

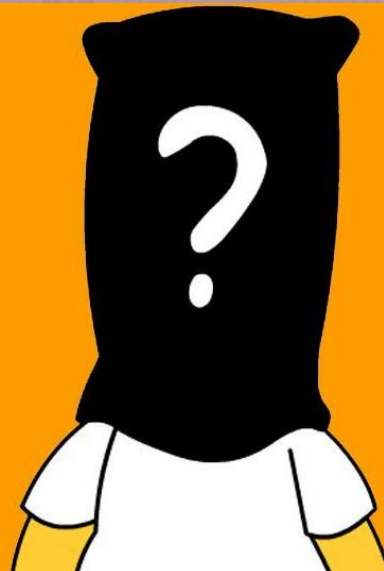


Using Common Criteria for procurement: International Procurement Initiatives

Index

- ❑ Who am I?
- ❑ Why this talk?
- ❑ Survey
 - Process
 - Results
- ❑ Worldwide Procurement Initiatives
- ❑ Conclusions

Who am I?



Who am I?

- ❑ Jose Ruiz – CTO at jtsec
- ❑ jtsec – CC and FIPS 140-2 Consultancy company - Based in Spain.
- ❑ ICCC and ICMC Program Director.
- ❑ More than 10 years of experience working with different labs and CBs as evaluator, lab manager and consultant.



Why this talk?



Why this talk?

- ❑ We support companies to meet their **business** expectations. e.g.- sales to governments.
- ❑ We like initiatives that make life **easier**.
- ❑ We think that it could be useful for developers, labs and government agencies to know what different countries do for **procurement**.



Why this talk?

- ❑ Speech on ICMC '18 – “Spanish Catalogue of Qualified Products: A New Way of Using CC for Procurement”
- ❑ During the speech, we talked about different **procurement initiatives worldwide.**
- ❑ Some of the attendees told me that it would be great to collect the information from all the **CCRA countries.**
- ❑ That's why I'm here .



