Certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

Certificate Holder:

Lufthansa Technik AG
Weg beim Jäger 193
22335 Hamburg
Germany

including the locations according to annex

Scope:

Engineering services and AVIATAR solutions, design of changes and repairs, design and production and installation of aircraft components, management of continuing airworthiness of commercial, governmental and special aircraft operators, integrated logistic services for technical goods and spare parts, maintenance training and examination organization, consulting in lean management and process optimization and central functions.

SoA V2.2 from 21.11.2025

Proof has been furnished by means of an audit that the requirements of ISO/IEC 27001:2022 are met.

Validity:

The certificate is valid from 2026-04-30 until 2029-04-29.
First certification 2020

2026-04-23

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Precisely Right.

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

No.	Location	Scope
/01	c/o Lufthansa Technik AG Weg beim Jäger 193 22335 Hamburg Germany	Maintenance of Engines of commercial operators and central functions. SoA V2.2: 21.11.2025
/02	c/o Lufthansa Technik AG Airportring 60549 Frankfurt am Main Germany	Engineering services and AVIATAR solutions, design of changes and repairs, design and production and installation of aircraft components, maintenance of aircraft, engines and aircraft components, management of continuing airworthiness of commercial, governmental and special aircraft operators, integrated logistic services for technical goods and spare parts, maintenance training and examination organization, consulting in lean management and process optimization and central functions. SoA 2.2: 21.11.202 5
/04	c/o Lufthansa Technik AERO Alzey GmbH Rudolf-Diesel-Str. 10 55232 Alzey Germany	Maintenance of Engines of commercial operators and central functions. SoA 2.2: 21.11.2025
/05	c/o Lufthansa Technik Sofia Airport Complex - Terminal 1, Block 3 1540 Sofia Bulgaria	Maintenance of aircraft of commercial operators and central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/06	c/o Lufthansa Technik Malta Building No.1 (Hangar 1&2&3 Workshops and administrative area) Hal-Farrug Road Luqa LQA 3079 Luqa Malta	Maintenance of aircraft of commercial operators and central functions. SoA 2.2: 21.11.2025
/07	c/o Lufthansa Technik Milan Fabbricato 181, Terminal 1 Milan Malpensa Airport 21019 Somma Lombardo VA Italy	Maintenance of aircraft of commercial operators and central functions. SoA 2.2: 21.11.2025
/08	c/o Lufthansa Technik Budapest Budapest Ferenc Liszt International Airport 1675 Budapest Hungary	Maintenance of aircraft of commercial operators and central functions. SoA 2.2: 21.11.2025
/09	c/o Lufthansa Technik Puerto Rico LLC PO Box 797 102 San Antonio Road 604 Aguadilla Puerto Rico	Maintenance of aircraft of commercial operators and central functions. SoA 2.2: 21.11.2025
/10	c/o Lufthansa Technik Landing Gear Services UK Unit 3 Dawley Park, Kestrel Way, Hayes Middlesex UB3 1HP United Kingdom	Maintenance of aircraft components of commercial operators and central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/11	c/o Lufthansa Technik Shenzhen Co. Ltd. Unified Social Credit Code: 91440300723043020B Shenzhen Bao'an Intl. Airport Shenzhen 518128 Guangdong P.R. China	Maintenance of engines and aircraft components of commercial operators and central functions. SoA 2.2: 21.11.2025
/15	c/o Lufthansa Technik AG Raunheim Am Messeplatz 1 65479 Raunheim Germany	Engineering services of commercial operators and AVIATAR solutions. SoA 2.2: 21.11.2025
/16	c/o Lufthansa Technik Mobile Engine Services Unit 1, Esprit Logistics Park Co Kildare W23 XNP4 Ireland	Maintenance of engines of commercial operators and central functions. SoA 2.2: 21.11.2025
/18	c/o Lufthansa Technik AG Carrer de Marià Cuber 17 46011 Valencia Spain	Engineering services of commercial operators and AVIATAR solutions. SoA 2.2: 21.11.2025
/19	c/o Lufthansa Technik Middle East 1-5 Warehouse 293511 Dubai World Central United Arab Emirates	Maintenance of aircraft components of commercial operators and central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/20	c/o Lufthansa Technik Services India Private RMZ Galleria Office Tower, 13th floor Karnataka 560064 India	Maintenance of aircraft components of commercial operators and central functions. SoA 2.2: 21.11.2025
/21	c/o Lufthansa Technik North America Holding Corp. 3515 N Sheridan Rd Tulsa 74115 USA	Central functions. SoA 2.2: 21.11.2025
/22	c/o LH Technik Component Services LLC 256 W Ivy Ave Inglewood CA 90302 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/23	c/o Lufthansa Technik LTTS Shannon World Aviation Park Shannon, County Clare V14EE03 Ireland	Maintenance of engines of commercial aircraft operators and central functions. SoA 2.2: 21.11.2025
