Best Practices for Cloud Adoption: Government

Nigel Cory
Associate Director, Trade Policy
August, 6 2023

Email: ncory@itif.org
Twitter: @nigelcory

About ITIF

- Independent, nonpartisan research and education institute focusing on intersection of technological innovation and public policy, including:
  - Innovation and competitiveness
  - IT and data
  - Telecommunications
  - Life sciences, agricultural biotech, and energy
- World's top think tank for science and technology policy, according to the University of Pennsylvania's authoritative *Global Go To Think Tank* Index

Cloud Benefits Governments

- Cost: Cheaper for agencies to use cloud computing than maintain their own computing resources.
  - USG spends over $100 billion annually on IT, with around 75% spent on operating and maintaining current systems.
- Scalability and increased operational efficiency and resilience.
  - Smaller govt agencies can access secure and cutting-edge cloud services.

Common Challenges Govt Agencies Face in Adopting Cloud

- Ensuring cybersecurity.
  - E.g. U.S. FedRAMP system, Australia's IRAP, Japan's ISMAP, & Germany's C5.
  - Use procurement to require higher cybersecurity protections.
- Procuring secure cloud services.
  - Ensuring agencies incorporate key practices/programs in cloud service procurement.
- Maintaining a skilled workforce.
  - Agencies need a skills gap analysis for cloud personnel as part of workforce development strategy.
- Agencies need to systemically track cloud costs and savings.

US: Federal Government Cloud Procurement under FedRAMP

- FedRAMP (2011) Federal Risk & Authorization Management Program.
- **Issue:** Procuring cloud computing services is too slow, costly, and inconsistent across agencies. Agencies cited cybersecurity as barrier.
- **Goal:** Provide a standard approach to evaluating, authorizing, and monitoring the security of cloud systems.
- **Benefits:** Improved cybersecurity, cost savings, access to cutting edge services, improved operational efficiency & public services.

U.S. FedRAMP

- Assesses cloud service offerings (CSO), not entire firms.
- Tailored to risk:
  - 123 baseline controls for low-impact systems.
  - 325 for moderate-impact systems: controlled, but unclassified information.
  - 421 for high-impact systems: sensitive (but unclassified) federal information, such as law enforcement, emergency services, and health care data

FedRAMP Marketplace

PRODUCTS | AGENCIES | ASSESSORS

Total FedRAMP Authorized Services **315**

Latest on Marketplace

AUTODESK

Autodesk for Government

Now in PMO Review

zoom

Zoom for Government - JAB

Now Authorized

collabware

Collabspace

Now Authorized

Search by Provider or Product

429 total

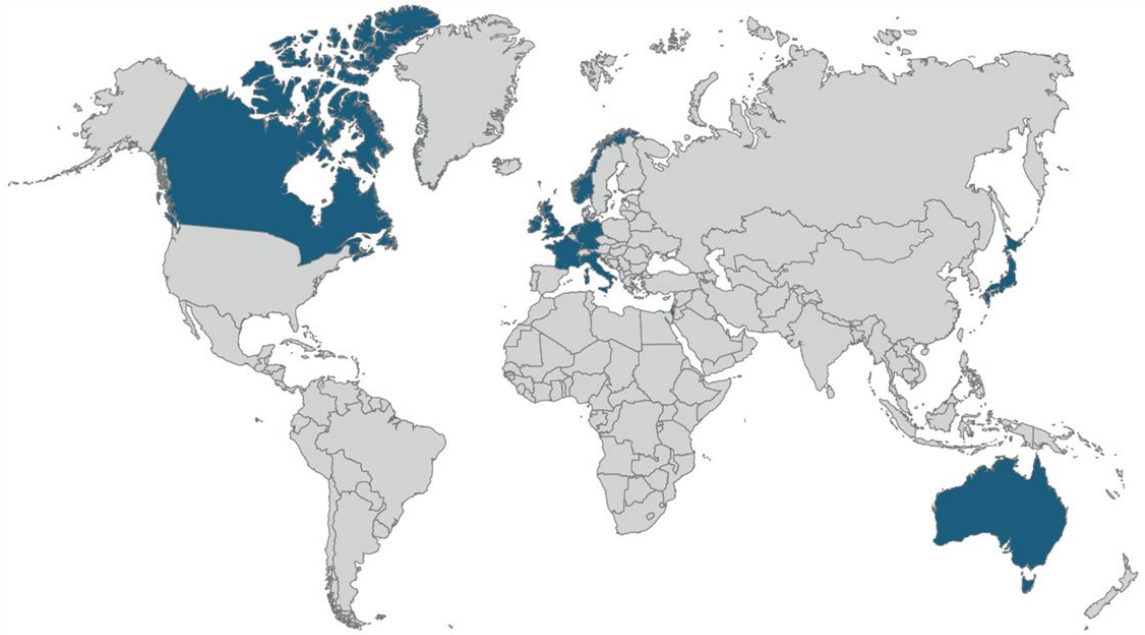
- Status +
- Business Category +
- Service Model +
- Impact Levels +
- Authorization Type +
- Deployment Models +
- Assessor +

