



DSP



Technical Guidelines for the implementation of minimum security measures for Digital Service Providers

K



Contact

Acknowledgements

Legal notice

Copyright Notice

02

Table of Contents

Executive Summary	6
1. Introduction	7
1.1 Background	7
	m m
	m
	m m
	K m mm
2. List of security objectives and measures for DSPs	11
2.1 Description	11
2.2 The role of risk assessment	12
2.3 SO 01 - Information security policy	12
	m
	m m
	K
2.4 SO 02 – Risk Management	14
	m
	m m
	K
2.5 SO 03 – Security Roles	15
	m
	m m
	K
2.6 SO 04 – Third party management	17
	m
	m m
	K
2.7 SO 05 – Background checks	19
	m
	m m
	K
2.8 SO 06 – Security knowledge and training	20
	m
	m m
	K
2.9 SO 07 – Personnel changes	22
	m
	m m

K			
2.10 SO 08 – Physical and environmental security			23
m			
	m	m	
K			
2.11 SO 09 – Security of supporting utilities			26
m			
	m	m	
K			
2.12 SO 10 – Access control to network and information systems			27
m			
	m	m	
K			
2.13 SO 11 – Integrity of network components and information systems			29
m			
	m	m	
K			
2.14 SO 12 – Operating procedures			30
m			
	m	m	
K			
2.15 SO 13 – Change management			31
m			
	m	m	
K			
2.16 SO 14 – Asset management			32
m			
	m	m	
K			
2.17 SO 15 – Security incident detection & Response			34
m			
	m	m	
K			
2.18 SO 16 – Security incident reporting			36
m			
	m	m	
K			
2.19 SO 17 – Business continuity			37
m			
	m	m	
K			
2.20 SO 18 – Disaster recovery capabilities			39

m			
K		m	m
2.21 SO 19 – Monitoring and logging			40
m			
K		m	m
2.22 SO 20 – System tests			41
m			
K		m	m
2.23 SO 21 – Security assessments			43
m			
K		m	m
2.24 SO 22 – Compliance			44
m			
K		m	m
2.25 SO 23 – Security of data at rest			46
m			
K		m	m
2.26 SO 24 –Interface security			48
m			
K		m	m
2.27 SO 25 –Software security			50
m			
K		m	m
2.28 SO 26 – Interoperability and portability			51
m			
K		m	m
2.29 SO 27 – Customer Monitoring and log access			52
m			
K		m	m
3. Summary			54

1.1 Background

m m m m
 \square m m m m m m
 \square m m m m m m
 \square K m m m m m m

- An online marketplace allows consumers and/or traders to conclude online sales and service contracts with traders, and is the final destination for the conclusion of those contracts. It does not*

- **Online search engines:**

- **Cloud computing service providers:**

Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this report, "cloud computing services" means services that enable access to a scalable and elastic pool of shareable computing resources. The term "computing resources" covers resources such as networks, servers or other infrastructure, storage, applications and services. "Scalable" means that, in order to handle fluctuations in demand, computing resources are flexibly allocated by the cloud service provider irrespective of the geographical location of the resources.

