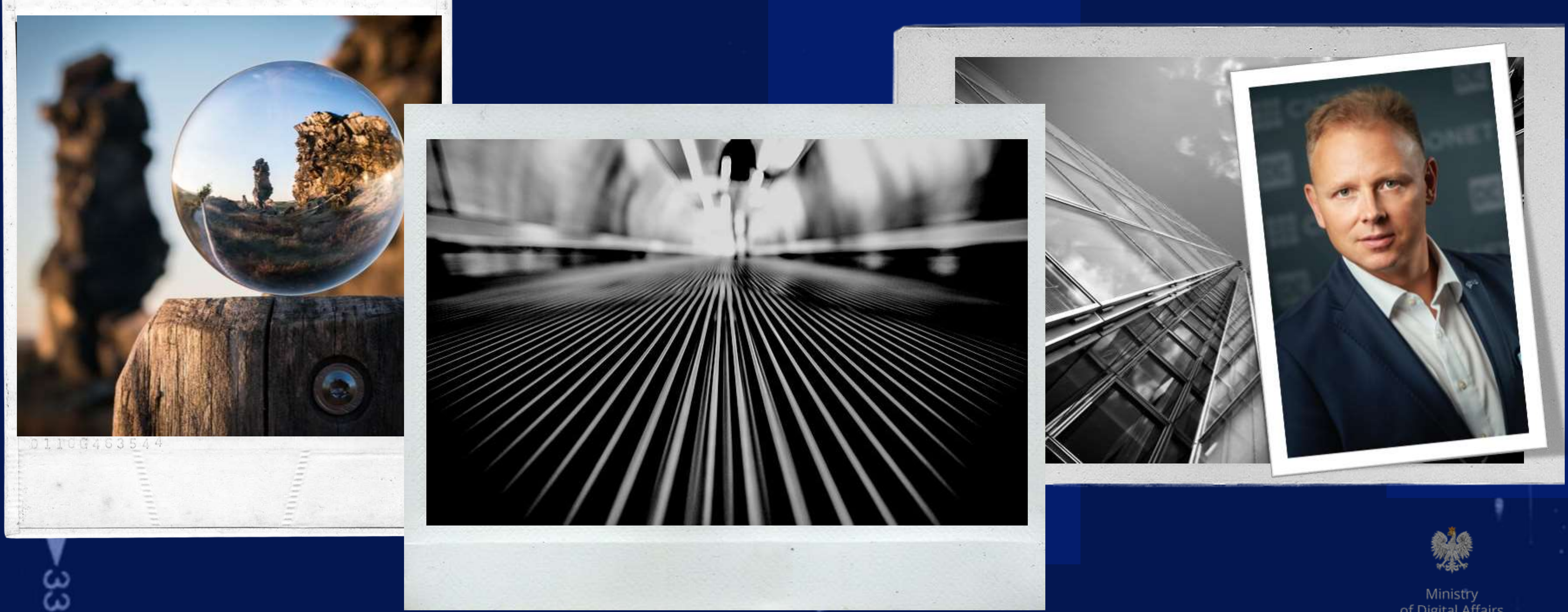


Ministry
of Digital Affairs

ROBERT KOŚLA, Lt. Col. (Ret.)

Director, Department of Cybersecurity,
Ministry of Digital Affairs

The Polish perspective on Cloud Computing Cybersecurity Requirements

Act on National Cybersecurity System – NIS in Poland

On 5 July 2018, the Polish Parliament passed the Act on the National Cybersecurity System ("ANCS" J. of Laws 2018.1560), which enter into force on 28 August 2018.

The ANCS implements the provisions of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive").

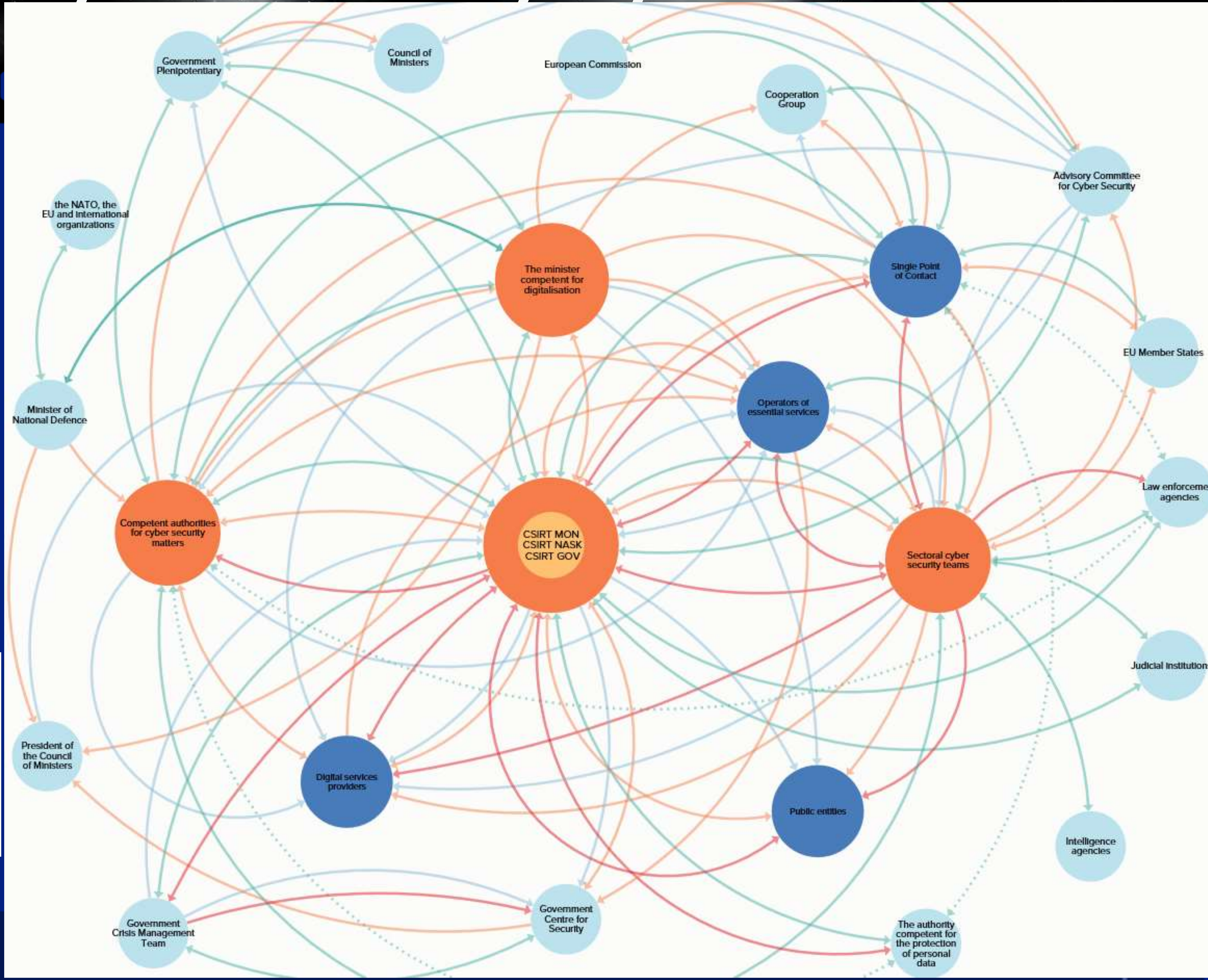
OK

33

Done ?