Export to CSV

Provider	Service Offering	Service Model	Impact Level	Status	Authorizations	Reuse
CLOUD.GOV	Cloud.Gov	PaaS	Moderate	FedRAMP Authorized	17	16
1901 Group	in3sight High	SaaS	High	FedRAMP In Process	1	1
1901 Group	in3sight	SaaS	Moderate	FedRAMP Authorized	2	1
3M	RevCycle Health Services Platform (RHSP)	SaaS	Moderate	FedRAMP Authorized	1	0
ABSOLUTE	Absolute Secure Endpoint product suite	SaaS	Moderate	FedRAMP Ready	0	0
ACADIS	Acadis Readiness Suite	SaaS	Moderate	FedRAMP Authorized	8	7
Accellion	Kiteworks Federal Cloud	SaaS	Moderate	FedRAMP Authorized	14	15

FedRAMP: Focuses on Technicalities of Cybersecurity

- FedRAMP focuses on the technicalities of cloud cybersecurity - not the ownership of a firm.
- Nov 2022: Of 285 authorized service providers, at least 20 were foreign firms.
- Uses specialist third-party assessors/audits. Ongoing assessments.
- U.S National Institute of Standards and Technology (NIST) sets the technical standards for FedRAMP.



GAO Study of FedRAMP Provides Good Lessons

- **Idea:** Economies should periodically review govt cloud programs.
- 2019 GAO Review of FedRAMP:
  - Authorizations of FedRAMP services increased 137% from 2017-2019.
  - However, many agencies continued to use unauthorized cloud services.

Highlight: Need for greater oversight, monitoring, and evaluation.

Source: 2019: GAO: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked

2019 GAO Study of FedRAMP Provides Lessons

13 of the agencies saved a combined $291 million between 2014-18.

However: Agencies did not systemically track savings/spending data.

Recommendation: Needs to improve.

Table 5: Information on Total Savings and Cost Avoidances For Investments with $1 Million or More in Life-Cycle Costs For Cloud Services, Provided by the 16 Selected Agencies for Fiscal Years 2014 through 2018 and Beyond (in millions of dollars)

	Number		Dollars (millions)		
Agency	Current cloud investments	Current cloud investments with reported savings	Fiscal years 2014-2016	Fiscal year 2017	Fiscal years 2018 and beyond[a]
Department of Agriculture	57	11	4.21	$7.11	18.74
Department of Commerce	16	2	22.98	15.20	4.83
Department of Defense	115	0	0.00	0.00	0.00
Department of Education	5	2	2.23	1.61	1.12
Department of Energy	40	16	33.82	6.52	9.04
Department of Health and Human Services	61	17	36.84	17.89	57.80
Department of Homeland Security	51	3	8.98	8.06	1.66
Department of Justice	29	1	3.47	4.70	4.88
Department of Labor	3	3	3.78	1.92	6.28
Department of State	16	0	0.00	0.00	0.00
Department of the Treasury	17	7	2.04	2.46	16.40
Department of Transportation	13	2	4.86	2.20	0.02
Department of Veterans Affairs	42	2	0.10	0.00	2.10
General Services Administration	16	9	79.53	20.89	26.12
Small Business Administration	4	2	0.00	0.00	1.35
Social Security Administration	3	0	0.00	0.00	0.00
Total	**488**	**77**	**202.83**	**88.58**	**150.30**

International Standards

- International standards
  - Developed by experts from many economies.
  - Represent a way to demonstrate international cybersecurity best practices.
- Use international, not economy-specific, standards because imposing additional economy-specific security requirements leads to:
  - unnecessary duplication,
  - an increase in compliance costs, and
  - a focus on documentation and not on improved security outcomes.

ISO/IEC 27001: Information Security Management Systems.

- ISO 27001 is a globally recognized certification
  - It is a vetted, comprehensive framework for organizational security.
  - Demonstrates commitment to information security, combining risk assessment, security management, and continuous monitoring to support a holistic cybersecurity defense.
  - Requires surveillance audits during the certification period.
  - Has 114 base line controls.