The importance of procurement as a prevention tool



The Survey



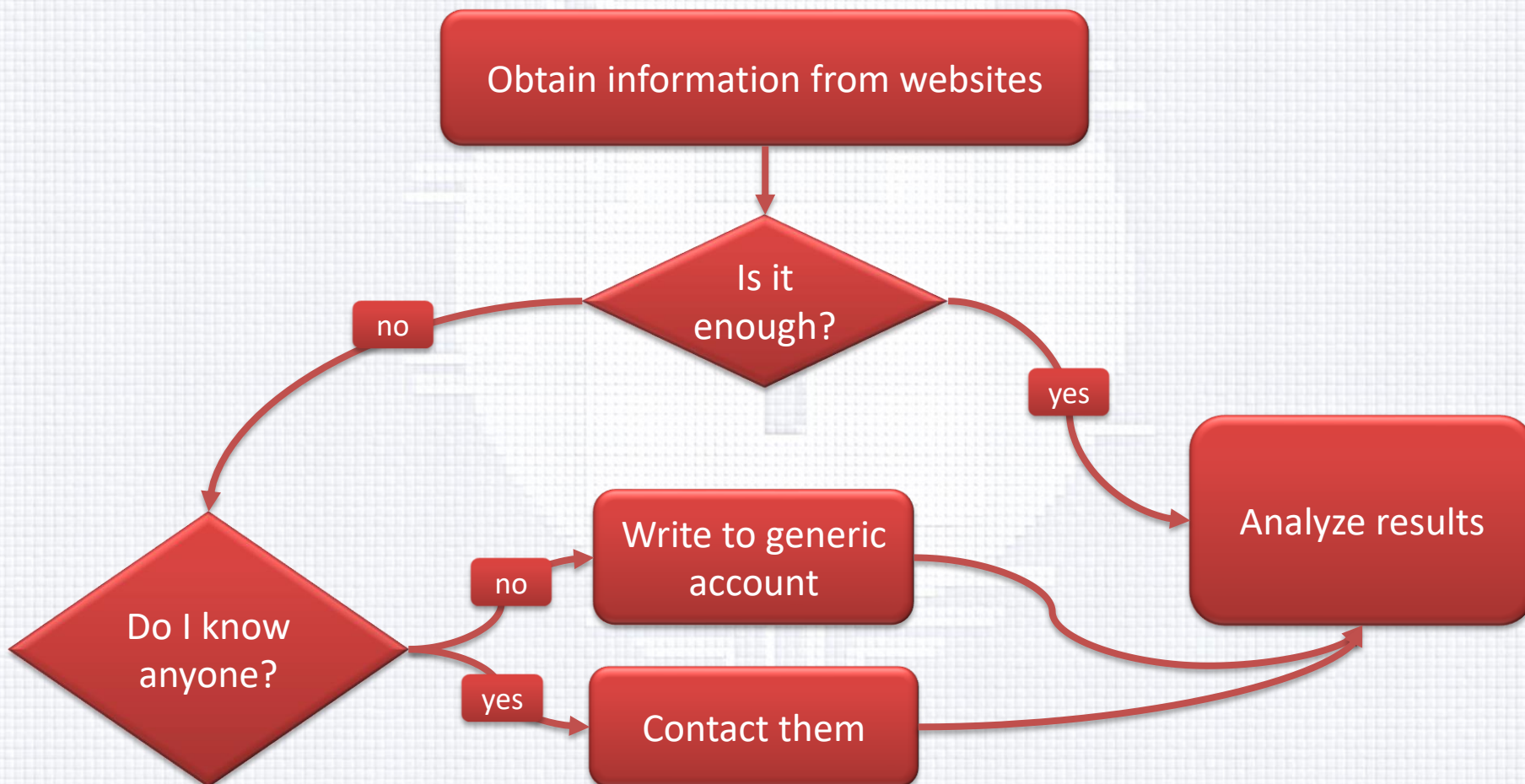
Disclaimer

- ☐ Mistakes happen! The information you are about to see can possibly contain errors.
- ☐ If you see any inconsistency, please let me know.





Survey Process

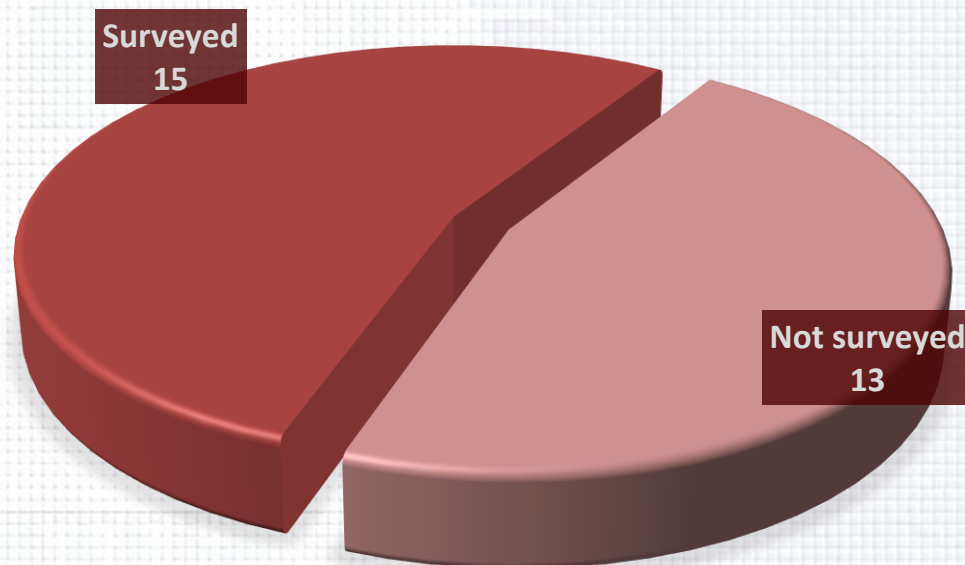


Survey Process

- ❑ The questions that I asked for the survey:
 - Does your country use Common Criteria for procurement? How?
 - Does your country use another evaluation methodology for procurement?
 - Do you think that CC meets all the certification needs? Why? (Just Informative purpose)

