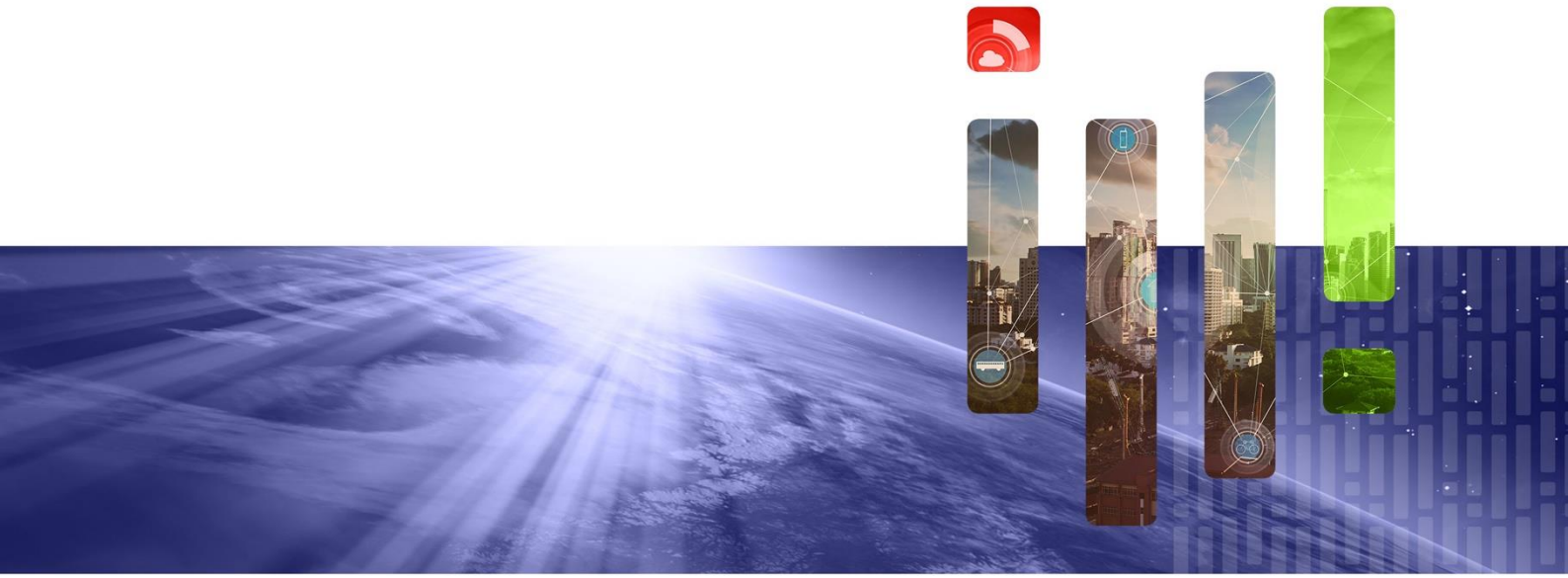
Statement of Applicability

REFERENCE	ISO27001:2022
DOC NUMBER	01-IMS-011
VERSION	v3.0
DATE	05 April 2024
STATUS	Approved
APPROVED BY	Teresa Cheung
AUTHOR	Teresa Cheung
CLASSIFICATION	Public



Distribution	
Name	**Organisation**
All Staff	Resillion
Customers and Partners	Any

Revision Record				
Date	**Version**	**Amendment**	**Author**	**Review**
2023-05-04	0.1	First Draft	Teresa Cheung	-
2023-06-23	0.2	Changed A.8.30 for Cyber UK to "Yes" to align with the previous SOA	Teresa Cheung	-
2023-06-28	0.3	Review with no comment	-	Dan Martland
2023-06-29	0.4	Review and comment	-	Edd Jones
2023-06-29	1.0	Approve	-	Teresa Cheung
2023-09-27	2.0	Rebrand to Resillion template, and updated applicability for A.8.4, A.8.26, A.8.31	Teresa Cheung	Boglarka Ronto, Dan Martland
2024-01-19	2.1	Review applicability for scripting and development	Teresa Cheung	Boglarka Ronto, Dan Martland
2024-04-05	3.0	Updated applicability for SZ regarding scripting and development; DLP not supported in US. Footnotes are inserted.	Teresa Cheung	Fan Zhang