Legend

- - - - - Opposite
— cooperation
— exchange of data
— incident managements
— recomendations
● Cybersecurity actors

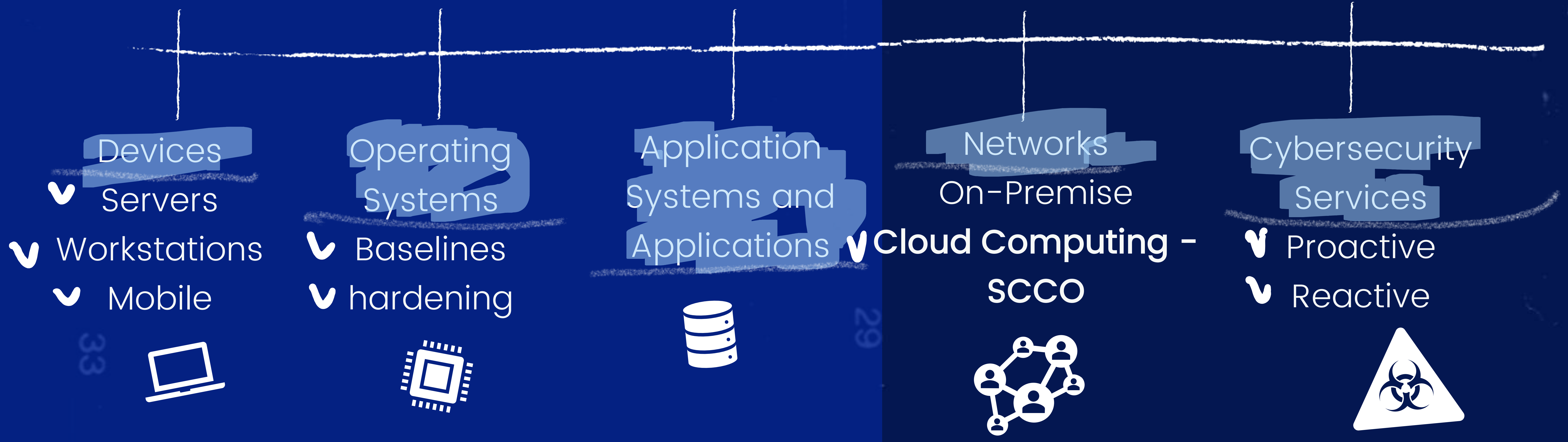


Government Plenipotentiary
Council of Ministers
European Commission
Cooperation Group
Advisory Committee for Cyber Security
the NATO, the EU and International organizations
The minister competent for digitalisation
Single Point of Contact
EU Member States
Minister of National Defence
Operators of essential services
Law enforceme agencies
Competent authorities for cyber security matters
CSIRT MON
CSIRT NASK
CSIRT GOV
Sectoral cyber security teams
Judicial Institution
President of the Council of Ministers
Digital services providers
Public entities
Intelligence agencies
Government Crisis Management Team
Government Centre for Security
The authority competent for the protection of personal data

Source: https://www.cybsecurity.org/pl/act-on-the-national-cyber-security-system/

National Standards for Cybersecurity (NSC)

Cybersecurity Requirements / Baselines / Recommendations



Devices

✓ Servers

✓ Workstations

✓ Mobile

Operating Systems

✓ Baselines

✓ hardening

Application Systems and Applications

Networks

On-Premise

✓ **Cloud Computing - SCCO**

Cybersecurity Services

✓ Proactive

✓ Reactive

Cybersecurity requirements for WIIP – Government Cloud and Public Cloud use

Cybersecurity in WIIP PROGRAM

Government Cloud Datacenters security requirements (WIIP - Appendix 1)

Cloud model classification criteria (WIIP - Appendix 2)

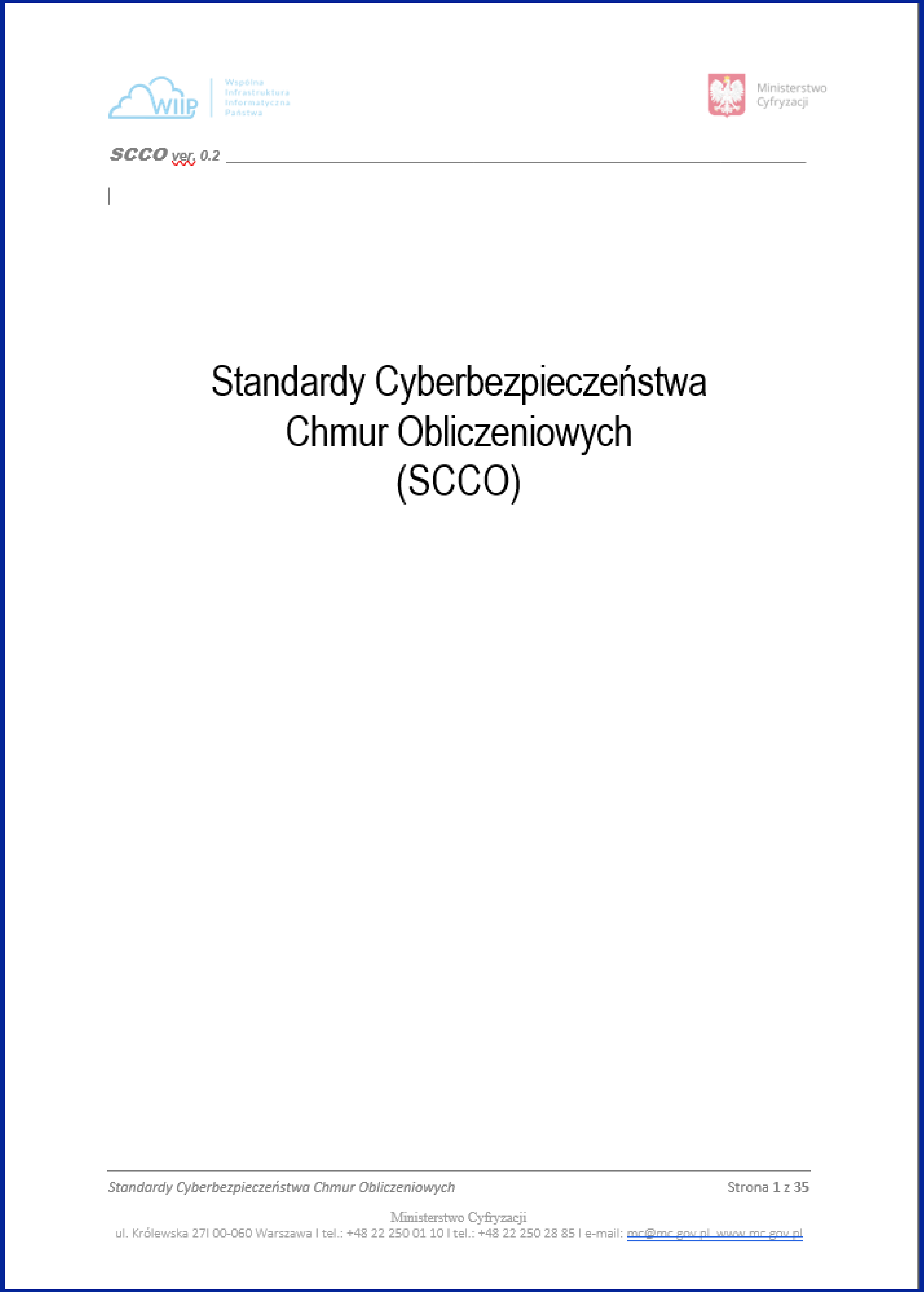
RKB – Government Cybersecurity Cluster

- SOC
- NOC
- Interconnections security

SCCO – Cybersecurity Requirements for Cloud Computing

Other initiatives e.g. PWCyber - Cybersecurity Cooperation Program with vendors and service providers