Survey Results

Surveyed	Not surveyed
Australia	Czech Republic
Austria	Denmark
Canada	Ethiopia
France	Finland
Germany	Greece
Hungary	India
Italy	Israel
Japan	Korea
Malaysia	New Zeland
Netherlands	Pakistan
Norway	Qatar
Spain	Singapore
Turkey	Sweden
UK	
USA	



Survey Results

	Does your country use CC for procurement?	Does your country use another evaluation methodology for procurement?
Australia	YES	YES
Austria	YES	NO
Canada	YES	YES
France	YES	YES
Germany	YES	YES
Hungary	YES	NO
Italy	YES	NO
Japan	YES	NO
Malaysia	NO	YES
Netherlands	YES	YES
Norway	YES	NO
Spain	YES	YES
Turkey	YES	NO
UK	YES	YES
USA	YES	YES

	Yes	No
Does your country use CC for procurement?	93%	7%
Does your country use another evaluation methodology for procurement?	60%	40%



Worldwide Procurement Initiatives



Worldwide Procurement Initiatives



- ❑ European Regulations apply to all the members of the European union.
- ❑ Several European Commission mandates include **certification requirements**. For example:
 - Electronic Identification
 - Authentication trust Services (EIDAS)
 - Tachograph (Vehicle Unit and Motion Sensor)





Worldwide Procurement Initiatives

❑ EIDAS Example:

- Electronic IDentification Authentication trust Services (EIDAS) - European regulation related to electronic ID and trust services.
- EIDAS Service example: A Qualified Signature Creation Device (QSCD) is a Secure Signature Generation Device that is **certified and approved** for being used to generate Qualified Electronic Signatures (QES).

EN 419 211 — Protection profiles for secure signature creation device, Parts 1 to 6 — as appropriate — as listed below:

- EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1: Overview
- EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation
- EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key import
- EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application
- EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application
- EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application





Worldwide Procurement Initiatives

- ❑ More to come: European Certification Framework.
 - The goal is to create a certification framework under which certification and assurance schemes can coexist.
 - A tailored architecture to improve efficiency and effectiveness of current assurance schemes.

EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position

08.06.2018

PRESS RELEASE

Towards the emerging EU framework on certification

The European Commission puts forward the creation of a EU certification framework for ICT security products in its 2017 proposal for a regulation.



Worldwide Procurement Initiatives

- ❑ US Government Requirements summary:
 - CC is mandatory for all IT products with security features that are deployed in U.S. National Security Systems (NSS).
 - Products are to be selected from the NIAP PCL meaning they have met a **NIAP approved Protection Profile** and compliance with the Committee on NSS Policy (CNSSP) governing the Acquisition of Information Assurance (IA) Products.
 - The NIAP is in charge of publishing approved PPs for evaluating COTS and maintaining the PCL.



Worldwide Procurement Initiatives

- ❑ US Government Requirements summary (2):
 - DoD's Information Network Approved Products List (**DoDIN APL**) .
 - Listing on the DoDIN APL is required for all products that are implemented into the technology infrastructure of the U.S. Department of Defense by mandate DoDI 8100.04 and fulfills Risk Management Framework (RMF) CS/IA testing requirements
 - **Common Criteria and very likely FIPS 140-2** validation are required.



Worldwide Procurement Initiatives

- ❑ Australian Government Requirements:
 - CC is mandatory for all products providing security functions within all Australian Government systems, unless the risks of not using CC products has been appropriately accepted and documented.
 - Products may be selected from the **Australian Evaluated Products List (EPL)** or the CC portal.
 - Another evaluation methodology for cryptographic products and high assurance applications is used. These evaluations are currently done in-house by the Australian Signals Directorate.



Worldwide Procurement Initiatives

- ❑ The Spanish Government maintains a catalogue (**CPSTIC**) of certified products which are then used by the public organisms affected by the National Security Scheme (ENS).
- ❑ **Scope:**
 - Qualified products -> Sensitive information (3 Security Levels)
 - Approved products -> Classified information (Defense)





Worldwide Procurement Initiatives

- The CPSTIC sorts products in six different categories, each of them divided in families (up to a total of 33 families).

Access Control	Network access control devices, Biometric Devices, ...	ESR
Operational Security	Anti-Virus, Endpoint Detection and Response tools, ...	ESR
Security Monitoring	IDS, IPS, Honeypot/Honeynet, Monitoring and traffic análisis, ...	ESR
Communication Protection	Routers, Switches, ...	ESR
Protection of information and information support	Encrypted data storage devices, ...	ESR
Device/Service protection	Mobile devices, Operating Systems, Anti-spam tools, ...	ESR



Worldwide Procurement Initiatives

- ❑ Requirements for each family:
 - Product family description:
 - Functionality
 - Usage case
 - Device's scope
 - CC evaluation requirements
 - Threats analysis
 - Environmental hypothesis
 - Assets
 - Threats
 - Mandatory Security Requirements (MSR)





Worldwide Procurement Initiatives

❑ Qualified Products Catalog Inclusion requirements:

- For High Security Level
 - Common Criteria - Low EAL
 - Compliance with PP or cPP required when available
- For Medium and Low Security Level
 - LINCE evaluation may be used
- The Security Target checked for **compliance with the MSR** defined in the catalogue.



❑ Approved Products Catalog Inclusion requirements:

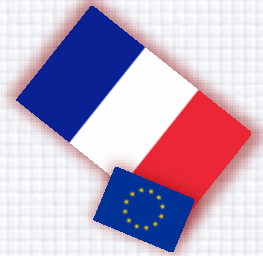
- Common Criteria required
 - High EAL



Worldwide Procurement Initiatives

❑ Canadian Government Requirements

- CC should be included as a requirement in Government of Canada RFPs/contracts **whenever possible**.
- Certified products evaluated against the **Protection Profile** for a given technology class may be selected.



Worldwide Procurement Initiatives

❑ French Government Requirements

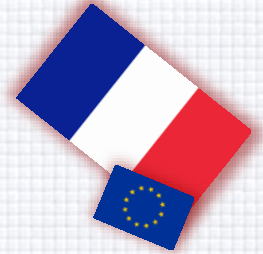
➤ **Types of certification used for procurement:**

- Common Criteria Certification
- **First Level Security Certification – CSPN**

➤ **Acquisition Policy:**

- CSPN for elementary qualification
- EAL3+VAN.3+FLR.3 for standard qualification or
- EAL4+VAN.5 +IMP.2+ DVS.2+FLR.3 for reinforced qualification

Worldwide Procurement Initiatives



- ☐ The First Level of Security Certification (CSPN) is a **lightweight** evaluation methodology based in Common Criteria.
- ☐ Cost effective alternative and **limited in time** (8 weeks)
- ☐ Focus on **Vulnerability Analysis and Penetration testing**.





Worldwide Procurement Initiatives

❑ UK Government Requirements

➤ **Types of certification used for procurement:**

- Common Criteria Certification
- Commercial Product Assurance – CPA

- **CPA:** A security product that passes assessment is awarded Foundation Grade certification - demonstrate good commercial security practice and suitable for lower threat environments.



National Cyber
Security Centre



Worldwide Procurement Initiatives

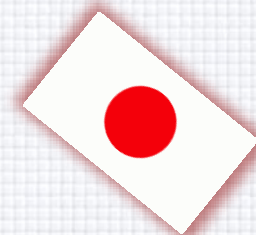
□ Italy Government Requirements:

- Common Criteria is used for procurement and certifications are often requested but there is no general procurement catalog for security-related products.
- An example of this can be found in the Direttiva 2004/18/CE:

Informazioni e formalita' necessarie per valutare la conformita' ai requisiti: A dimostrazione dell'idoneita' per la partecipazione alla gara deve essere prodotta la seguente documentazione:

with «ICAO Application», Basic Access Control, **BSI-CC-PP-0055** Versione 1.10 (almeno di livello EAL 4+) [ovvero] che il prodotto (chip + sistema operativo) ha superato con successo la fase di valutazione della sicurezza presso un laboratorio accreditato;

- No other evaluation methodology is used, although they often require other standard certifications such as ISO27001.