/24	c/o Lufthansa Technik Montreal (YUL) 800 Chemin St-Francois Dorval Montreal H9P 2P6 Canada	Maintenance engines of commercial aircraft operators and central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/25	c/o Lufthansa Technik Logistik Services GmbH Lufthansa Basis Tor 23 Geb. 401 60549 Frankfurt Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/26	c/o Lufthansa Technik Logistik Services GmbH Technische Basis Geb. 983 1300 Wien Austria	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/27	c/o Lufthansa Technik Logistik Services GmbH Wartungsallee 1 85356 München-Flughafen Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/28	c/o Lufthansa Technik Logistik Services GmbH Heinrich-Steinmann-Straße 51147 Köln Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/29	c/o IDAir GmbH Weg beim Jäger 193 22335 Hamburg Germany	Maintenance of commercial, governmental and special aircraft operators and central functions. SoA 2.2: 21.11.2025
/30	c/o Lufthansa Technical Training GmbH Wartungsallee 1 85356 München-Flughafen Germany	Maintenance training and examination organization. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/31	c/o Lufthansa Technical Training Villamor Air Base Pasay City 1309 Philippines	Maintenance training and examination organisation and central functions. SoA 2.2: 21.11.2025
/32	c/o Lufthansa Technical Training GmbH Unterschweinstiege 12 60549 Frankfurt am Main Germany	Maintenance training and examination organization. SoA 2.2: 21.11.2025
/33	c/o Lufthansa Technik Component Services Asia Pacific 35 F Connaught Road West Sheung Wan Hong Kong	Maintenance of aircraft components of commercial, aircraft operators and central functions. SoA 2.2: 21.11.2025
/34	c/o Lufthansa Technik Intercoat GmbH Kisdorfer Weg 36-38 24568 Kaltenkirchen Germany	Maintenance of aircraft components of commercial, aircraft operators and central functions. SoA 2.2: 21.11.2025
/35	c/o Lufthansa Technik North America Holding Corp. USA Miami 5875 NW 163rd St Miami Lakes FL 33014-5618 USA	Central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/36	c/o LH Technik Component Services LLC 6501 E Apache St Tulsa OK 74115-3640 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/37	c/o LH Technik Component Services LLC 1640 HEMPSTEAD BETHPAGE Turnpike New York NY 11554 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/38	c/o LH Technik Component Services LLC 23 Cargo Building New York NY 11430 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/39	c/o LH Technik Component Services LLC 2600 SW 36th St Fort Lauderdale FL 33312-5037 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/40	c/o LH Technik Component Services LLC 5875 NW 163rd St Miami Lakes FL 33014-5618 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/41	c/o LH Technik Component Services LLC Avenida Ejercito Nacional Mexicano 418 11560 Mexico Mexico	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/42	c/o LH Technik Component Services LLC 6838 S 220th St. Kent WA 98032 USA	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/43	c/o Lufthansa Technik AG Sofia (AES) SOF Sofia Airport, Hangar 2 1540 Sofia Bulgaria	Engineering services. SoA 2.2: 21.11.2025
/44	c/o Lufthansa Technik Engine Services 3515 North Sheridan Road Tulsa 74115 USA	Maintenance of engines of commercial aircraft operators. SoA 2.2: 21.11.2025
/45	c/o Lufthansa Technik EME Aero Sp. z o.o. ul. Jasionka 949 36-002 Trzebownisko-Jasionka Poland	Maintenance of engines of commercial aircraft operators and central functions. SoA 2.2: 21.11.2025
/46	c/o Lufthansa Technik Logistik Services GmbH, Hamburg Weg beim Jäger 193 22335 Hamburg Germany	Logistic services for technical goods and spare parts and central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/47	c/o Lufthansa Technik Logistik Services GmbH, Hamburg Heselstücken 9 22453 Hamburg Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/48	c/o Lufthansa Technik Logistik Services GmbH Hamburg Lautenschlagerstr. 2 70173 Stuttgart Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/49	c/o Lufthansa Technik Logistik Services GmbH Hamburg Wanheimer Str. 61 40472 Düsseldorf Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/50	c/o Lufthansa Technik Logistik Services GmbH Hamburg Elly-Beinhorn-Ring 4 12529 Schönefeld Germany	Logistic services for technical goods and spare parts. SoA 2.2: 21.11.2025
/51	c/o Avionic Design GmbH Hamburg Wragekamp 10 22397 Hamburg Germany	Design and production of aircraft components. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/52	c/o Lufthansa Technical Training GmbH Weg beim Jäger 193 22335 Hamburg Germany	Maintenance training and examination organization and central functions. SoA 2.2: 21.11.2025
/53	c/o Lufthansa Technik Portugal LTPT Edificio Oceanus, Avenida da Boavista 3265 4.2 4100-137 Porto Portugal	Maintenance of engines of commercial aircraft operators and central functions. SoA 2.2: 21.11.2025
/54	c/o Lufthansa Technik Canada 150 9 Ave SW, Suite # 1240 Calgary, AB T2P 3H9 Canada	Maintenance of engines of commercial aircraft operators and central functions. SoA 2.2: 21.11.2025
/55	c/o Lumics LUM Weg beim Jäger 193 22335 Hamburg Germany	Consulting in lean management and process optimization and central functions. SoA 2.2: 21.11.2025
/56	c/o vAeroLabs AD Bulgaria vAEro Racho Petkov Kazandzhiyata Business Center Alpha 4 1766 Sofia Bulgaria	Central functions. SoA 2.2: 21.11.2025

