

#### European DIGITAL SME Alliance

#### The SME Guide for the Implementation of ISO/IEC 27001

#### Fabio GUASCONI



# **Speaker introduction**

#### Fabio GUASCONI

- Chairman DIGITAL SME WG CYBER & DATA working group
- President UNINFO CT 510 ISO/IEC JTC 1 SC 27 mirror
- SBS expert
- $\circ~$  CLUSIT association board of directors
- Partner and co-founder @ Bl4ckswan S.r.l., SECMES S.r.l.





#### European DIGITAL SME Alliance

# **30 members**

Representing more than 20,000 digital SMEs across Europe

DIGITAL SME's members consists of national, supranational and regional associations and clusters.

## **DIGITAL SME – voice of the European SMEs**

DIGITAL SME works with its members and voices their priorities through its Working Groups:



## How Guide was created: DIGITAL SME and SBS



DIGITAL SME is a founding member of Small Business Standards (SBS)

SBS represents and defends SMEs' interests in the standardisation process at European and international levels.

SBS is one of the Annex III organisations of Regulation (EU) 1025/2012. As an Annex III organisation, SBS represents SMEs in European Standardisation Activities, including:

- Financing experts to represent SMEs in International and European Standardisation Organisations
- Implementing an annual Working Programme on standardisation in several sectors

DIGITAL SME leads SBS Sectoral Approach on ICT

As a part of its SBS activities, DIGITAL SME involved WG CYBER to the creation of *The SME Guide for the Implementation of ISO/IEC 27001* 

#### **SME Guide**

When it comes to information security management there is no need to reinvent the wheel, several international reference standards can be used, among which **ISO/IEC 27001** is, without doubt, the most solid and affirmed choice.

Unluckily SMEs in most cases don't:

- know that ISO/IEC 27001 exists
- want to buy the standard
- have the competence to understand and apply it

SBS and DIGITAL SME has then decided to **develop a guide dedicated to SMEs** for the implementation of information security management based on ISO/IEC 27001.



#### **SME Guide**

Step 1: Establish information security foundations	Step 2: Understand what must be protected	Step 3: Evaluate information security risks	Step 4: Design, apply and monitor information security controls
+			+
Step 1.1: Assign roles and responsibilities	Step 2.1 Identify what information is used	Step 3.1 Understand the value of assets	Step 4.1 Identify controls to be implemented and set up an Information Security Plan
•			
Step 1.2: (optional) Establish the Information Security Management System (ISMS)	Step 2.2 Identify which other assets are used	Step 3.2 Evaluate the type of context in which the organization works	Step 4.2 Manage the Information Security Plan
			+
	Step 2.3 Understand the connection between information and other assets	Step 3.3 Identify which controls are already in place	Step 4.3 Control information security
			Step 4.4 Monitor information security

#### **SME Guide**

The main principles that have been taken into account while developing the guide are to:

- a) describe an approach that can be used as a **first step and upgraded** towards a certification
- **b) remove the most "formal" parts** of an information security management system
- c) simplify technical terms used in international standards
- d) add tips and examples throughout the text
- e) provide a practical approach towards risk management
- f) provide sensitive sets of simplified information security controls

The guide is freely accessible at the SBS website: <u>http://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management</u>

## **Advantages of the Guide**

1) Dissemination of **high level information** concerning information security management in small businesses



Digital SMEs expressed a need for such simplified information on cybersecurity standards implementation through DIGITAL SME's position on The EU Cybersecurity Act and the role of standards for SMEs (outcomes of the SBS ICT Forum 2019)

- 2) Increased uptake of information security management concepts based on ISO/IEC 27001 by European SMEs
- 3) Publication of a **reference Guide** that will represent the port of call for SMEs willing sort out the wild ecosystem of Information Security Management

## **Success of the Guide**

In addition to its original **English** version, the Guide has been made available for SMEs in:

- Greek
- French
- Polish







ΟΔΗΓΟΣ ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ **ISO / IEC 27001** ΣΕ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΤΑΙΡΕΙΕΣ (**MME**) ΓΙΑ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ



# **FUTURE – our upcoming new guide for SMEs!**

#### **SME Guide on Information Security Controls**

- Complements the SME Guide for the Implementation of ISO/IEC 27001
- Complies with GDPR ISO/IEC 27701 (WG5)
- Design and operate controls (ISO/IEC 27002 WG4/5)
  - Incident Management
  - ICT Readiness for Business Continuity
  - Internet & Cyber security
  - Forensics
  - Network security
  - Identity & Access Control...
- Current state: Selecting most suitable controls for SMEs
- Prospect publication: Q3/2021



# Thank You



🖂 fabio.guasconi@bl4ckswan.com