Worldwide Procurement Initiatives

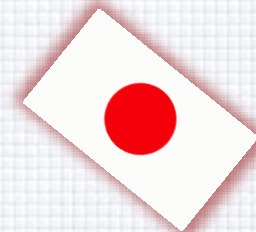
❑ Japan Government Requirements

- They have 11 product areas to which they apply Common Criteria for procurement.


MFP	Firewall	IDS/IPS	Operating System
Database	USB	Smartcard/IC	Router
HDD	Mobile device	VPN	


- There are standards for things like government-recommended encryption, although there is no mandatory or unified certification.


Worldwide Procurement Initiatives



- List of Protection Profiles to use under the Japanese scheme and a list of certified products in the IPA website.

Certification #	Supplier	TOE Name for Overseas	Certification Date	Conformance Claim/PP	Recognized By
		TOE Name for Japan			
New C0619	Xerox Corporation	Xerox D136 Copier/Printer Controller+PS ROM Ver. 1.200.15	2018-09	●PP(U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)	

New C0618	Xerox Corporation	Xerox D95/D110/D125 Copier/Printer Controller+PS ROM Ver. 1.204.17	2018-09	●PP(U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)	

New C0617	KYOCERA Document Solutions Inc.	TASKalfa 3212i, TASKalfa 3212iG(KYOCERA), 3262i(TA Triumph-Adler/UTAX) all of the above with Data Security Kit and FAX System System: 2V6 20IS.C01.010 Panel: 2V6 70IS.C01.010 FAX: 3R2 5100.003.012	2018-09	EAL2	
		TASKalfa 3212i, TASKalfa 3212iG(KYOCERA), 3262i(TA Triumph-Adler/UTAX) all of the above with Data Security Kit and FAX System			

Certification #	Sponsor	PP Name	Certification Date	Conformance Claim
C0553	Information-technology Promotion Agency, Japan	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015	2016-05	PP Compliant
C0500	Ministry of Foreign Affairs, Japan	Protection Profile for ePassport IC with SAC (BAC + PACE) and Active Authentication 1.00	2016-03	EAL4+ ALC_DVS.2
C0499	Ministry of Foreign Affairs, Japan	Protection Profile for ePassport IC with SAC (PACE) and Active Authentication 1.00	2016-03	EAL4+ ALC_DVS.2, AVA_VAN.5
C0431	Japan Agency for Local Authority Information Systems	Personal Number Cards Protection Profile 1.00	2014-05	EAL4+ ALC_DVS.2, AVA_VAN.5
C0247	Ministry of Foreign Affairs, Japan	Protection Profile for ePassport IC with Active Authentication 1.00	2010-02	EAL4+ ALC_DVS.2, AVA_VAN.5

Worldwide Procurement Initiatives



❑ Netherlands Government Requirements

- Common Criteria procurement is not mandatory in general, but needed for some projects (e.g. e-passports).
- They use BSPA as a different evaluation methodology for procurement.
 - “The Dutch Baseline Security Product Assessment (BSPA) provides information on the suitability of IT security products for use in the ‘sensitive but unclassified’ domain” – State of the Union 2017, Cybersecurity factsheet.

Worldwide Procurement Initiatives



- ❑ Hungary Government Requirements
 - Common Criteria is not enforced by default. Only when required due to **European regulation**.
 - No other certification methodologies are applied.
 - There is a law about the information security of governmental systems. This makes it compulsory for the governmental offices to classify the systems based on a risk analysis into one of the categories, and there are requirements for each category.