m G m m

m m m m m m m m

m m mm m m m m m m m m m m

m m m m m m m m m m m m mm

m m m m m m m m m m m m m

m m m m m m m m m m m m m m

mm m m m m m m m m m m m m m m

m m m m m m m m m m m m m m

m m m m m m m m m m m m m m

1.1.4 Document overview

m m m m m m

m m m m m m

m m m m m m

1.1.5 Methodology

security measures security requirements, security objectives security measures

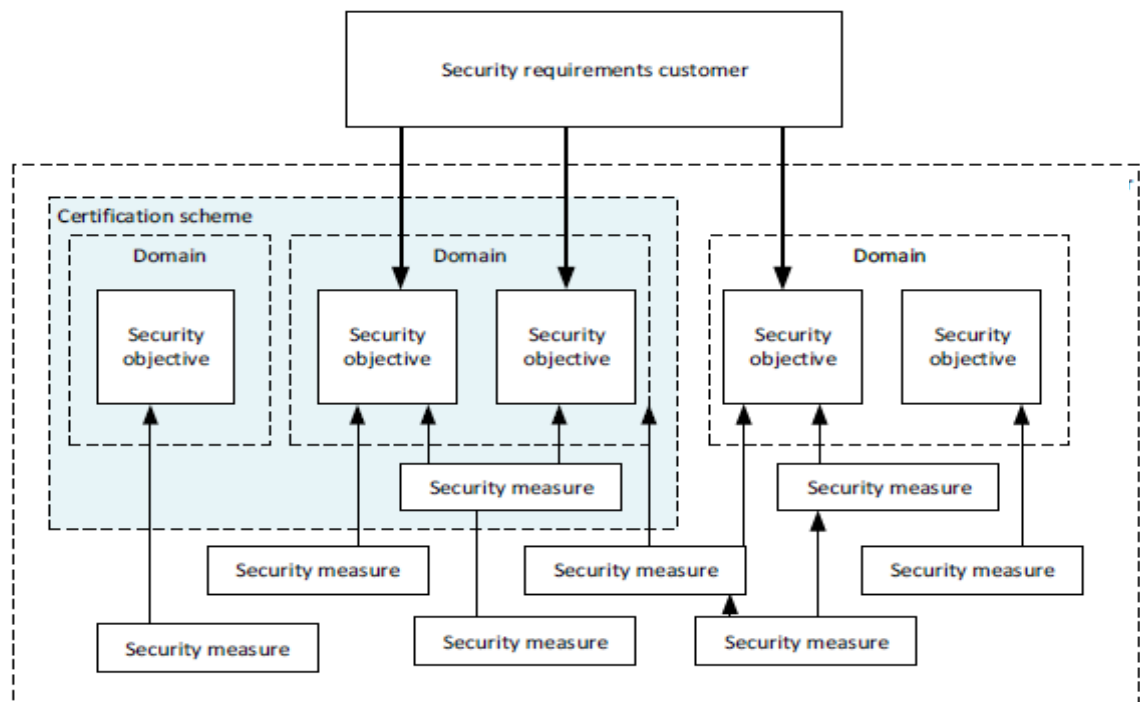


Figure 1: Terminology explained in a diagram extracted from "Cloud Certification Schemes Meta framework"

- **Security requirement:**

m G m m m m m

m m

- **Security objectives:**

m m m m m m m m m

m m m m m m m m m m

- **Security measures:**

m m m m m m

m m m m m m m m

- **ISO/IEC 27001:**

- **CSA CCM:** m m m K

- **BSI C5:** m m m m m m m m m m

- **COBIT5:** m m m m G

- **CCS CSC:** G m m m m

- **OCF:** K GG G K G

- **NIST:** m m G m G , m , m G

- **PCI DSS:** G G m m

- **CES:** m m m m

2.1 Description

G

[illegible]

Description

m m m m m m m

[illegible]

<u>ISO27001:</u>	G	m		m	K	K	K	K	K	K	K
K	K										
<u>CSA CCM:</u>	K	K	K	K	K	K	K	K	K	m	
K											
<u>BSI C5:</u>	G	G	G								
<u>CCS:</u>	m	m	K		K		m	m	m		
m	K		m	K		K				K	
<u>OCF:</u>	K	K	K	K	K	K	K	K	K	K	K
m		K									
<u>NIST:</u>	G		m	m	m	m					
<u>PCI-DSS:</u>		K		m			m	m	m	m	

[illegible][illegible]



Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m m • K m m 	<ul style="list-style-type: none"> • m m G m m m • mm m m m
	<ul style="list-style-type: none"> • m m m m • K m m m m 	<ul style="list-style-type: none"> • m m G m m m m • m m m m m m • m m m m m m
	<ul style="list-style-type: none"> • m m m • m m 	<ul style="list-style-type: none"> • m m m m m m • m m m m m m

ISO27001:

G m m

CSA CCM:

m G K GK GK GK GK
m K m m m m K
G m m K m m K G
K G K m m m

BSI C5:

G G G K

CCS:

K m m m m K

OCF:

m K m m G G G G G G m
m m m K G K K K K K K K
m K K m K K K K K K K
K K K m K K K K K K K
GK GK GK GK GK GK GK GK GK GK
G K m m m

NIST:

G K m m m m m m

PCI-DSS:

K m m m m

Description

m m m m m

m m m m m

m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> m m G m m m m m m 	<ul style="list-style-type: none"> m m m m G m m m m o m o o m m

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m • m m m m • m 	<ul style="list-style-type: none"> ○ m m ○ ○ m m ○ m m • G m G m m m m
	<ul style="list-style-type: none"> • m m m • m m m m • m m m m m • m m m m m • m m m m • K m 	<ul style="list-style-type: none"> • m m m m • m m m m • m m m m m • m m m m m • m m m m m • m m m m m • K m m m m m
	<ul style="list-style-type: none"> • m mm • m m m m • m m m m m 	<ul style="list-style-type: none"> • m mm • m m m m • m m m m • G m m m m m ○ G m m m m m ○ G m m m m m ○ G m m m m m

Mapping

2.7 SO 05 – Background checks

Description

m

m

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m • G m m m 	<ul style="list-style-type: none"> • m m m

Mapping

ISO27001:	m m m m
CSA CCM:	K m
BSI C5:	
CCS:	m K K m
OCF:	m
NIST:	G m m m m
PCI-DSS:	K m m m m

2.8 SO 06 – Security knowledge and training

Description

m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m • m • m 	<ul style="list-style-type: none"> • m m m • m
	<ul style="list-style-type: none"> • G m m m 	<ul style="list-style-type: none"> • m m m

Mapping

ISO27001:															
CSA CCM:															
BSI C5:															
COBIT5:															
CCS:															
OCF:															
NIST:															
PCI-DSS:															

2.9 SO 07 – Personnel changes

Description

m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m
	<ul style="list-style-type: none"> G m m m m m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m m m m m m m m m m m m

Mapping

2.10 SO 08 – Physical and environmental security

Description

Security measures within sophistication levels

Description

m m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	m m	m m m
	• G m m m m • G m m m	• m m m m m m • m m m m m mm m m m m m m
	• m m • m m	mm m m m m m m m m m m m m mm

Mapping

CF:

	K			m			G	G	G	G	G	G	G		m
	G	m			K										
				m	G	G	G	G	G	G	G	G	G	G	G
G	G	G				m									

Description

$$\begin{array}{ccccccc} & & m & m & & m & m \\ m & m & G & m & m & m & m \end{array}$$

Security measures within sophistication levels

Mapping

m m m m m

2.13 SO 11 – Integrity of network components and information systems

Description

m m m m m m m m

m m m m m m m m

Security measures within sophistication levels

[illegible]

Mapping

ISO27001:																			
BSI C5:																			
CCS:																			
OCF:																			
NIST:																			
PCI-DSS:																			

2.14 SO 12 – Operating procedures

Description

m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m	m
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	m m m m m m	m m m m m m m m m m m m
	G m m m m m	m m m m m m m m m m m m m m

LEVEL	SECURITY MEASURES	EXAMPLES
	m m m m	m m m m
	m m m m	m m m m
	m m m m	m m m m

Mapping

ISO27001: G G

CCS: m K K m K

BSI C5 K K GK G G
G K K K K

OCF:

K m m m m
m K G G G G G G G m m m
K K K K K K K K K K K
m K G G G G G G G G G G G
G G G G m

2.15 SO 13 – Change management

Description

m m m m m m m m

m m m m m m mm m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m • G m m m 	<ul style="list-style-type: none"> • m m m m • m m m m
	<ul style="list-style-type: none"> • G m m m 	<ul style="list-style-type: none"> • m m m m m m m m

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> m m m m m m m m m m m 	<ul style="list-style-type: none"> m m
	<ul style="list-style-type: none"> m m m m 	<ul style="list-style-type: none"> m m m m

Mapping

[illegible]