SCCO – Cybersecurity Standards for Cloud Computing



WIIP Wspólna Infrastruktura Informatyczna Państwa

Ministerstwo Cyfryzacji

SCCO ver. 0.2

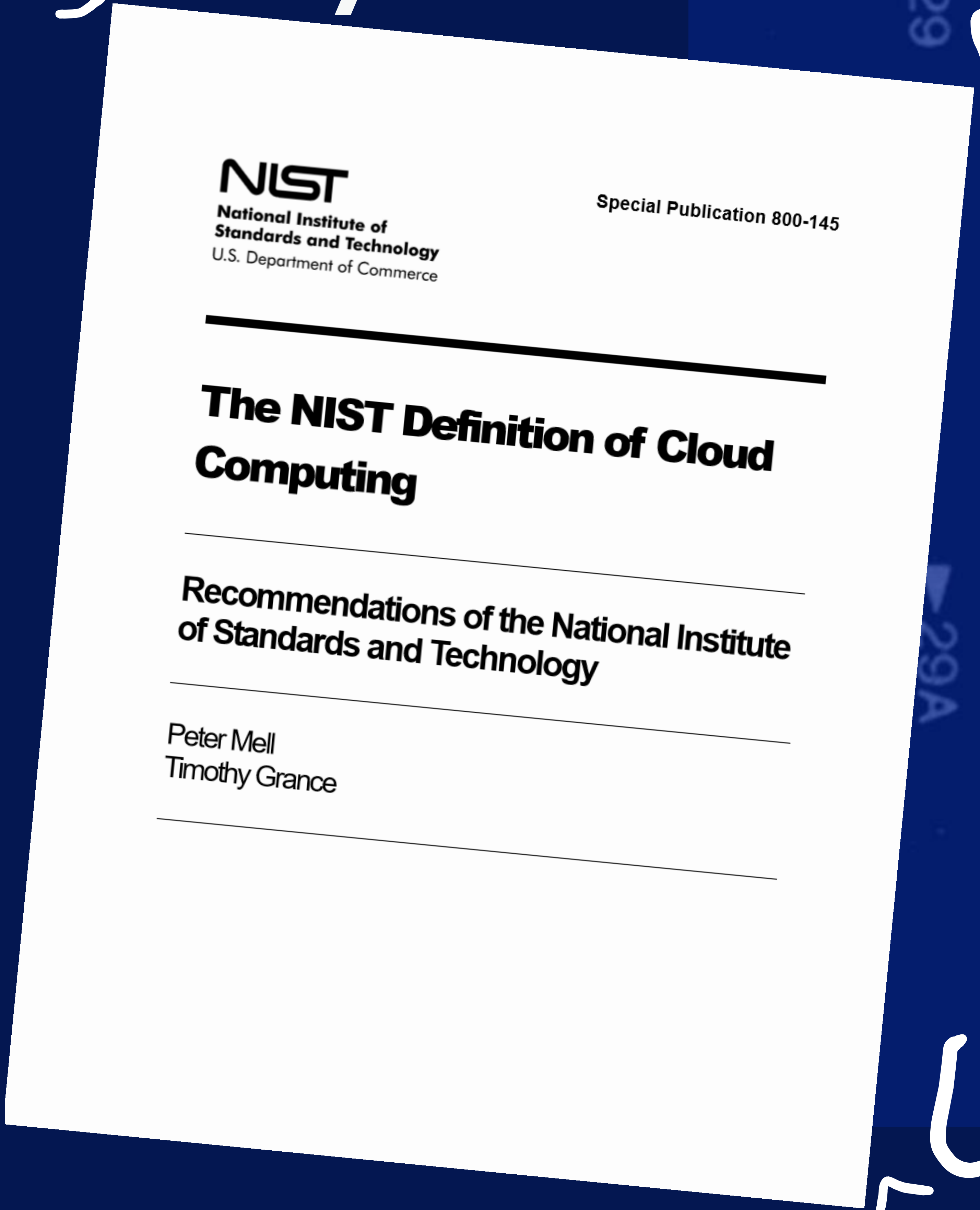
Standardy Cyberbezpieczeństwa
Chmur Obliczeniowych
(SCCO)

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych Strona 1 z 35

Ministerstwo Cyfryzacji
ul. Królewska 27l 00-060 Warszawa l tel.: +48 22 250 01 10 l tel.: +48 22 250 28 85 l e-mail: mc@mc.gov.pl www.mc.gov.pl

- SCCO Background and Goals
  - Integral part of National Standards for Cybersecurity (NSC)
  - Standardized approach to security assessment, authorization, and continuous monitoring of cloud based services
  - Introduction for Cloud Computing deployment and service models
  - Definition of Cloud Computing Cybersecurity Impact Levels (C3IL)
  - Practical mapping between C3IL and Security Controls/Measures
- Future references to EU wide Cloud Computing Certification Program