Annex to certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 2200605**

/57	c/o Lufthansa Technik Shenzhen Co. Ltd Unified Social Credit Code: 91440300723043020B 2nd floor, Area A, Building 7, Phase III Huangtian Community Yangbei Industrial Zone Hangcheng Sub-district, Bao 'an District 518101 Shenzhen P.R. China	Maintenance of engines and aircraft components of commercial aircraft operators and central functions.SoA 2.2: 21.11.2025

2026-04-23

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

ISO/IEC 27001:2022 Annex A Controls

Annex	Chapter	Control target	Control	Statement of Applicability	Justification	Implementation Status
A.5 Organizational Controls	A 5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	Internal requirements	Implemented
	A 5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	Yes	Internal requirements	Implemented
	A 5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes	Risk treatment	Implemented
	A 5.4	Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	Risk treatment	Implemented
	A 5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	Yes	Legal Requirement	Implemented
	A 5.6	Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	Legal Requirement	Implemented
	A 5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Yes	Risk treatment	Implemented
	A 5.8	Information security in project management	Information security should be integrated into project management.	Yes	Risk treatment	Implemented
	A 5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes	Risk treatment	Implemented
	A 5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Yes	Risk treatment	Implemented
	A 5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes	Risk treatment	Implemented
	A 5.12	Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes	Risk treatment	Implemented
	A 5.13	Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Risk treatment	Implemented
	A 5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	Risk treatment	Implemented
	A 5.15	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Yes	Risk treatment	Implemented
	A 5.16	Identity management	The full life cycle of identities should be managed.	Yes	Risk treatment	Implemented
	A 5.17	Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes	Risk treatment	Implemented
	A 5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	Risk treatment	Implemented
	A 5.19	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	Risk treatment	Implemented
	A 5.20	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes	Risk treatment	Implemented
	A 5.21	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	Risk treatment	Implemented
	A 5.22	Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	Risk treatment	Implemented
	A 5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Yes	Risk treatment	Implemented
	A 5.24	Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	Risk treatment	Implemented
	A 5.25	Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	Yes	Risk treatment	Implemented
	A 5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Yes	Risk treatment	Implemented
	A 5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Yes	Risk treatment	Implemented
	A 5.28	Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	Risk treatment	Implemented
	A 5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Yes	Internal requirements	Implemented
	A 5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Risk treatment	Implemented
	A 5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	Yes	Risk treatment	Implemented
	A 5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	Yes	Risk treatment	Implemented
	A 5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	Risk treatment	Implemented
	A 5.34	Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Legal Requirement	Implemented
	A 5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Yes	Risk treatment	Implemented
	A 5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Yes	Risk treatment	Implemented
	A 5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Yes	Risk treatment	Implemented
	A 6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Legal Requirement	Implemented
	A 6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Yes	Risk treatment	Implemented

