ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3539 (01/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Cloud Computing

Cloud computing – Framework of risk management

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3599**
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3539

Cloud computing – Framework of risk management

Summary

Recommendation ITU-T Y.3539 provides a framework of risk management in a cloud computing environment, including risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. It also provides a complete set of management processes and effective measures to reduce risks in the cloud computing environments.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3539	2023-01-13	13	11.1002/1000/15241

Keywords

Cloud computing, risk assessment, risk management, risk treatment.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3539

Cloud computing – Framework of risk management

1 Scope

This Recommendation provides an overview of and framework for risk management in the cloud computing environment. It focuses on the risk management processes of a cloud service provider (CSP) by addressing the following subjects:

– Overview and framework of risk management in a cloud computing environment;

– Risk assessment in a cloud computing environment;

– Risk treatment in a cloud computing environment.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ISO/IEC 27005] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: 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.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.5 vulnerability [b-ISO/IEC 27000]: Weakness of an asset or control that can be exploited by one or more threats.

3.1.6 risk [b-ISO/IEC 27000]: Effect of uncertainty on objectives.

3.1.7 risk assessment [b-ISO/IEC 27000]: Overall process of risk identification, risk and risk evaluation.

3.1.8 risk management [b-ISO/IEC 27000]: Coordinated activities to direct and control an organization with regard to risk.

3.1.9 risk treatment [b-ISO/IEC 27000]: Process to modify risk.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSC Cloud Service Customer

CSP Cloud Service Provider

CVE Collaborative Virtual Environment

DMZ Demilitarized Zone

NaaS Network as a Service

SQL Structured Query Language

XSS Cross-Site Scripting

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

In the body of this Recommendation and its annexes, the words should and may sometimes appear, in which case they are to be interpreted, respectively, as is recommended and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative is to be interpreted as having no normative intent.

6 Overview and framework of risk management in the cloud computing environment

With the rapid development of cloud computing, risk management has become increasingly important. In the actual production environment, network instability, equipment failure and other problems are inevitable. There are several potential risks associated with the life cycle of cloud services.

It is required that the CSP provide the following: cloud service security and risk manager with a complete set of processes for risk management and effective measures to reduce risks. The framework of risk management in the cloud computing environment provides management capabilities as shown in Figure 6-1. These management capabilities are based on the procedure described in [ISO/IEC 27005], specifically relating to the cloud computing environment aspect.

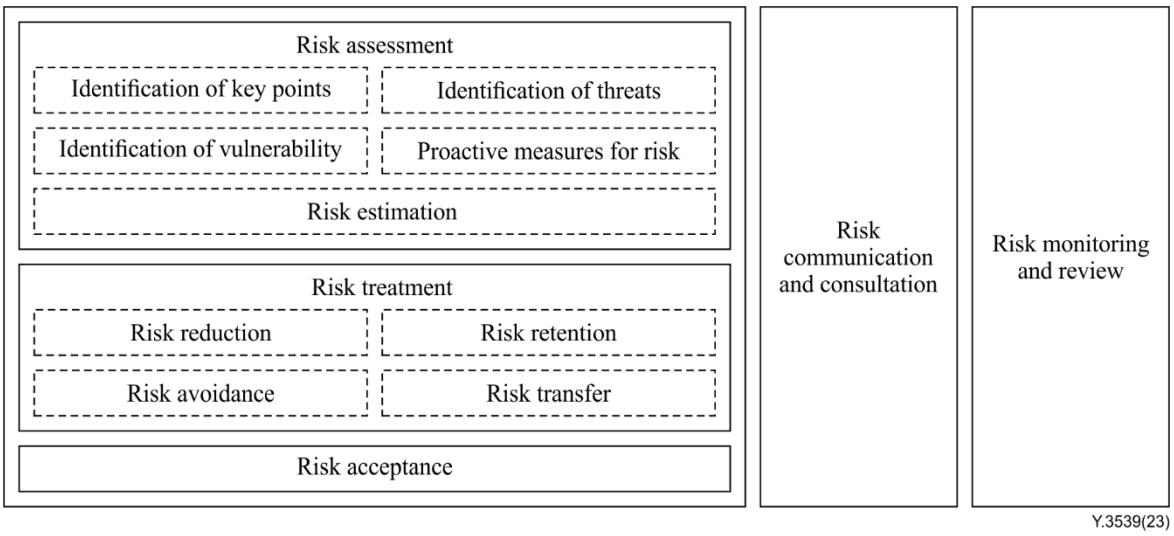

Figure 6-1 – Framework of risk management in the cloud computing environment

– Risk assessment: management capability for identifying and estimating risks in the cloud computing environment.

– Risk treatment: management capability for taking measures to keep risk within an acceptable range based on the results of a risk assessment, including risk reduction, risk retention, risk avoidance and risk transfer, which is presented in clause 8.

– Risk acceptance: management capability for accepting residual risks when the risk acceptance criteria are met. The following factors should be considered criteria:

  • Accepting a residual risk that leads to a small loss.

    NOTE 1 – Residual risk will not affect the cloud service in some cases, such as with some system vulnerabilities created by useless components. If the influence is small based on the risk evaluation, then the residual risk can be accepted.

  • When a key point has a risk that cannot be resolved, this risk is acceptable if the key point can bring very high benefits for the CSP.

    NOTE 2 – Some key points may bring risks and benefits simultaneously. For example, using open source components in cloud service may bring risks such as licence infringement and open source security incidents. Open source components could also bring benefits such as cost decreasing or rapid technology iteration. If the key point brings many more benefits then risks, it can be accepted.

  • Accepting the risk when the CSP cannot afford to reduce it.

– Risk communication and consultation: management capability for timely informing the cloud service customers (CSCs) of security risk events, including but not limited to:

  • Vulnerabilities that could threaten data and applications in cloud services;

  • Major changes of cloud services or CSP;

  • Security events that have occurred, such as data loss and data breach.

– Risk monitoring and review: management capability for intelligently paying timely attention to any security warning notices, vulnerability notices and other threat notices and generating a risk report on a regular basis for regulatory review.

7 Risk assessment in the cloud computing environment

7.1 Identification of key points

Risk management in the cloud computing environment involves many key points, including infrastructure, network resource, computing resource, storage resource, application, data, human factor and operation management. Categories and examples are shown in Table 7-1.

Table 7-1 – The key points for risk management in the cloud computing environment

Category	Example
Infrastructure	• Power • Air conditioning
Network resource	• Network equipment • Network architecture
Computing resource	• Physical server • Virtual host
Storage resource	• Storage equipment • Storage architecture
Application	• Service portal
Data	• User data • System data
Human factor	• CSP: cloud service operations manager
Operation management	• Cloud service life cycle management • Emergency response management
Shared responsibility	• Responsibilities of CSP • Responsibilities of CSC

The key points in the cloud computing environment should be valued based on the degree of impact. Table I.1 provides the reference weights for different levels in risk management in the cloud computing environment.

7.2 Identification of threats

Threat is a possible factor that can cause potential damage to the cloud computing environment and exists objectively. The causes of threats include environmental factors, technical failures and human factors. Categories and descriptions of threats are shown in Table 7-2.

Table 7-2 – Threat classification

Category	Description
Environmental factors	Environmental conditions and natural disasters such as: • Outage • Static electricity • Dust • Moist • Temperature • Flood • Fire • Earthquake

Table 7-2 – Threat classification

Category		Description
Technical failures		• Hardware failures • Cloud service software vulnerability
Human factors	Outsider threats	• Hacker attack • System intrusion • Unauthorized system access • System tampering • Information eavesdropping
	Insider threats	• Misoperation • Malicious behaviour

Estimating the frequency of threats is an important work of threat identification. The threat frequency can be divided into multiple levels representing different number of times threats are realised. The higher the level, the higher the frequency of the threats, and the greater the risky impact in the cloud computing environment. Table II.1 provides the reference levels and descriptions of threat frequency in the cloud computing environment.