SCCO – Cloud Computing deployment and delivery models



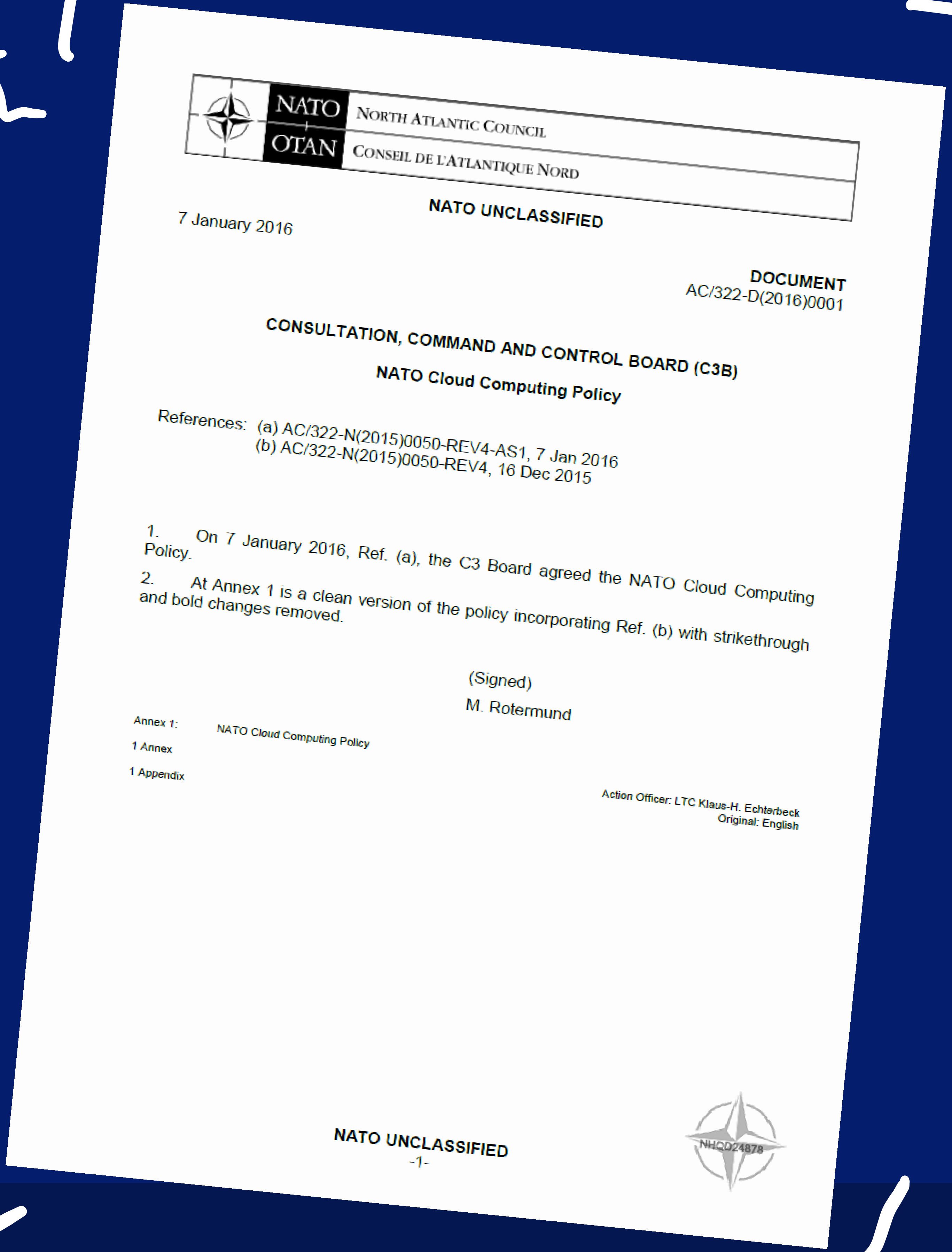
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance



NATO / OTAN
NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

7 January 2016

DOCUMENT
AC/322-D(2016)0001

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

NATO Cloud Computing Policy

References: (a) AC/322-N(2015)0050-REV4-AS1, 7 Jan 2016
(b) AC/322-N(2015)0050-REV4, 16 Dec 2015

1. On 7 January 2016, Ref. (a), the C3 Board agreed the NATO Cloud Computing Policy.

2. At Annex 1 is a clean version of the policy incorporating Ref. (b) with strikethrough and bold changes removed.

(Signed)
M. Rotermund

Annex 1: NATO Cloud Computing Policy
1 Annex
1 Appendix

Action Officer: LTC Klaus-H. Echterbeck
Original: English

NATO UNCLASSIFIED
-1-

NHQD24878

SCCO – Security Objectives and Potential Impact – Security Category

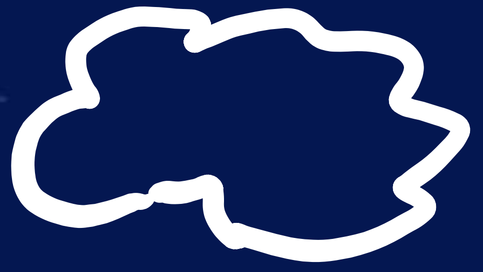
Based on FIPS PUB 199

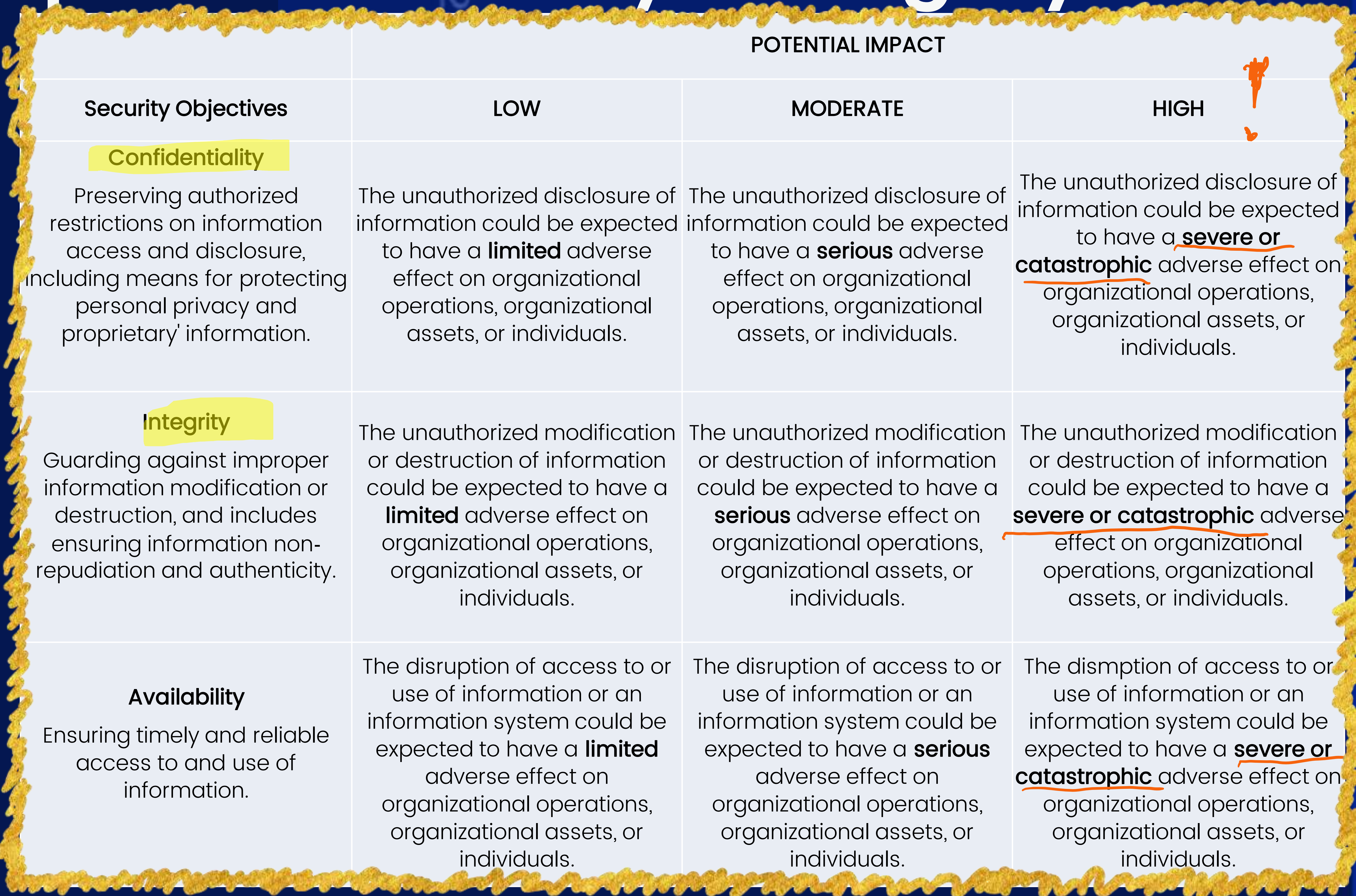
Security Category (SC) of an information system is:

SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH

$sc = (x, x, x)$





	POTENTIAL IMPACT		
Security Objectives	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary' information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The dismption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

SCCO – Security Requirements Areas

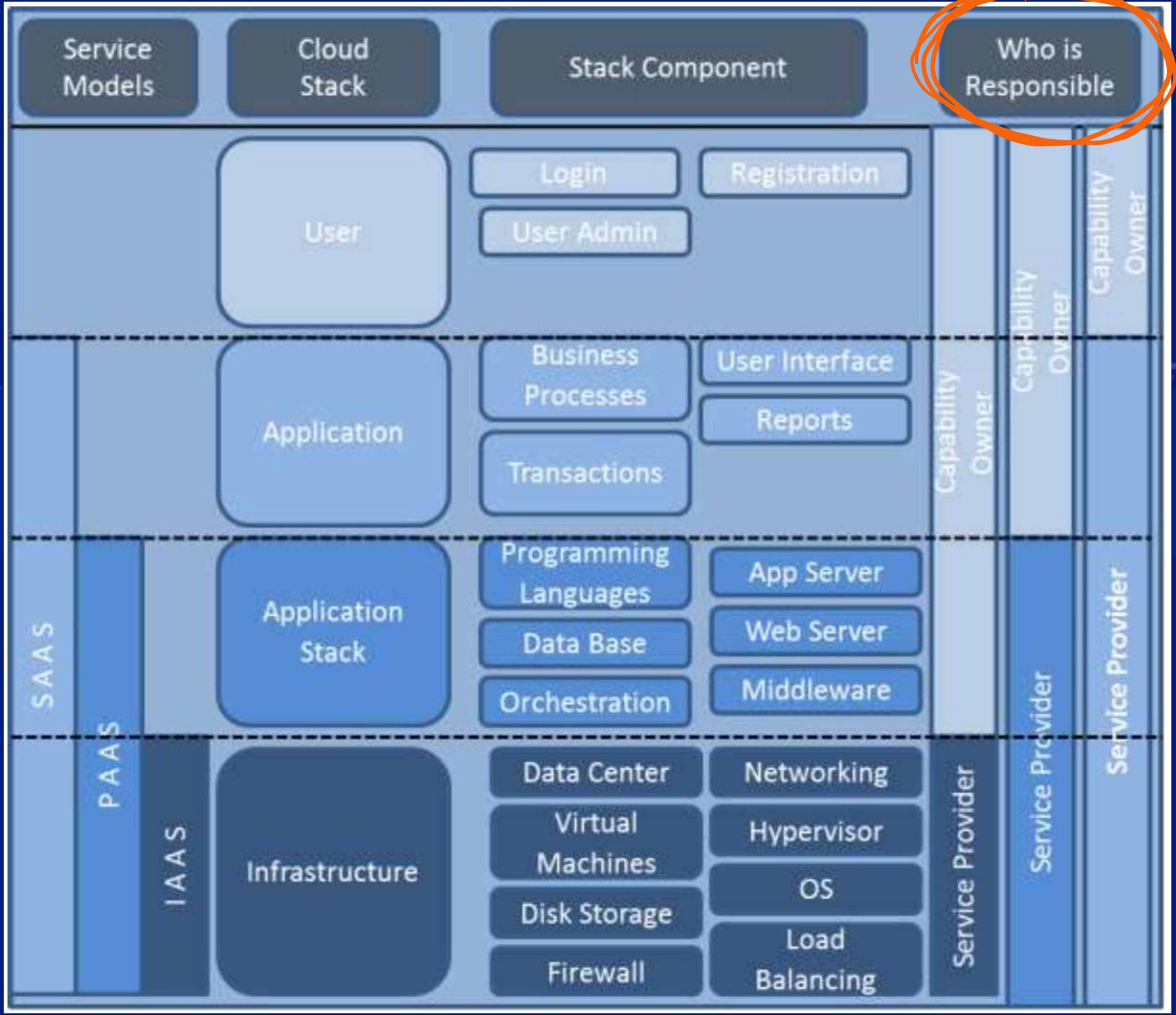
Based on FIPS PUB 200

17 Areas

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

SCCO – Cloud Stack Model

NATO & NATIONS VIEW ON CLOUD



Service Models

Cloud Stack

Stack Component

Who is Responsible

User

Login

Registration

User Admin

Application

Business Processes

User Interface

Reports

Transactions

Application Stack

Programming Languages

App Server

Data Base

Web Server

Orchestration

Middleware

Infrastructure

Data Center

Networking

Virtual Machines

Hypervisor

Disk Storage

OS

Firewall

Load Balancing

SAAS

PAAS

IAAS

Capability Owner

Capability Owner

Capability Owner

Service Provider

Service Provider

Service Provider

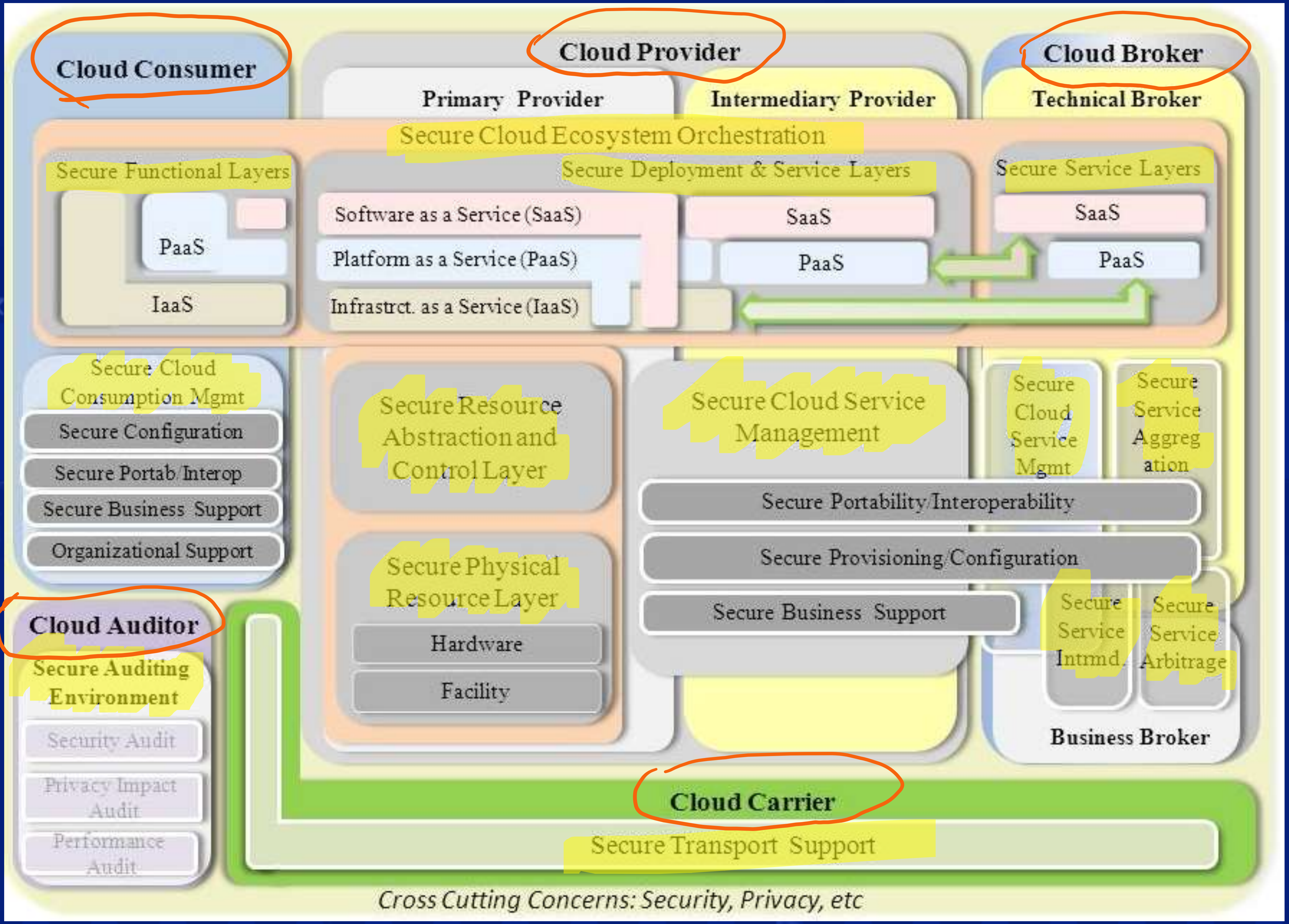
Based on NATO Cloud Computing Policy - AC/322-D(2016)0001