Worldwide Procurement Initiatives

- ❑ Malaysia Government Requirements
 - CC is **not used** for procurement
 - Malaysia is currently looking into enforcing Common Criteria for procurement of products to be used in **critical national infrastructures**.
 - CyberSecurity Malaysia has launched another scheme which is Technology Security Assurance (TSA) as a parallel evaluation methodology.

Technology Security Assurance certification to be made mandatory

Bernama / Bernama
September 25, 2018 23:02 pm +08

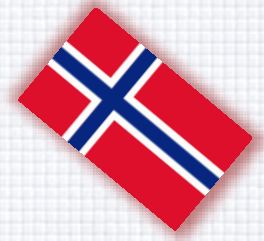
KKMM plans to make technology security assurance certification mandatory

Last update: 26/09/2018



Worldwide Procurement Initiatives

- ❑ Turkey Government Requirements
 - No general procurement catalog for security-related products
 - Some ministries and government organizations have regulations about Common Criteria.
- ❑ Some examples of these regulations are:
 - EAL 4+ certification for Digital Signature products.
 - EAL 4+ certification for Email Service providers' products.
 - EAL 2 certification for Health Informatic Software.
 - New Generation Cash Register Fiscal Application Software to be conformant to the "New Generation Cash Register Fiscal Application Software" PP.



Worldwide Procurement Initiatives

- ❑ Norway Government Requirements:
 - No national regulations regarding the use of Common Criteria for procurement in Norway except for **classified systems** under the Security act.
 - Some EU directives implemented in Norway require use of Certified products. In any other case, the use of certified products is voluntary in Norway.
 - Acquisition Authorities in Norway are bound to follow the Public Procurement Act, which does not mandate Certification requirements itself. It is up to the Acquisition Authority to decide and define which selection or evaluation criteria to use.

Worldwide Procurement Initiatives



- ❑ German Government Requirements:
 - Common Criteria is **widely used** in Germany's government, in particular, in the framework of the digitization projects and the area of further regulation requirements.
 - Other CC-based methodologies are used

Worldwide Procurement Initiatives



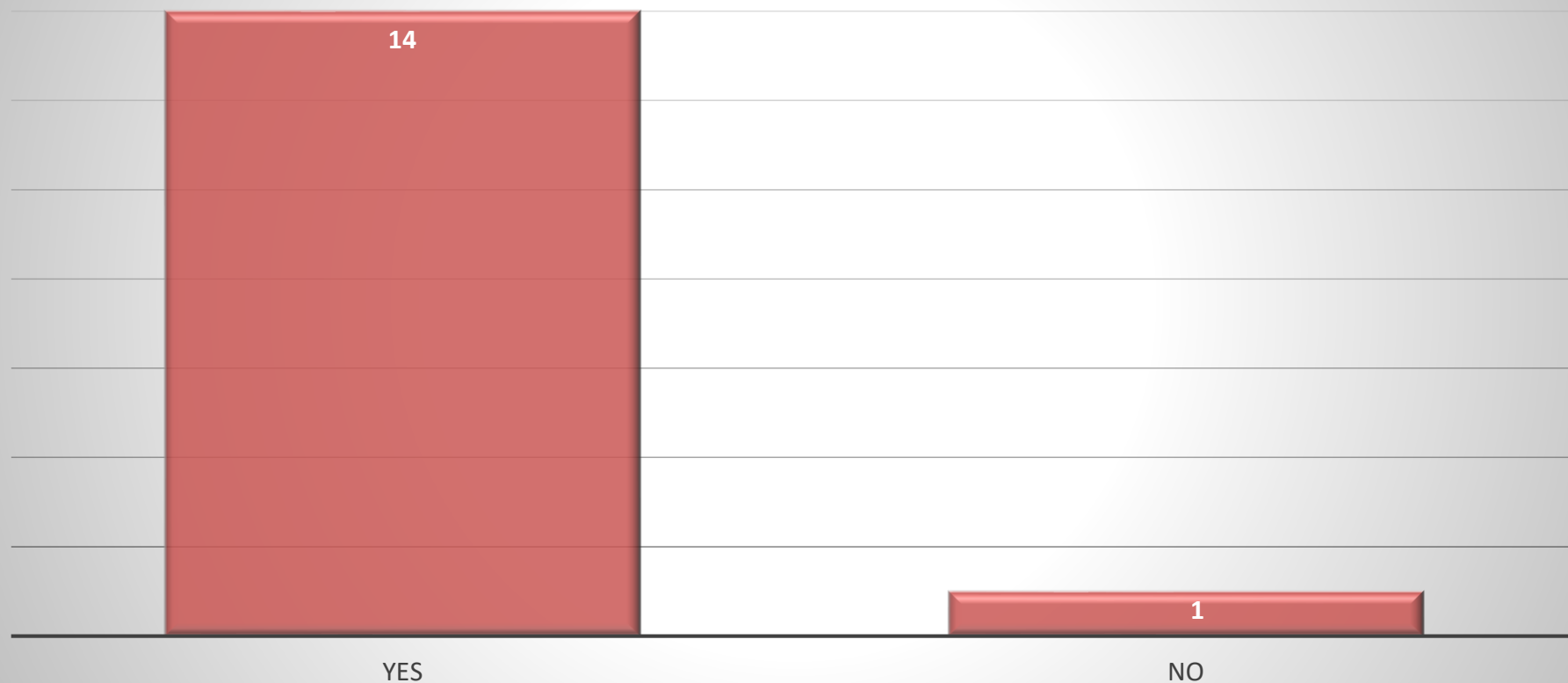
- ❑ Austria Government Requirements:
 - CC is not formalized as a general requirement - Only when required due to **European regulation**. There are organism who use CC but it is not required and depends largely on the product and vendor.
 - No other certification is used for procurement.
 - In some cases, service providers may have to follow the Austrian Information Security Manual, which is similar to ISO 27001.