2.16 SO 14 – Asset management

Description

m m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m m m m • K m m m m 	<ul style="list-style-type: none"> • m m m m ○ m m m ○ m m ○ m m m m m m • m
G	m m m m m m m	<ul style="list-style-type: none"> • m m m m m m m m m m • m m m m m m m m m m • m m m m m m m m m m
	<ul style="list-style-type: none"> • m m m m m m m m m m • m m m m m m m m m m • m m m m m m m m m m 	<ul style="list-style-type: none"> • m m m m m m m m m m • m m m m m m m m m m • m m m m m m m m m m

ISO27001:	G	G				G	G					G	G
	G	G											
CSA CCM:		G											m
BSI C5:	K		K		K		K		K		K		K
COBIT 5:	G		G		G		G		G		G		
CCS:			m	K			m	m				K	
						m			m	K			m m m
OCF:	G		G		G		G		G			G m	m
													K
	G	G	G	G	G	G	G	G	G	G	G	G	m
	m												G
													G
NIST:				m			m	m	m			m	m
PCI-DSS:			K		m				m	m		m	m

Description

m m m m m m m m m

m m m m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m • K m m 	<ul style="list-style-type: none"> • m m m • m m m m • G m m m
	<ul style="list-style-type: none"> • G m m 	<ul style="list-style-type: none"> • G m K GK mm G m

[illegible]

Description

m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<p>m m m m</p> <p>m m</p> <p>m m m</p>	<ul style="list-style-type: none"> m m m m o m m m m m m m o m m m m m m o m m m m o m m m
	<p>G m m m</p> <p>m m m</p>	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m

Mapping

2.19 SO 17 – Business continuity

Description

m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<p>G m m m m m</p>	<ul style="list-style-type: none"> m m m m K m m
	<ul style="list-style-type: none"> G m m K m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m m m m m m m m m
	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m

[illegible]

Description

Security measures within sophistication levels¹¹

LEVEL	SECURITY MEASURES	EXAMPLES
	<p>m m m m m m m</p>	<p>K m m m m m m m</p>
	<ul style="list-style-type: none"> G m m m m m G m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m G m m m m m m

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m

Mapping

ISO27001:	G G
CSA CCM:	m m m m
BSI C5:	K K
COBIT 5:	
CCS:	m m G m K
OCF:	K K m K K K K K K K K
NIST:	G m m
PCI-DSS:	K m m m m

2.21 SO 19 – Monitoring and logging

Description

m m m m m m m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	G m m m m	m m m m m m m m

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> G m m m m m m m mm m m m mm m m m m 	<ul style="list-style-type: none"> m m m o m m m m m o m m m o m o m m m m m m m m m m m m m m m m m mm m m m m m m m m m m m m
	<ul style="list-style-type: none"> mm m m m m m m m m m m m m 	<ul style="list-style-type: none"> mm m m m m m m m m m m m m m m

Mapping

ISO27001:	G G
CSA CCM:	K G G m m G m m
BSI C5:	
CCS:	m K
OCF:	G G G G G G G G G G G G G
G	m
NIST:	K m m m m
PCI-DSS:	m G m m m

2.22 SO 20 – System tests

Description

m m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m m m • m m m m 	<ul style="list-style-type: none"> • m m m m m m m • m m m
	<ul style="list-style-type: none"> • G m m m • G nm m m • m m m m m 	<ul style="list-style-type: none"> • m m m m m m • m m m m m • m m m m m m m • m m m m m m m
	<ul style="list-style-type: none"> • m m m m m • m m m m m • m m m m m 	<ul style="list-style-type: none"> • m m m m m m m • m m m m m m m

Mapping

2.23 SO 21 – Security assessments

Description

m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> m m m m m m m 	<ul style="list-style-type: none"> m m m m
	<ul style="list-style-type: none"> G m m m m m m m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m

Mapping

2.24 SO 22 – Compliance

Description

m
 m
 m
 m
 m
 m
 m

Security measures within sophistication levels

Mapping

[illegible]

2.25 SO 23 – Security of data at rest

Description

m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> G m m m m m m m m m m m m G m m m m m m m m m m m m m m m m m m G m m m G m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m
	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m

m m m m m m m m m m m m

ISO27001:

G G
G G

G G

CSA CCM:

G G G G G G G

BSI CS5:

K K K G K K

COBIT 5:

G G

CCS:

m m m m m m m K m

m m m

OCF:

G G G G m G

m

m K m

m m m m K

G m m K

K K K K m K K K K

K K K K K K K K K K K K K K K

GK GK GK GK GK GK GK GK GK GK GK GK GK GK GK

GK G K G G G G G G G G G G G G

G G G G G m G G G G G G G G

m m

K m

NIST:

G m m m m m m m m mm

m m m m G m mm

m

PCI-DSS:

K m m m m m

Description

A diagram illustrating a sequence of points on a horizontal line. Above the line, there are four 'm' characters. Below the line, there are several 'm' characters and some 'mm' characters. The points are distributed along the line, with some appearing in pairs above and below the line.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m m • K m m m • m m • m 	<ul style="list-style-type: none"> • m m m m • m m m m • m m m m • m m • m m
	<ul style="list-style-type: none"> • m m m m m m m • K m m m m m • m m m m • G m m 	<ul style="list-style-type: none"> • m m m m m m • m m m m m m • m m m m m m
	<ul style="list-style-type: none"> • m m m m m m • m m m m 	<ul style="list-style-type: none"> • m m m m m m • m m m m m m • m m m m m m

CSA CCM: G G G G m G

BSI C5: G G ~~G~~ ~~G~~ ~~G~~ ~~G~~ ~~G~~ ~~G~~
G K

CCS: m m m m

OCF: G G G G m G K K K K K K K
m K K K m K K K K K K K
K K K m K GK GK GK GK GK GK
GK GK GK GK GK GK GK G G G G G G
G G G G G G G G G G G
m G G G G G G m m m m

PCI-DSS: m m m m m m m

Description

m m m

LEVEL	SECURITY MEASURES	EXAMPLES
	<p>• Physical Security</p> <ul style="list-style-type: none"> • Access Control • Surveillance • Physical Barriers • Environmental Controls 	<p>• Physical Security</p> <ul style="list-style-type: none"> • Access Control • Surveillance • Physical Barriers • Environmental Controls
	<p>• Network Security</p> <ul style="list-style-type: none"> • Encryption • Firewalls • Intrusion Detection • Secure Protocols 	<p>• Network Security</p> <ul style="list-style-type: none"> • Encryption • Firewalls • Intrusion Detection • Secure Protocols

G m m m m m m m m

m m m K m

Mapping

2.28 SO 26 – Interoperability and portability

Description

m m m m m

m m mm m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	G m m m m	<ul style="list-style-type: none"> m K K m m m m m m m m m m m m
	G m m m m	<ul style="list-style-type: none"> m K K m m m m m m m m m m m G m m m m
	<ul style="list-style-type: none"> m m m m m m m m 	<ul style="list-style-type: none"> m m m m m m m m m m m m m m

Mapping

CSA CCM:	G	G	G	G	G	G	m	m
BSI C5:	G	G	G	G	G			
CCS:		m	K	m	m		K	m m
OCF:	G	G	G	G	G	G	m	m

2.29 SO 27 – Customer Monitoring and log access

Description

m m m m m m m m m

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
	<ul style="list-style-type: none"> • m m m • G m m m m 	<ul style="list-style-type: none"> • m m m m m m
	<ul style="list-style-type: none"> • G m m m m m m • m m m m m m m • m m m m m m m 	<ul style="list-style-type: none"> • m m m m m m m • m m m m m m m • m m m m m m m
	<ul style="list-style-type: none"> • m m m m m m m • m m m m m m m 	<ul style="list-style-type: none"> • m m m m m m m • m m m m m m m

Mapping

3. Summary

The diagram illustrates a sequence of 100 points in a 2D plane. The points are labeled 'm' and 'G'. The 'm' points are distributed across the plane, while the 'G' points are scattered. The points are connected by lines, forming a network structure. The diagram is a visualization of a sequence of points and their connections, likely representing a data set or a network.

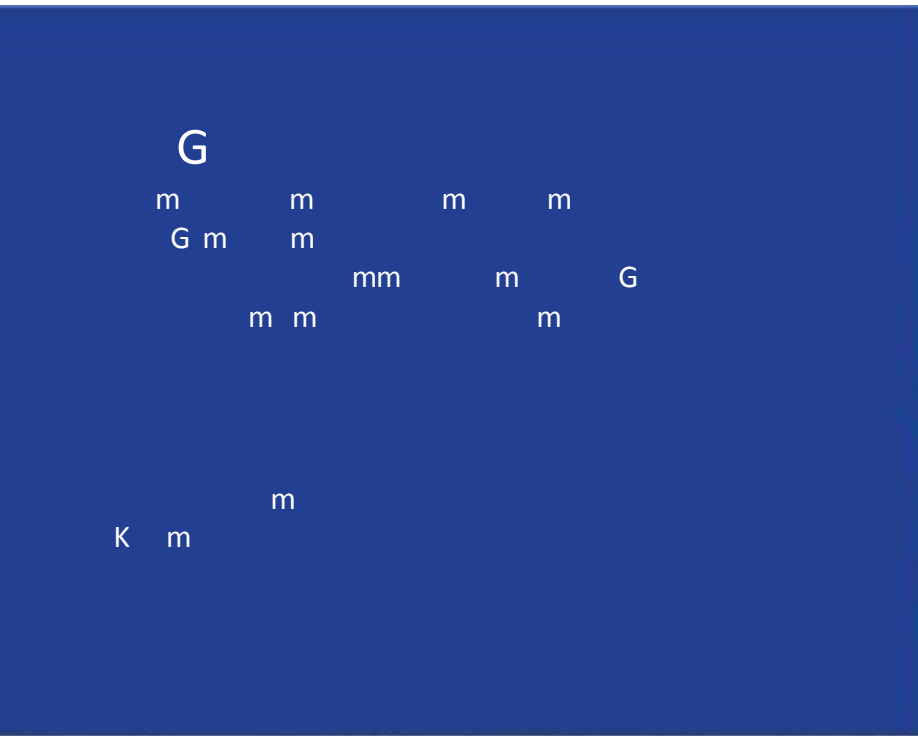
SECURITY OBJECTIVES	CLOUD PROVID-ERS	ONLINE MARKET PLACES	ONLINE SEARCH EN-GINES
G m m m	✓	✓	✓
K	✓	✓	✓
m	✓	✓	✓
	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
m m	✓	✓	✓
m m m m m m	✓	✓	✓
G m m m m m m	✓	✓	✓
m	✓	✓	✓
	✓	✓	✓
	✓	✓	✓
m m	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
K m m m	✓	✓	✓
	✓	✓	✓

	✓	✓	✓
m	✓	✓	✓
m	✓	✓	✓
G	✓	✓	✓
m	✓	✓	✓
G m m	✓	✓	✗
m K m m m	✓	✗	✗

$$\begin{array}{ccccccc} & & m & & m & & G \\ m & m & m & m & m & & m \end{array}$$

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES ¹⁷
G m m m	●	●	●		●	●	●	●	
	●	●	●		●	●	●	●	
m	●	●	●		●	●	●	●	
m	●	●	●		●	●	●	●	
m	●	●	●		●	●	●	●	
m	●	●	●	●	●	●	●	●	
m	●	●	●		●	●	●	●	
m m	●	●	●		●	●	●	●	
m m m m	●	●	●	●	●	●	●	●	●
G m m m	●		●		●	●	●	●	●
m	●				●	●			●
	●	●	●	●	●	●	●	●	●
	●	●	●	●	●	●	●	●	●
m m	●	●	●	●	●	●	●	●	
m	●	●	●	●	●	●	●	●	
m	●	●	●		●	●	●	●	

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES ¹⁷
m	•	•	•	•	•	•	•	•	
K m m m	•	•	•		•	•	•	•	•
m	•		•		•	•	•	•	•
	•	•	•		•	•		•	•
m	•	•	•		•	•			
m	•	•	•	•	•	•	•	•	•
G		•	•		•	•		•	•
m		•	•		•	•	•	•	
G m		•	•		•	•			
m									
m m m m	•	•	•	•	•	•	•	•	•



m m
m m
www.enisa.europa.eu

G
G