SCCO - Cloud Computing Roles and Responsibilities

5 Cloud Roles

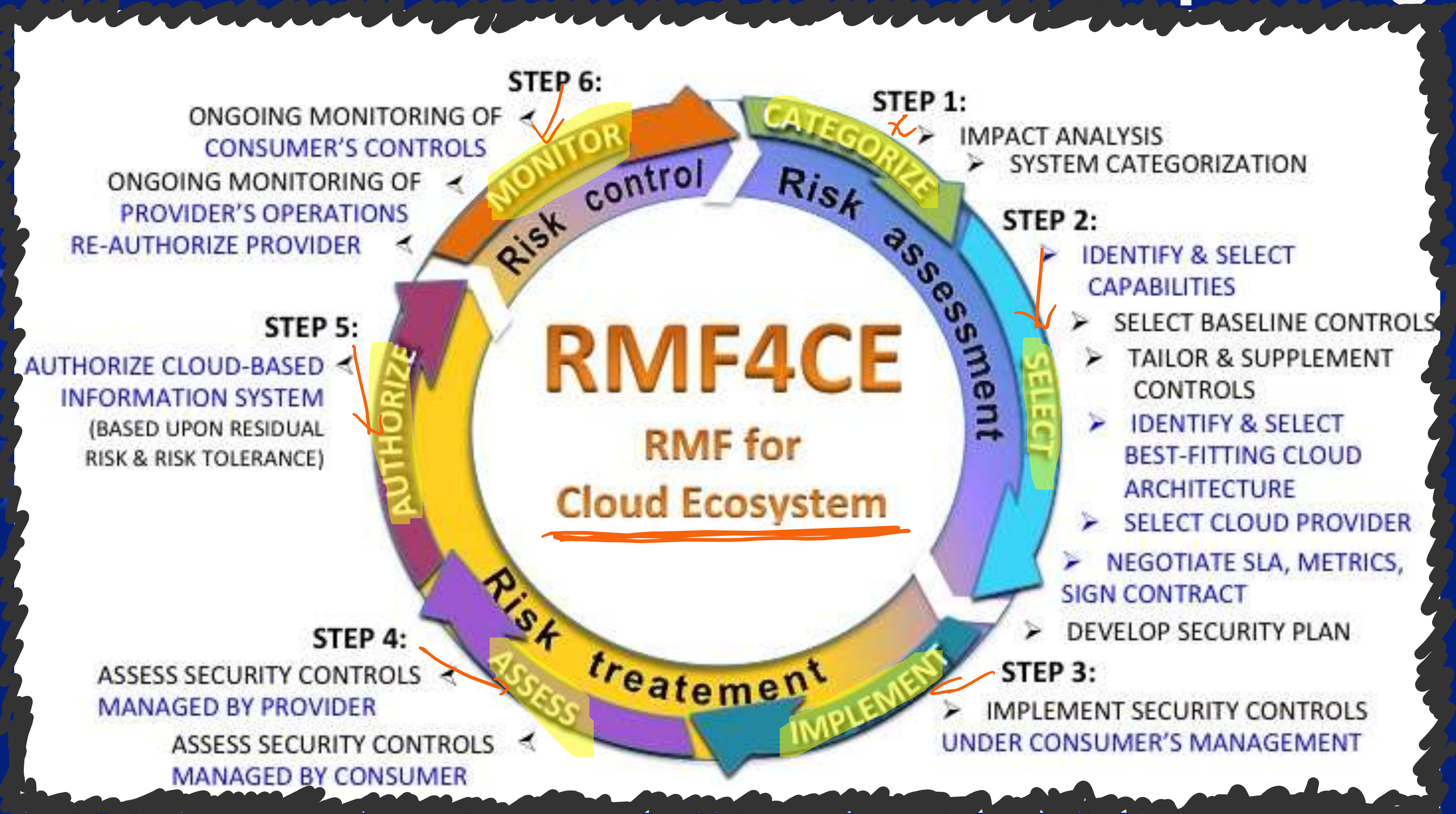
- Cloud Consumer - a person or organization that maintains a business relationship with, and uses service from, Cloud Providers
- Cloud Provider - a person, organization, or entity responsible for making a service available to interested parties
- Cloud Auditor - a party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation
- Cloud Broker - an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers
- Cloud Carrier - an intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers

SCCO – Cloud Computing security reference architecture


Cloud Consumer
Cloud Provider
Cloud Broker
Primary Provider
Intermediary Provider
Technical Broker
Secure Cloud Ecosystem Orchestration
Secure Functional Layers
Secure Deployment & Service Layers
Secure Service Layers
PaaS
IaaS
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastrct. as a Service (IaaS)
SaaS
PaaS
SaaS
PaaS
Secure Cloud Consumption Mgmt
Secure Configuration
Secure Portab/Interop
Secure Business Support
Organizational Support
Secure Resource Abstraction and Control Layer
Secure Physical Resource Layer
Hardware
Facility
Secure Cloud Service Management
Secure Portability/Interoperability
Secure Provisioning/Configuration
Secure Business Support
Secure Cloud Service Mgmt
Secure Service Aggreg ation
Secure Service Intrmd.
Secure Service Arbitrage
Business Broker
Cloud Auditor
Secure Auditing Environment
Security Audit
Privacy Impact Audit
Performance Audit
Cloud Carrier
Secure Transport Support
Cross Cutting Concerns: Security, Privacy, etc

Based on NIST SP 500-299 - NIST Cloud Computing Security Reference Architecture

SCCO –Risk Management Framework application for secure Cloud Computing



STEP 1:

- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION

STEP 2:

- IDENTIFY & SELECT CAPABILITIES
- SELECT BASELINE CONTROLS
- TAILOR & SUPPLEMENT CONTROLS
- IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
- SELECT CLOUD PROVIDER
- NEGOTIATE SLA, METRICS, SIGN CONTRACT
- DEVELOP SECURITY PLAN

