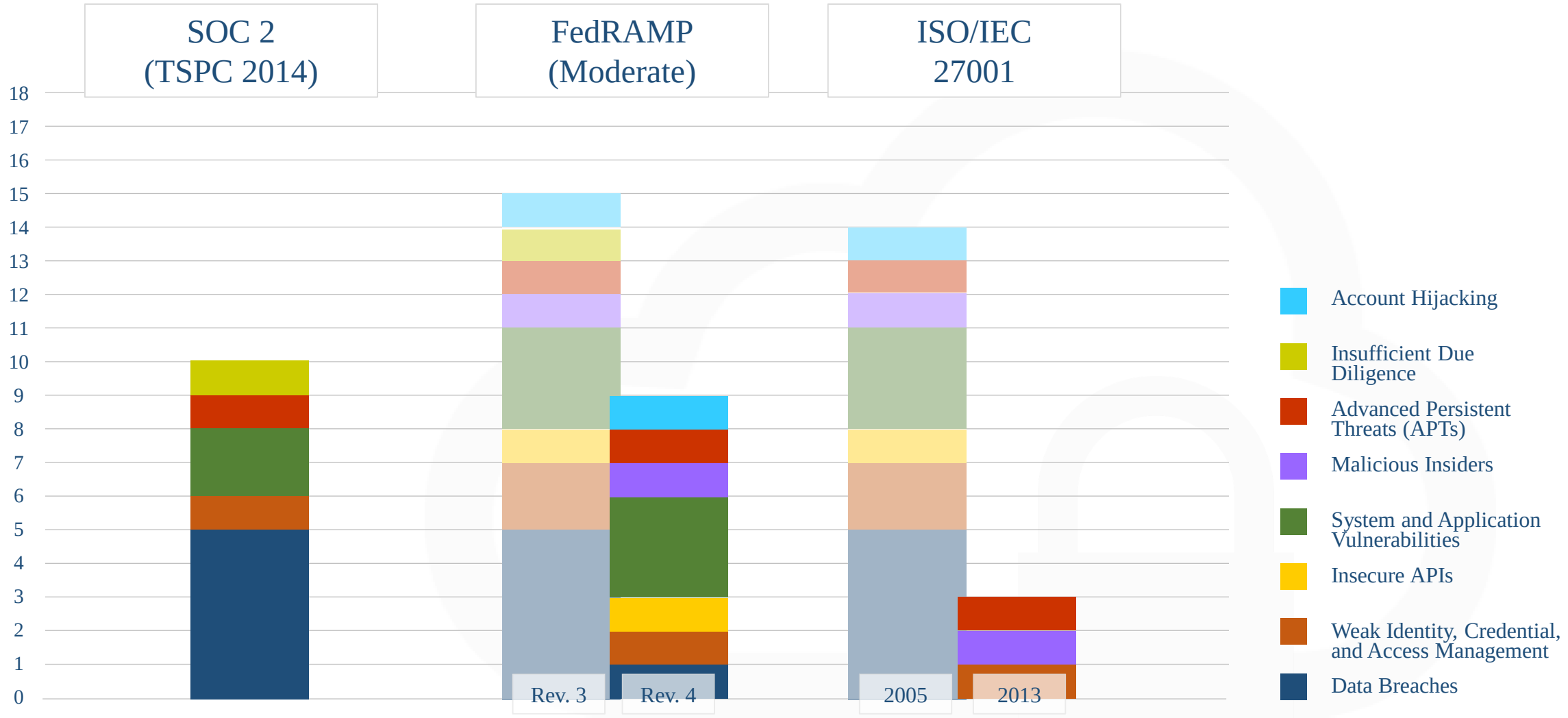
Timeline and Missing Controls (CSA CCM)



Comparison on Missing Controls (CSA CCM)



Potential Issues (CSA Treacherous 12)



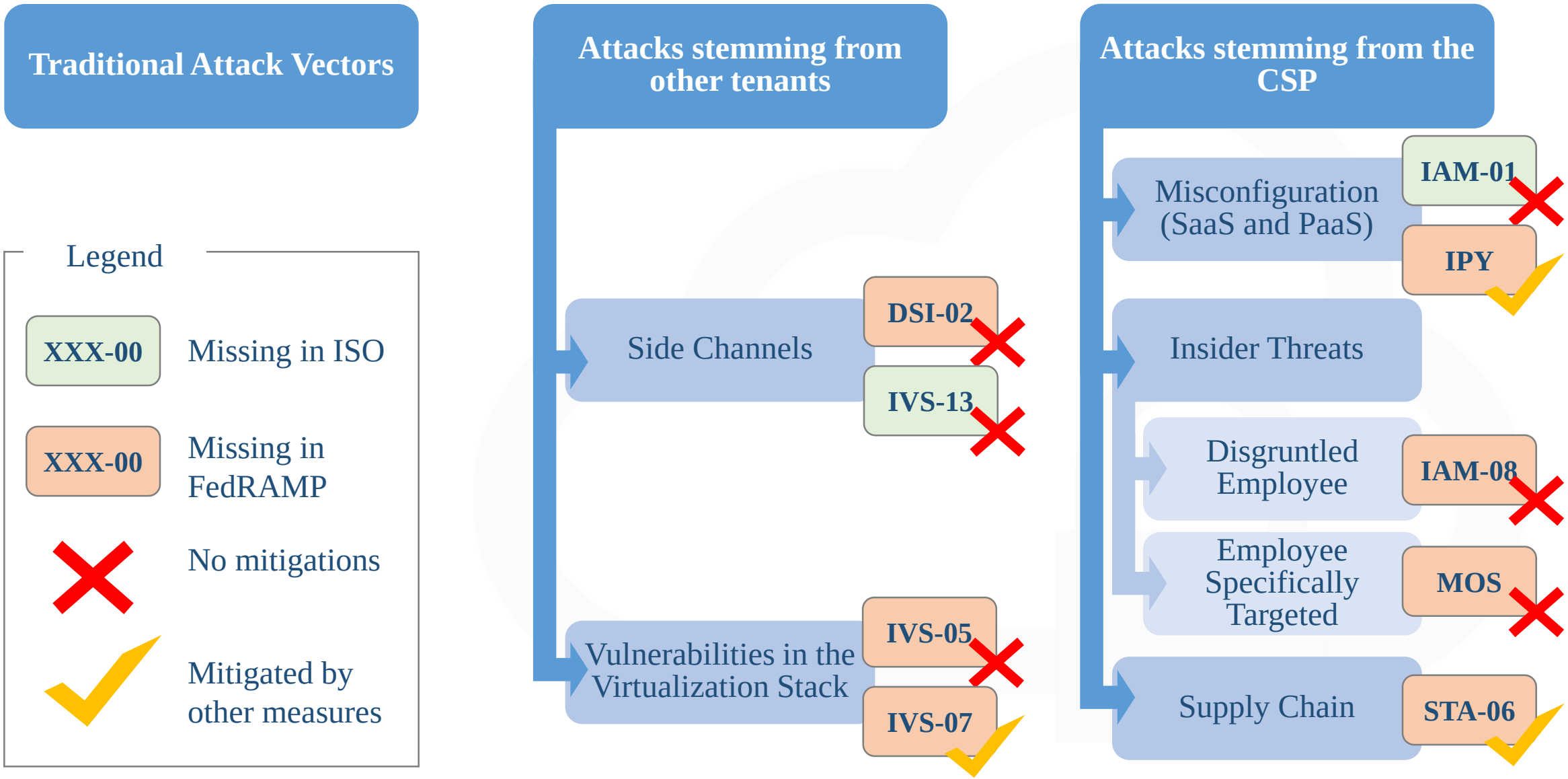
Issues Breakdown (CSA Treacherous Twelve)

DSI-02 ✗	Data Breaches	
IVS-13 ✗	Advanced Persistent Threats (APTs)	
IVS-05 ✗	Advanced Persistent Threats (APTs)	System and Application Vulnerabilities
IAM-01 ✗	Weak Identity, Credential, and Access Management	Malicious Insiders
IVS-07 ✓	Advanced Persistent Threats (APTs)	System and Application Vulnerabilities
IPY ✓		
IAM-08 ✗	Account Hijacking System and Application Vulnerabilities	Weak Identity, Credential, and Access Management Malicious Insiders Insecure APIs
MOS ✗		
STA-06 ✓	Data Breaches	

Legend

- XXX-00 — Missing in ISO
- XXX-00 — Missing in FedRAMP
- ✗ — No mitigations
- ✓ — Mitigated by other measures

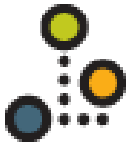
Attack Tree (missing controls in CSA CCM)



Conclusions and Future Work

- FedRAMP high has a minor impact on current measures
- The absence of MOS is relevant as source of threats
- Multiple certifications = more extensive coverage, although only a small effort is required to reach full adequacy

- Expand our research including more standards in the study (e.g. SOC 2 following TSPC 2016)
- Dive deeper in the standards analyzed to find other possible flaws
- Offer more suggestions for improvement



For more information:

Carlo Di Giulio: cdigiul2illinois.edu