A.6 People Controls	A 6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes	Risk treatment	Implemented
	A 6.4	Disciplinary process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	Risk treatment	Implemented
	A 6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	Risk treatment	Implemented
	A 6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Risk treatment	Implemented
	A 6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	Risk treatment	Implemented
	A 6.8	Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	Risk treatment	Implemented
A.7 Physical Controls	A 7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Yes	Risk treatment	Implemented
	A 7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Yes	Risk treatment	Implemented
	A 7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Yes	Risk treatment	Implemented
	A 7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	Yes	Risk treatment	Implemented
	A 7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Yes	Risk treatment	Implemented
	A 7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Yes	Risk treatment	Implemented
	A 7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes	Risk treatment	Implemented
	A 7.8	Equipment siting and protection	To reduce the risks from physical and environmental threats, and from unauthorized access and damage.	Yes	Risk treatment	Implemented
	A 7.9	Security of assets off-premises	Off-site assets should be protected.	Yes	Risk treatment	Implemented
	A 7.10	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Risk treatment	Implemented
	A 7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Risk treatment	Implemented
	A 7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Yes	Internal requirements	Implemented
	A 7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	Risk treatment	Implemented
	A 7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Risk treatment	Implemented
A.8 Technological Controls	A 8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes	Risk treatment	Implemented
	A 8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Yes	Risk treatment	Implemented
	A 8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes	Risk treatment	Implemented
	A 8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes	Risk treatment	Implemented
	A 8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	Risk treatment	Implemented
	A 8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Yes	Risk treatment	Implemented
	A 8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Yes	Risk treatment	Implemented
	A 8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Yes	Risk treatment	Implemented
	A 8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Yes	Risk treatment	Implemented
	A 8.10	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Yes	Risk treatment	Implemented
	A 8.11	Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	Risk treatment	Implemented
	A 8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	Risk treatment	Implemented
	A 8.13	Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Risk treatment	Implemented
	A 8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes	Risk treatment	Implemented
	A 8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes	Risk treatment	Implemented
	A 8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	Risk treatment	Implemented
	A 8.17	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Yes	Risk treatment	Implemented
	A 8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes	Risk treatment	Implemented
	A 8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes	Risk treatment	Implemented
	A 8.20	Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes	Risk treatment	Implemented
	A 8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Yes	Risk treatment	Implemented
	A 8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks.	Yes	Risk treatment	Implemented
	A 8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Yes	Risk treatment	Implemented
	A 8.24	Use of cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.	Yes	Risk treatment	Implemented

	A 8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	Yes	Risk treatment	Implemented
	A 8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes	Risk treatment	Implemented
	A 8.27	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Yes	Risk treatment	Implemented
	A 8.28	Secure coding	Secure coding principles should be applied to software development.	Yes	Risk treatment	Implemented
	A 8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Yes	Risk treatment	Implemented
	A 8.30	Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	Yes	Risk treatment	Implemented
	A 8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	Yes	Risk treatment	Implemented
	A 8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes	Risk treatment	Implemented
	A 8.33	Test information	Test information should be appropriately selected, protected and managed.	Yes	Risk treatment	Implemented
	A 8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Yes	Risk treatment	Implemented