STEP 3:

- IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT

STEP 4:

- ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
- ASSESS SECURITY CONTROLS MANAGED BY CONSUMER

STEP 5:

- AUTHORIZE CLOUD-BASED INFORMATION SYSTEM (BASED UPON RESIDUAL RISK & RISK TOLERANCE)

STEP 6:

- ONGOING MONITORING OF CONSUMER'S CONTROLS
- ONGOING MONITORING OF PROVIDER'S OPERATIONS
- RE-AUTHORIZE PROVIDER

Based on NIST SP 500-299 - NIST Cloud Computing Security Reference Architecture

SCCO - Cloud Computing Cybersecurity (C3) Impact Levels – C3IL

- C3 Impact Level **4** – Classified Information (not included in WIIP)
- C3 Impact Level **3** – Controlled Sensitive Official Information
- C3 Impact Level **2** – Controlled Official Information
- C3 Impact Level **1** – Non-Controlled Unclassified Information

WIIP

SCCO - Cloud Computing Cybersecurity (C3) Impact Levels – C3IL

- C3 Impact Level **1** – Non-Controlled Unclassified Information
  - Public Cloud processing allowed ✓
  - Includes all data approved for public access with a low level of confidentiality
  - Internet access to services allowed ✓
  - Includes public information that:
    - does not contain personal data subject to protection
    - is not a legally protected information
    - may have copyright-related restrictions
  - Consequences of disclosure:
    - no negative consequences of access by unauthorized persons or consequences in the form of legal effects related to copyright
  - Level 1 supports LOW level of confidentiality and a maximum of MODERATE integrity level SC = (L, M, x).

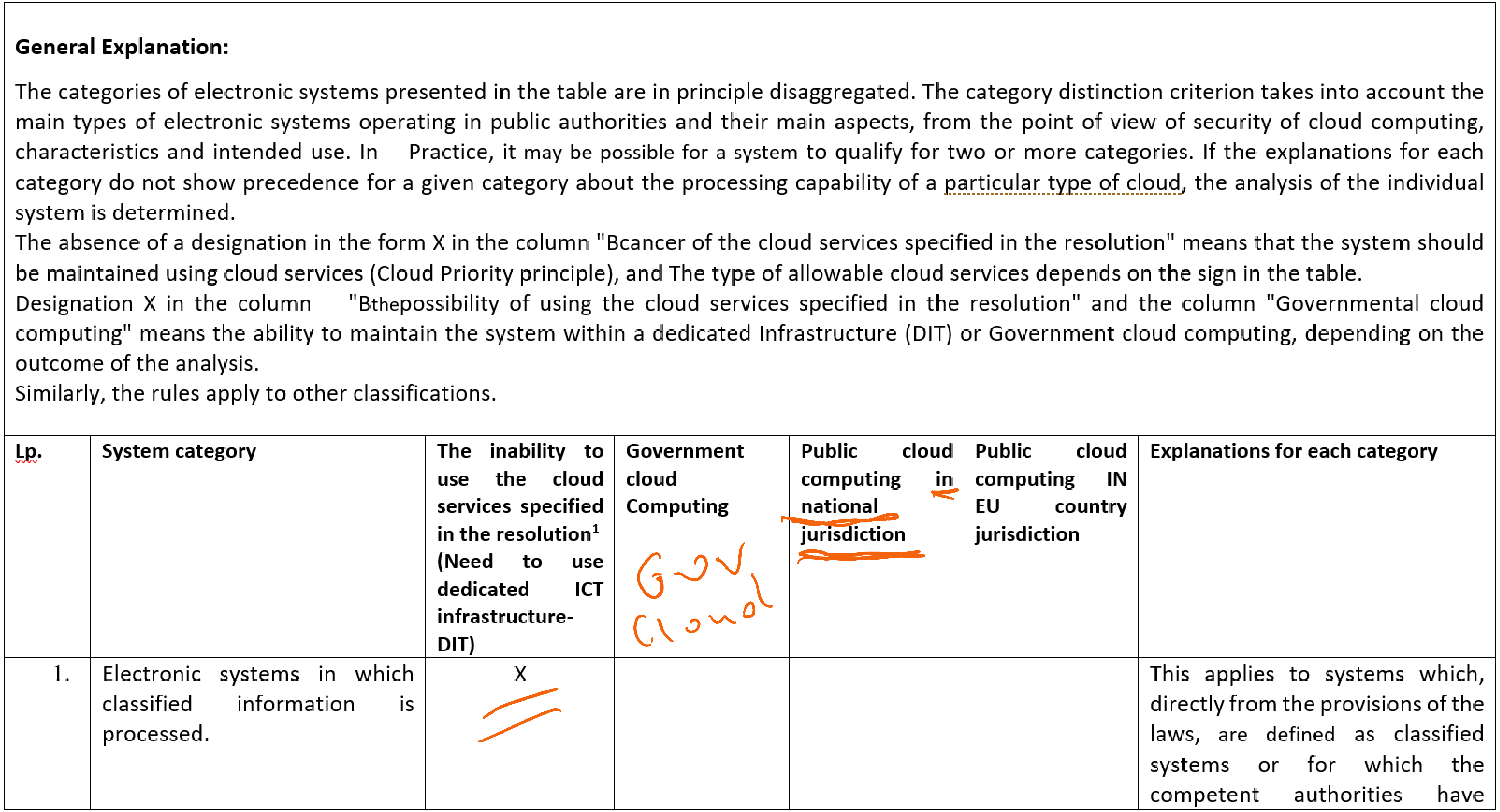
SCCO - Cloud Computing Cybersecurity (C3) Impact Levels – C3IL

- C3 Impact Level **2** – Controlled Official Information
  - Public Cloud within Polish jurisdiction
  - Data relevant to the statutory operation of a public administration, available without restriction to the staff of the institution or on the basis of confidentiality agreements
  - Level 2 includes public information that:
    - Contains personal data subject to statutory protection (GDPR)
    - Information containing the trader's secret, including trade secrets protected
  - Consequences of disclosing information:
    - The negative consequences of unauthorized access - breach of Data Protection Act; reach of the laws on the protection of trade secrets, the breach of the trade secret and, consequently, may trigger certain Statutory sanctions (e.g. article 23 of the Public Information Provision Act).
  - Level 2 supports information with MODERATE level of confidentiality and MODERATE integrity level SC = (M, M, H).

SCCO - Cloud Computing Cybersecurity (C3) Impact Levels – C3IL

- C3 Impact Level **3** – Controlled Sensitive Official Information
  - Government Cloud Only
  - Level 3 includes sensitive, legally protected information and referential national registries data – defined in dedicated legislation (incl. data critical to Public Safety)
  - Level 3 supports HIGH level of confidentiality and HIGH level of integrity information: SC = (H, H, H).