Germany and Singapore: International Standards as Baseline

- Both use international standards as baseline requirements in their respective accreditation schemes:
  - ISO/IEC 27001,
  - ISO/IEC 27017 (guidelines for information security controls applicable to the provision and use of cloud services), and
  - ISO 27018 (code of practice for protection of personally identifiable information in public clouds).

Singapore's MTCS vs. ISO 27001 – Large Overlap

Level 1

The table below provides a high level summary of the differences between ISO/IEC 27001:2013 and MTCS SS Level 1. Cloud Service Providers looking to be cross certified to ISO/IEC 27001:2013 can refer to this table for total requirements applicable to this level[1]:

Total Clauses in ISO/IEC27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
	Total	%	Total	%	Total	%	Total	%
254	220	87%	34	13%	32	13%	2	1%

[1]The figures presented in the table may have a rounding variation of ±1%

Level 2

The table below provides a high level summary of the differences between ISO/IEC 27001:2013 and MTCS SS Level 2. Cloud Service Providers looking to be cross certified to ISO/IEC 27001:2013 can refer to this table for total requirements applicable to this level[1]:

Total Clauses in ISO/IEC27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
	Total	%	Total	%	Total	%	Total	%
254	228	90%	26	10%	25	10%	1	1%

[1]The figures presented in the table may have a rounding variation of ±1%

Level 3

The table below provides a high level summary of the differences between ISO/IEC 27001:2013 and MTCS SS Level 3. Cloud Service Providers looking to be cross certified to ISO/IEC 27001:2013 can refer to this table for total requirements applicable to this level[1]:

Total Clauses in ISO/IEC27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
	Total	%	Total	%	Total	%	Total	%
254	230	91%	24	9%	24	9%	0	0%

[1]The figures presented in the table may have a rounding variation of ±1%

Comparison: Audits, Controls, and International Standards

Certification Name	Country	Frequency of Audits	Number of Controls	Submission language	Recognition of ISO	Verification method
ISMAP	Japan	Annual	1,157	Japanese	No	External audit
FedRAMP	US	1/3 assessed annually, full assessment quadrennially	125 (Low), 325 (Medium), 421 (High)	English	No	External audit
BSI C5	Germany	Annual	121	English, German	Yes	External audit
ENS	Spain	Biennial	73	Spanish	Yes	External audit
CSPN	France	Triennial	N/A	English, French (report produced by government will always be French)	No	Third party evaluation company + ANSSI certification for final accreditation
AgID	Italy	Biennial	20	Italian	No	Self-assessment
Cyber Essentials	UK	Annual	89	English	No	Self-assessment
Cyber Essentials +	UK	Annual	89	English	No	External audit
IRAP	Australia	Biennial	837	English	vidence used for ISO	External audit
ISO 27001	International	Annual verification audits, triennial full audits	93 Annex A Controls	English	Yes	External audit
Common Criteria	International	Five year life-span	Varies depending on security target	English	No	External audit (certified testing labs)

Common Components & Takeaways for Policymakers

- Govts can use cloud procurement to use a set of specific controls to provide an additional, higher, and independent level assurance.
- Focus on technical aspects of cybersecurity & use ISO standards.
  - Similar to Singapore, U.S. FedRAMP standards (NIST 800-53) include a mapping to ISO 27001 controls.
- Consider third-party certification/auditing.
  - But ensure auditing is accessible and reasonable in terms of time between and depth of audits.
- Support the idea of continuous improvement/assessments.

Common Components & Takeaways for Policymakers

- Ensure accreditation team is well staffed and the process is quick.
  - FedRAMP process was initially 12-24 months, now 6 months or less.
- Ensure process is not paperwork overload. Focus on the essential.
- Create an agency liaison program to trains individuals to be cloud procurement experts within their respective agencies.
- Host meetups for small businesses and start-ups, offered in-person training sessions, and created a training platform to help local cloud firms understand and navigate the process.

Common Components & Takeaways for Policymakers

- Ensure program is non-discriminatory.
  - Cloud procurement needs to comply with WTO trade law - the General Procurement Agreement (GPA) & General Agreement on Trade in Services (GATS).
  - Unlike the European Union's emerging Cloud Cybersecurity Certification Regime (EUCS).

See: ITIF Report: Europe's Cloud Security Regime Should Focus on Technology, Not Nationality

Idea: Adapt/Recognize Other Economies Accreditation Schemes

- Economies could recognize and/or adapt accreditations from other economies.
  - Fast way to identify cloud services offerings that adhere to best practices.
- For example: New Zealand recognizes Australia's Information Security Registered Assessors Program (IRAP) accreditation.
  - It could also include the U.S. FedRAMP or Germany's C5 accreditations.

Thank You!

Nigel Cory | ncory@itif.org | Twitter: @nigelcory