CSA | EU Summit 2020

Cybersecurity Certification

Andreas Fuchsberger

WHY IS CERTIFICATION IMPORTANT?

Societies around the world are growing dependent on ICT for virtually all aspects of economic and social life

The cybersecurity market, one of the fastest growing markets in the ICT sector, yields huge economic opportunities. However, it is crucial to acknowledge that cybersecurity challenges are global, there is no “Europe versus the rest”

Certifications are an important mechanism for establishing trust in cybersecurity, and our products and services are compliant with numerous national and international frameworks

As a global company, Microsoft has a wider impact on the sector. We believe this gives us a larger responsibility in relation to the ICT sector.

CSA | EU Summit 2020

Best Practices

Microsoft's Perspective

Microsoft Cloud Compliance Certifications and Attestations

	Regulatory and Compliance Domain	Office 365	Microsoft Azure	Microsoft Dynamics CRM	Microsoft Intune
Broadly Applicable	ISO 27018:2014	✓	✓	✓	✓
	ISO 27001:2013	✓	✓	✓	✓
	SOC 1 Type 2 (SSAE 16/ISAE 3402)	✓	✓	✓	✓
	SOC 2 Type 2 (AT Section 101)	✓	✓	No	✓
	CSA STAR 1	✓	✓	✓	No
United States Government	FedRAMP Moderate	✓	✓	No	No
	CJIS Security Policy, Version 5.3	✓	✓	✓	No
	DISA SRG Level 2 P-ATO	✓	✓	No	No
	FDA 21 CFR Part 11	No	✓	No	No
	ITAR	✓	✓	No	No
	IRS 1075	✓	✓	No	No
Industry Specific	HIPAA BAA	✓	✓	✓	✓
	PCI DSS Level 1	N/A	✓	N/A	N/A
	FERPA	✓	✓	N/A	N/A
	CDSA	N/A	✓	N/A	N/A
Region/Country Specific	EU Model Clauses	✓	✓	✓	✓
	UK G-Cloud v6	✓	✓	✓	✓
	Australia Gov ASD	✓	✓	No	No
	Singapore MTCS	✓	✓	✓	No
	Japan FISC	✓	✓	No	No
	New Zealand GCIO	✓	✓	No	✓

MICROSOFT’S PERSPECTIVE ON EU CERTIFICATION

The EU Cybersecurity Act and Cybersecurity Certification Framework raises the bar for the whole industry and allows to concentrate efforts and resources in a centralized concept.

Mandatory framework, but voluntary certification schemes allows to ensure adaptability, boost innovation and support growth.

Security standardisation is no longer just a technical discussion but transcends multiple disciplines, from technology through policy experts and decision makers.

A MULTITUDE OF DIFFERENT OPERATORS

At the beginning of a certification something sets the rules. Many Standards Development Organisations (SDOs) involved in the setting thier rules

- ISO/IEC – International Organisation for Standardization/International Electrotechnical Commission
- CEN/CENELEC - European Committee for Standardization/European Committee for Electro-technical Standardization
- ETSI – European Telecommunications Standards Institute
- NIST - National Institute of Standards and Technology

And many more that do claim to be an SDO

- ENISA – European Cybersecurity Agency
- CSA – Cloud Security Alliance

MICROSOFT EXPERTISE IN THE EU CLOUD SERVICES CERTIFICATION SCHEME DEVELOPMENT

Through close collaboration with the Cloud Security Alliance, Microsoft expertise is being brought to the ENISA ad hoc working group on cloud services to create a new European certification for information and cyber security of cloud services.

The certification scheme comes under the EU Cybersecurity Act’s Certification Framework

- To increase the use of cybersecurity certification in Europe
- To go beyond national schemes and offer mutual recognition at a European level
- Enable customers to take informed decisions about cybersecurity
- Based on regulation 765/2008 and ISO/IEC 17065, and the existing accreditation network

3 KEYS TO THE CERTIFICATION SCOPE

Core decisions

Cloud computing

Definition based on ISO/IEC 17788

cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

cloud service: One or more capabilities offered via *cloud computing* invoked using a defined interface.

All cloud capabilities

Also based on ISO/IEC 17788

All cloud capabilities are supported: Infrastructure, Platform, Application

Preferred for clarity to references to IaaS, PaaS, SaaS, XXaaS

No mention of deployment model

Three assurance levels

As defined in the Cybersecurity Act

'basic' , 'substantial' and 'high'

All levels based on an assessment by an accredited third-party

UNDERSTANDING THE LEVELS

Gradual increase of assurance in scope, depth, and rigour

‘basic’

Demonstrates an intention from the CSP to implement security controls

Intended to resist simple known attacks

Document review is required

Entry level with limited guarantees, as a first step or for low-risk applications

‘substantial’

Demonstrates that the CSP has correctly implemented security controls

Intended to resist know attacks by actors with limited means

Functional testing is required

Core level with real guarantees, for mainstream applications in all fields

‘high’

Demonstrates the effectiveness of the CSP’s controls against attacks

Intended to resist complex attacks using state-of-the-art techniques

Penetration testing is required

Level with strong guarantees, for critical applications in sensitive fields

LOOKING FORWARD

Global or at least regional schemes ensure wide applicability and usefulness.

Once widely applicable schemes become established, anticipate vertical or industry specific certifications.

Anything from consumer IoT through industrial control systems to critical infrastructure.

Expect some of these may well become mandatory for regulated business or market access.

Microsoft

For more information on Microsoft and security certifications

www.microsoft.com/trust-center