7.3 Identification of vulnerability

Vulnerability identification methods include questionnaire surveys, tool detection, manual verification, log review and penetration testing.

Vulnerability is identified based on the key points for risk management in the cloud computing environment and corresponds to CSPs' measures for risk. For those systems with strong proactive measures for risk, the vulnerability is often low or does not exist.

7.4 Proactive measures for risk

7.4.1 Infrastructure risk

Proactive measures for infrastructure risk include:

- **Power redundancy** – the ability to resist power accidents, including data centre power redundancy, transformer redundancy, backup diesel generator redundancy and uninterruptible power supply system configuration redundancy.
- **Air conditioning redundancy** – the ability to resist air conditioning accidents, including chiller and cooling pump redundancy.
- **Reliability of building** – the ability to resist emergencies, including data centre seismic, fire, waterproof and antistatic level.
- **Entrance limitation** – the ability to use access control and video surveillance to ensure physical security.
- **Fire protection** – the ability to resist fire accidents, including through use of an automatic fire extinguishing system and fire alarm system.
- **Backup data centre** – the ability to deploy cloud services in active-standby data centres to maintain service continuation.

7.4.2 Network resource risk

Proactive measures for network resource risk include:

- **Network redundancy** – the ability of the redundancy of the NaaS CSP's network devices and network links.

- **Network isolation** – the ability of the division of the NaaS CSP's network security domain and network isolation for multitenant.

NOTE 1 – The network security domain includes the production domain, operation and maintenance management domain, office domain, DMZ domain and Internet domain.

- **Access control** – the ability to deploy access control mechanisms and setting of access control rules at the boundaries of different network domains.
- **Attack defence** – the ability of monitoring network attack behaviour, recording the attack type, attack time, attack traffic and so on, and taking corresponding defensive measures.
- **Invasion defence** – the ability of detecting network intrusion behaviour, recording the information of intrusion behaviour and taking the corresponding defensive measures.

NOTE 2 – Intrusion behaviour includes port scanning, SQL injection, command execution, code injection and XSS cross-site attack.

- **Cable protection** – the ability to use certain security measures to protect the NaaS CSP's cables.

7.4.3 Computing resource risk

Proactive measures for computing resource risk include:

- **Computing resource redundancy** – the ability to ensure the CSP's computing resource redundancy, including the design of high availability of computing resources, dual-machine hot backup, etc.
- **Vulnerability management** – the ability to scan and repair high-risk vulnerabilities, including the vulnerabilities in the collaborative virtual environment (CVE) and other public vulnerability databases, system software vulnerabilities and other high-risk vulnerabilities.
- **Baseline check** – the ability to check on the physical server, virtual host, system software and so on, including the CSC account security check, weak password check, configuration risk check, port status check and process status check.
- **Virus management** – the ability to check and kill viruses, including website backdoors and Trojan horses.

7.4.4 Storage resource risk

Proactive measures for storage resource risk include:

- **Storage redundancy** – the ability to ensure the CSP's storage redundancy in case of system or hardware failure.
- **Data backup strategy** – the ability to take appropriate strategies to back up the data, including full copy and erasure code copy.

7.4.5 Application risk

Proactive measures for application risk include:

- **Web vulnerability management** – the ability to scan and fix web vulnerability, including injection vulnerabilities, cross-site script vulnerabilities, invalid identity authentication and session management, unsafe direct object references, security configuration errors, sensitive information leaks, cross-site request forgery, components containing known vulnerabilities, unverified redirection and forwarding.
- **Web protection management** – the ability to have defence systems for web application.
- **Account security management** – the ability to check the security of CSCs' accounts, including weak password checking, anti-violence cracking and antimalicious registration.

7.4.6 Data risk

Proactive measures for data risk include:

- **Data persistence management** – the ability to take control measures to ensure there is no data lost, such as by making data tamper-proof.
- **Data availability management** – the ability to take control measures to ensure the normal use of data.
- **Data confidentiality management** – the ability to keep data confidential, including through data isolation and data encryption.