Conclusions



Conclusions

☐ Does your country use CC for procurement?



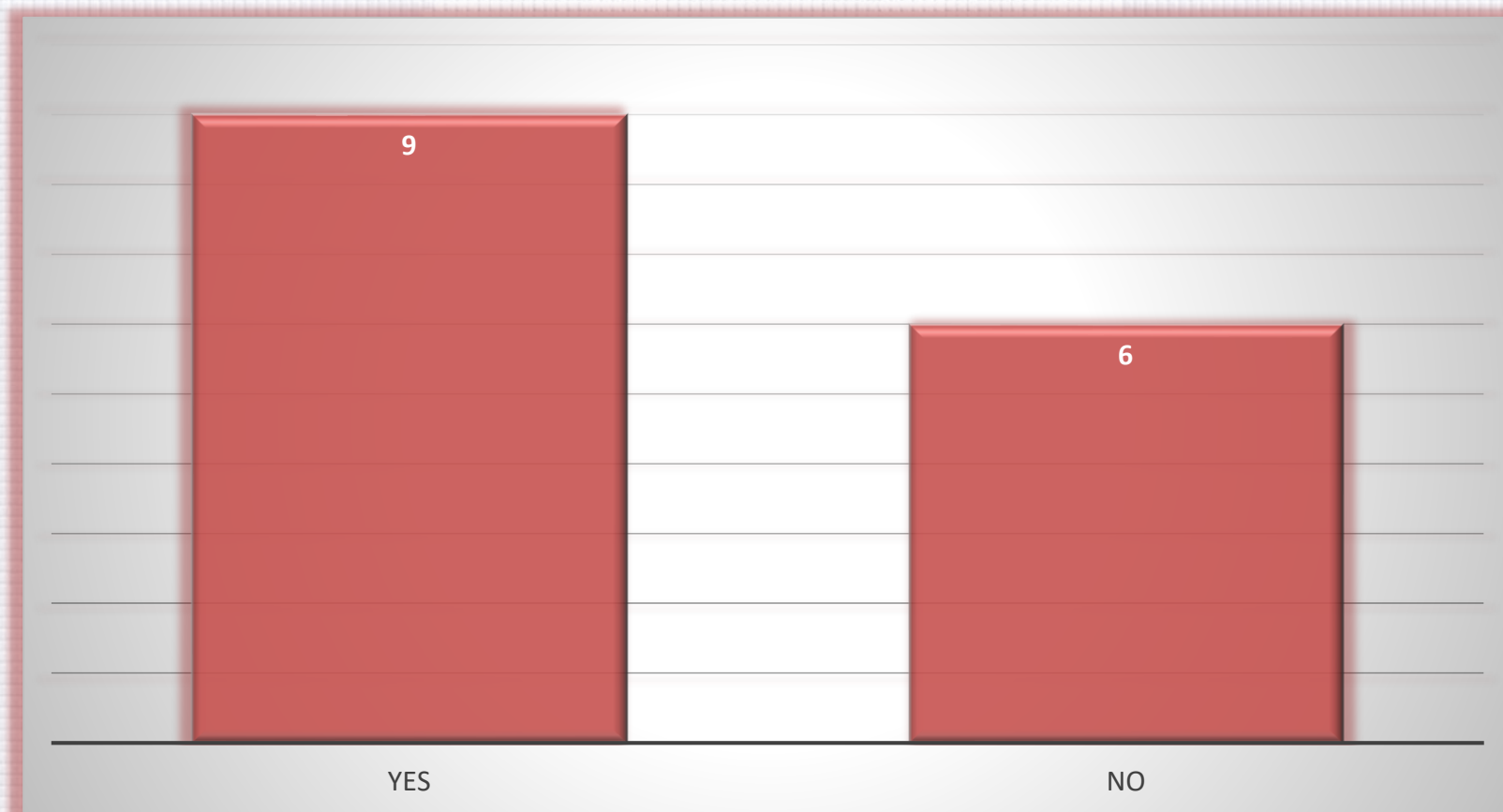
Conclusions

❑ 4 Different Approaches:

- Use of a **Product List/Catalogue** with certified products.
- **Regulations** include Common Criteria or other methodologies for Procurement.
- Common Criteria or other methodologies are used **on demand** for procurement process.
- **No use** of Common Criteria or other methodologies for procurement.

Conclusions

- ☐ Does your country use another evaluation methodology for procurement?



The third question

❑ Does Common Criteria meet all the certification needs of your country?

“The approach should be that, whenever possible, only CC certified validated products are trusted.”

“CC meets all requirement items needed for government procurement. If we need another requirement in the future, we will request CC to add it.”

“CC meets all the certification needs, although its application **involves time and effort which may be unavailable.**”

“CC does not always represent a **necessary or sufficient level** of product assurance.”

“CC might work well for products where proven and widely used standards exist. For specifically tailored products or services, or also **for emerging technologies there is some doubt** if applying rigid certification requirements in procurement is fit for purpose.”

“The Common Criteria are a very powerful, flexible and long-time experienced and well-proven tool for the security evaluation and certification of products. For the application, we prefer and recommend the use of Protection Profiles.”

“CC meets all the certification needs as long as it is based on enforced PPs.”

“Common Criteria has **met all our certification needs so far**, but that cannot be guaranteed for the **future.**”

“CC is **far from perfect** and its shortcomings are often pointed out by government users. Usual complaints are around **cost and duration**, but also regarding the lack of sufficient assurance. Yet, CC outperforms other existing evaluation schemes.”

My Conclusion

- ❑ Does Common Criteria meet all the certification needs?
 - “Common Criteria is a very powerful methodology that must be adapted to meet all the market needs in terms of cost, time to market and new technology trends.”
- ❑ Preferred approach for procurement:
 - Use of a **Product List/Catalogue** is more straightforward and easy

Thank you!

jtsec: Beyond IT Security

c/ Abeto s/n Edificio CEG Oficina 2B

CP 18230 Granada – Atarfe – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es



**“Any fool can make something complicated. It
takes a genius to make it simple.” - Woody
Guthrie**