SCCO – Cloud model classification criteria (WIIP – Appendix 2)

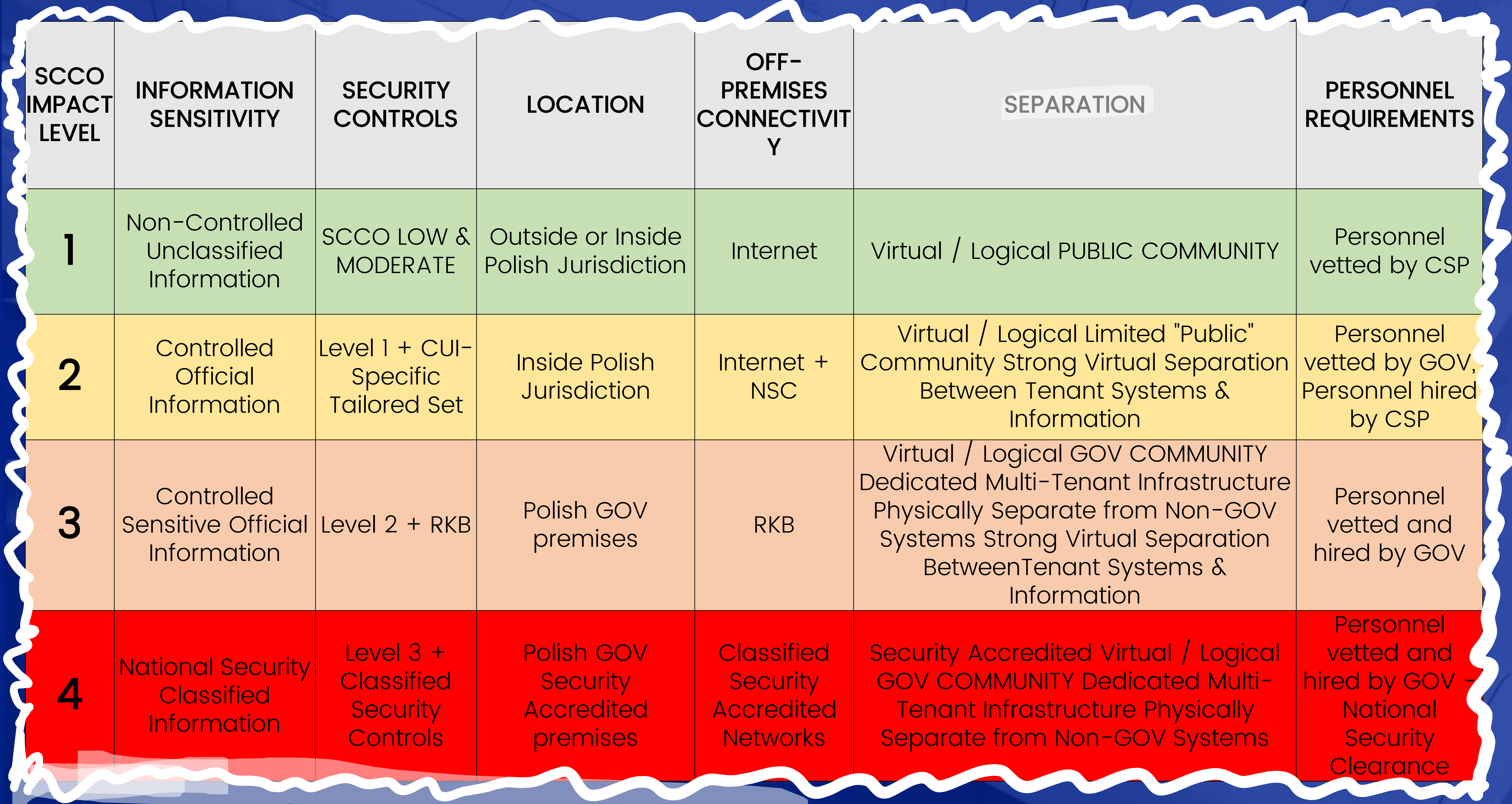


General Explanation:

The categories of electronic systems presented in the table are in principle disaggregated. The category distinction criterion takes into account the main types of electronic systems operating in public authorities and their main aspects, from the point of view of security of cloud computing, characteristics and intended use. In Practice, it may be possible for a system to qualify for two or more categories. If the explanations for each category do not show precedence for a given category about the processing capability of a particular type of cloud, the analysis of the individual system is determined.
The absence of a designation in the form X in the column "Bcancer of the cloud services specified in the resolution" means that the system should be maintained using cloud services (Cloud Priority principle), and The type of allowable cloud services depends on the sign in the table.
Designation X in the column "Bthepossibility of using the cloud services specified in the resolution" and the column "Governmental cloud computing" means the ability to maintain the system within a dedicated Infrastructure (DIT) or Government cloud computing, depending on the outcome of the analysis.
Similarly, the rules apply to other classifications.

Lp.	System category	The inability to use the cloud services specified in the resolution[1] (Need to use dedicated ICT infrastructure-DIT)	Government cloud Computing	Public cloud computing in national jurisdiction	Public cloud computing IN EU country jurisdiction	Explanations for each category
			Gov Cloud			
1.	Electronic systems in which classified information is processed.	X				This applies to systems which, directly from the provisions of the laws, are defined as classified systems or for which the competent authorities have

SCCO Impact Levels and Security Requirements



SCCO IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
1	Non-Controlled Unclassified Information	SCCO LOW & MODERATE	Outside or Inside Polish Jurisdiction	Internet	Virtual / Logical PUBLIC COMMUNITY	Personnel vetted by CSP
2	Controlled Official Information	Level 1 + CUI-Specific Tailored Set	Inside Polish Jurisdiction	Internet + NSC	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	Personnel vetted by GOV, Personnel hired by CSP
3	Controlled Sensitive Official Information	Level 2 + RKB	Polish GOV premises	RKB	Virtual / Logical GOV COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-GOV Systems Strong Virtual Separation BetweenTenant Systems & Information	Personnel vetted and hired by GOV
4	National Security Classified Information	Level 3 + Classified Security Controls	Polish GOV Security Accredited premises	Classified Security Accredited Networks	Security Accredited Virtual / Logical GOV COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-GOV Systems	Personnel vetted and hired by GOV - National Security Clearance

SCCO –Security Requirments for C3ILs

- Security Controls based on the **Low**, **Moderate**, and **High** baselines recommended in NIST SP 800-53(R5 Draft) catalog of security controls

POL / SCCO vs. US / Fed RAMP

- SCCO leverage the work done as part of the US FedRAMP assessment methodology, and adding specific security controls and requirements necessary to meet Public Sector and Critical Information Infrastructure requirements defined in the Polish legislation

Based on NIST SP 800-53

Thank you...

The Polish perspective on Cloud Computing Cybersecurity Requirements

and now Discussion in Panel...

ROBERT KOŚLA,

Director, Department of Cybersecurity
Ministry of Digital Affairs

E-mail: robert.kosla@mc.gov.pl
Office: sekretariat.dc@mc.gov.pl

Twitter: @RobertKosla

EXPERT PANEL DISCUSSION

Cyber security and certification – the CEE administration and business perspective

ROBERT TRĘTKOWSKI

Vice President of the Management Board of Krajowa Izba Rozliczeniowa

ROBERT KOŚLA

Moderator

SZYMON MITORAJ

Chief Information Officer, PZU S.A.

KAROL OKOŃSKI

Secretary of State,
Ministry of Digital Affairs, the Government Plenipotentiary for Cybersecurity

KRZYSZTOF SILICKI

Deputy Director for Cybersecurity and Innivations, NASK, ENISA vice chairman