7.4.7 Operation risk

Proactive measures for operation risk includes:

- **Monitoring ability** – the ability to monitor all hardware and systems which carry cloud services, including power environment monitoring, physical equipment monitoring, network traffic monitoring, database monitoring and application monitoring and to represent results from a visual monitoring platform.
- **Alarm management** – the ability to provide alarm content management, fault detection and processing.
- **Authority management** – the ability to manage the authority of operation and maintenance personnel, including account management, authentication management, authority management and audit management.
- **Log management** – the ability to carry out log recording and log audit, including through user access logs, operation and maintenance personnel operation logs and system logs.
- **Asset management** – the ability to manage the software and hardware information assets related to cloud services, including information collection, asset change management and statistical reports.
- **Billing management** – the ability to carry out accurate billing, including implementing billing rule settings and billing item configuration.
- **Operation tool management** – the ability to approve, control and monitor the use of information system maintenance tools.

7.4.8 Shared responsibility risk

Proactive measures for shared responsibility risk include:

- **Division of security responsibilities** – the ability to clarify the responsibilities of the CSC and the different roles of CSP.
- **Notification of responsibilities** – the ability to inform the CSC in advance of risk events that are not covered by the CSP.

7.5 Risk estimation

After identifying key points, threats, vulnerabilities and proactive measures for risk in the cloud computing environment, the risk value is obtained by combining key point weight, threat frequency level and the coefficient of proactive measures. Appendix IV and Appendix V demonstrate the mapping of the key points, threats and proactive measures, among other things.

Once the proactive measures for risk in clause 7.4 are in place, the corresponding coefficient is 0; otherwise, it is 1. The specific formula is given in Appendix III.

8 Risk treatment in the cloud computing environment

Based on the results of risk assessment, the risk treatment is selected, whose procedure is presented in Figure 8-1.

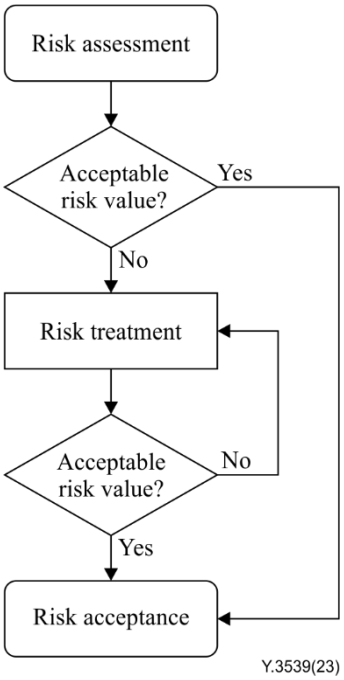

Figure 8-1 – Risk treatment process in the cloud computing environment

8.1 Risk reduction

Risk reduction refers to the ability to reduce the risk level through relevant selection control measures and tp enable the residual risk to reach an acceptable level when it is assessed again. Control measures include:

- Optimizing management system, including objectives, roles, responsibilities and processes.
- Repairing software and hardware defects.
- Introducing advanced technologies and tools in risk management in the cloud computing environment, such as automated monitoring systems and intelligent analysis systems.

When selecting control measures, the cost of acquiring, implementing, managing, operating, monitoring and maintaining control measures should be weighed against the value of key points for risk management in the cloud computing environment.

8.2 Risk retention

Risk retention refers to the ability to make the decision of not taking further risk preservation steps based on the risk assessment. If the risk level meets the risk acceptance criteria, then there is no need to implement additional control measures and the risk can be retained.

8.3 Risk avoidance

Risk avoidance refers to the ability to avoid activities or conditions that cause specific risks. When the identified risk is considered too high or the cost of other risk treatment options exceeds the threshold, the planned or existing activities should be withdrawn to avoid risks.

The above activities refer to changes made by CSP related with key points for risk management, such as storage architecture adjustments and large-scale data migrations.

8.4 Risk transfer

Risk transfer refers to the ability to transfer the risk to another party who can effectively manage the specific risk. The typical approach is to buy insurance that covers cloud service outages, data loss and cyberattacks.

NOTE – Risk transfer may generate new risks or change existing risks.

Appendix I

Key point weight for risk management in the cloud computing environment

(This appendix does not form an integral part of this Recommendation.)

Table I.1 shows key point weights for different levels in risk management in the cloud computing environment.

Table I.1 – Key point weights for different levels in risk management in the cloud computing environment

Weight	Identification	Description
3	High	Significantly important, it may cause very serious damage to cloud services
2	Medium	Moderately important, it may cause moderate loss to cloud services.
1	Low	Less important, it may cause less loss to cloud services.

Appendix II

Threat frequency in the cloud computing environment

(This appendix does not form an integral part of this Recommendation.)

Table II.1 shows level and description of threat frequency in the cloud computing environment.

Table II.1 – Level for threat frequency in the cloud computing environment

Level	Identification	Description
3	High	Frequency of threats which will inevitably happen in most cases or can be proved to happen often.
2	Medium	Frequency of threats which may occur in some cases or be proven to have happened.
1	Low	Frequency of threats which are generally unlikely and have not been proven to happen.

Appendix III

The formula of risk estimation

(This appendix does not form an integral part of this Recommendation.)

The following formula shows the equation of risk value estimation.

$$Risk\ value = \sum Proactive\ measure\ coefficient * Key\ point\ weight * Threat\ frequency$$

For example, user data is very important, so its weight is 3. When CSP suffers from frequent theft of user data, its threat frequency is 3. If a CSP has no protection measures for this threat, then the proactive measure coefficient is 1, and the current risk value is 9 based on the above formula.

Appendix IV

Mapping of threats and key points for risk management in the cloud computing environment

(This appendix does not form an integral part of this Recommendation.)

Table IV.1 shows a mapping of threats and key points for risk management in the cloud computing environment.

The letter 'Y' in a cell formed by the intersection of the table rows and columns designates that a particular threat for cloud service is addressed by a corresponding key point for risk management in the cloud computing environment.

Table IV.1 – Mapping of threats and key points for risk management in the cloud computing environment

Risk assessment		**Identification of threats**																
		Environmental factors								**Technical failures**		**Human factors**						
												Outsider threats					**Insider threats**	
		Outage	Static electricity	Dust	Moisture	Temperature	Flood	Fire	Earthquake	Hardware failures	Cloud service software vulnerability	Hacker attack	System intrusion	Unauthorized system access	System tampering	Information eavesdropping	Misoperation	Malicious behaviour
Identification of key points	**Infrastructure**	Y	Y	Y	Y	Y	Y	Y	Y	—	—	—	—	—	—	—	—	—
	Network resource	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	—	—
	Computing resource	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	—	—
	Storage resource	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	—	—
	Application	—	—	—	—	—	—	—	—		Y	Y	Y	Y	Y	Y	—	—
	Data	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	—	—
	Human factor	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	Y
	Operation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table IV.1 – Mapping of threats and key points for risk management in the cloud computing environment

Risk assessment		Identification of threats																
		Environmental factors								Technical failures		Human factors						
												Outsider threats					Insider threats	
		Outage	Static electricity	Dust	Moisture	Temperature	Flood	Fire	Earthquake	Hardware failures	Cloud service software vulnerability	Hacker attack	System intrusion	Unauthorized system access	System tampering	Information eavesdropping	Misoperation	Malicious behaviour
	Shared responsibility	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	—	—

Appendix V

Mapping of threats and proactive measures for risk in the cloud computing environment

(This appendix does not form an integral part of this Recommendation.)

Table V.1 shows a mapping of threats and proactive measures for risk in the cloud computing environment.

The letter 'Y' in a cell formed by the intersection of the table rows and columns designates that a particular threat for cloud service is addressed by a corresponding proactive measure for risk.

Table V.1 – Mapping of threats and proactive measures for risk in the cloud computing environment

Risk assessment			Identification of threats																
			Environmental factors								Technical failures		Human factors						
													Outsider threats					Insider threats	
			Outage	Static electricity	Dust	Moisture	Temperature	Flood	Fire	Earthquake	Hardware failures	Cloud service software vulnerability	Hacker attack	System intrusion	Unauthorized system access	System tampering	Information eavesdropping	Misoperation	Malicious behaviour
Proactive measures for risk	Infrastructure risk	Power redundancy	Y	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
		Air conditioning redundancy	—	—	—	Y	Y	—	—	—	—	—	—	—	—	—	—	—	—
		Reliability of building	—	Y	Y	—	—	Y	Y	Y	—	—	—	—	—	—	—	—	—
		Entrance limitation	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y
		Fire protection	—	—	—		—		Y	—	—	—	—	—	—	—	—	—	—
		Backup data centre	Y	—	—	—	—	Y	Y	Y	—	—	—	—	—	—	—	—	—

Table V.1 – Mapping of threats and proactive measures for risk in the cloud computing environment

Risk assessment			Identification of threats																
			Environmental factors								Technical failures		Human factors						
													Outsider threats					Insider threats	
			Outage	Static electricity	Dust	Moisture	Temperature	Flood	Fire	Earthquake	Hardware failures	Cloud service software vulnerability	Hacker attack	System intrusion	Unauthorized system access	System tampering	Information eavesdropping	Misoperation	Malicious behaviour
	Network resource risk	Network redundancy	Y	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—	—
		Network isolation	Y	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—	—
		Access control	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	—	—
		Attack defence	—	—	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—
		Invasion defence	—	—	—	—	—	—	—	—	—	Y		Y	Y	Y	Y	—	—
		Cable protection	—	—	—	—	—	Y	Y	Y	—	—	—	—	—	—	—	—	—
	Computing resource risk	Computing resource redundancy	—	—	—	—	—	—	—	—	Y	—	—	—	—	—	—	—	—
		Vulnerability management	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	—	—
		Baseline check	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	Y	Y
		Virus management	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	—	—

Table V.1 – Mapping of threats and proactive measures for risk in the cloud computing environment

Risk assessment		Identification of threats																
		Environmental factors								Technical failures		Human factors						
												Outsider threats					Insider threats	
		Outage	Static electricity	Dust	Moisture	Temperature	Flood	Fire	Earthquake	Hardware failures	Cloud service software vulnerability	Hacker attack	System intrusion	Unauthorized system access	System tampering	Information eavesdropping	Misoperation	Malicious behaviour
Storage resource risk	Storage devices redundancy	—	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—	—
	Data backup strategy	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Application risk	Web vulnerability management	—	—	—	—	—	—	—	—	—	Y	—	—	—	—	—	—	—
	Web protection management	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	—	—
	Account security management	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y
Data risk	Data persistence management	—	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—	—
	Data availability management	—	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—	—
	Data confidentiality management	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	—	—
Operation risk	Monitoring ability	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	—	—	—	Y	Y
	Alarm management	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	—	—	—	Y	Y
	Authority management	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y

Table V.1 – Mapping of threats and proactive measures for risk in the cloud computing environment

Risk assessment			Identification of threats																
			Environmental factors								Technical failures		Human factors						
													Outsider threats					Insider threats	
			Outage	Static electricity	Dust	Moisture	Temperature	Flood	Fire	Earthquake	Hardware failures	Cloud service software vulnerability	Hacker attack	System intrusion	Unauthorized system access	System tampering	Information eavesdropping	Misoperation	Malicious behaviour
		Log management	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	—	—	—	Y	Y
		Asset management	—	—	—	—	—	—	—	—	Y	Y	—	—	—	—	—	—	—
		Billing management	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	Y
		Operation and maintenance tool management	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	Y
	Shared responsibility risk	Division of security responsibilities	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	Y	Y	—	—
		Notification of responsibilities	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—

Bibliography

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023