resillion

Statement of Applicability – ISO27001:2022

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.5 Organizational Controls											
A.5.1	Policies for information security	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.2	Information security roles and responsibilities	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.3	Segregation of duties	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.4	Management responsibilities	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.5	Contact with authorities	Yes, all sites	Best practice, Legal / regulatory requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.6	Contact with special interest groups	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.7	Threat intelligence	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.8	Information security in project management	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.9	Inventory of information and	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
	other associated assets										
A.5.10	Acceptable use of information and other associated assets	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.11	Return of assets	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.12	Classification of information	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.13	Labelling of information	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.14	Information transfer	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.15	Access control	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.16	Identity management	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.17	Authentication information	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.18	Access rights	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.19	Information security in supplier relationships	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.20	Addressing information security	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
	within supplier agreements										
A.5.21	Managing information security in the ICT supply chain	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.22	Monitoring, review, and change management of supplier services	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.23	Information security for use of cloud services	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.24	Information security incident management planning and preparation	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.25	Assessment and decision on information security events	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.5.26	Response to information security incidents	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.27	Learning from information security incidents	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.28	Collection of evidence	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.29	Information security during disruption	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.30	ICT readiness for business continuity	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.31	Legal, statutory, regulatory, and contractual requirements	Yes, all sites	Best practice, Legal / regulatory requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.32	Intellectual property rights	Yes, all sites	Best practice, Legal / regulatory requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.33	Protection of records	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.5.34	Privacy and protection of PII	Yes, all sites	Legal / regulatory requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.35	Independent review of information security	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.36	Compliance with policies, rules, and standards for information security	Yes, all sites	Risk analysis, Legal / regulatory requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.5.37	Documented operating procedures	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6 People Controls											
A.6.1	Screening	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6.2	Terms and conditions of employment	Yes, all sites	Risk analysis, Legal / regulatory requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6.3	Information security awareness, education, and training	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6.4	Disciplinary process	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.6.5	Responsibilities after termination or change of employment	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6.6	Confidentiality or non-disclosure agreements	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6.7	Remote working	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.6.8	Information security event reporting	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7 Physical Controls											
A.7.1	Physical security perimeter	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.2	Physical entry	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.3	Securing offices, rooms, and facilities	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.4	Physical security monitoring	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.5	Protecting against external and environmental threats	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.7.6	Working in secure areas	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.7	Clear desk and clear screen	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.8	Equipment siting and protection	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.9	Security of assets off-premises	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.10	Storage media	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.11	Supporting utilities	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.12	Cabling security	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.13	Equipment maintenance	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.7.14	Secure disposal or re-use of equipment	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8 Technological Controls											
A.8.1	User endpoint devices	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.2	Privileged access rights	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.3	Information access restriction	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.8.4	Access to source code	Product Development and Scripting	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No[1]
A.8.5	Secure authentication	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.6	Capacity management	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.7	Protection against malware	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.8	Management of technical vulnerabilities	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.9	Configuration management	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.10	Information deletion	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.11	Data masking[2]	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.12	Data leakage prevention	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	No[3]	Yes	Yes
A.8.13	Information backup	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] China only have access to test case scripts for executing testing services for customers.
[2] Data masking is rarely needed in our operations but the capability is supported by our cyber experts.
[3] DLP is not yet supported for US but it is planned.

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
A.8.14	Redundancy of information processing facilities	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.15	Logging	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.16	Monitoring activities	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.17	Clock synchronisation	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.18	Use of privileged utility programs	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.19	Installation of software on operational systems	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.20	Networks security	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.21	Security of network services	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.22	Segregation in networks	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.23	Web filtering	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.24	Use of cryptography	Yes, all sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.25	Secure development life cycle	Product Development Only	Risk analysis Applicable to sites that	Yes	No	Yes	Yes	No	Yes	No	No

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
			manage product development								
A.8.26	Application security requirements	Yes, all sites	Best practice Applicable to development and acquisition of applications[4]	Yes	Yes*	Yes	Yes	Yes*	Yes	Yes*	No
A.8.27	Secure system architecture and engineering principles	Teams with engineering activities	Risk analysis Applicable to engineering activities	Yes	Yes	Yes	Yes	No	Yes	No	No
A.8.28	Secure coding	Product Development and Scripting	Risk analysis Applicable to all scripting activities	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
A.8.29	Security testing in development and acceptance	Product Development Only	Risk analysis Applicable to products developed for customers	Yes	No	Yes	Yes	No	Yes	No	No
A.8.30	Outsourced development	Yes, all sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

[4] *Commissum, NL and GTC do not develop applications on their own, and therefore only acquisition of applications applies to these sites.

ANNEX	TOPIC	SCOPE	JUSTIFICATION	EDGE	COMMISSUM	BRISTOL	BELGIUM	NL	US	GTC	CHINA
			Applicable to applications developed for internal use and for customers								
A.8.31	Separation of development, test, and production environments	Teams with engineering activities	Risk analysis Applicable to engineering activities	Yes	Yes	Yes	Yes	Yes	Yes	No	No
A.8.32	Change management	All sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.33	Test information	All sites	Risk analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
A.8.34	Protection of information systems during audit testing	All sites	Best practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes