International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2023, Vol. 7, No. 2, IJSKM782

Risk Management Portfolio for Secure Telework

Hiroki Koyama [*], Yuuna Nakagawa [*], Shigeaki Tanimoto [*],
Teruo Endo [†], Takashi Hatashima [‡], Atsushi Kanai [§]

Abstract

In Japan, telework is attracting renewed attention due to the government-led "work style reform". The advent of COVID-19 in 2020 has led to the rapid spread of teleworking, and its current state of widespread adoption may be attributed to transient factors as a counter to the spread of COVID-19. A current problem is that dealing with the emergence of risks has been postponed or overlooked because telework was hastily promoted and introduced even though sufficient preparations had not been made. In this work, we conducted a risk assessment from the viewpoints of both companies and employees, identified 28 risk factors, and proposed countermeasures for these factors in order to make teleworking permanently safe and secure in the new normal era. We also proposed the establishment of various systems related to the telework environment and the effective use of cloud computing as measures for both companies and employees. The results of an evaluation of these risk countermeasure proposals using risk values showed that they could reduce risk by approximately 61%. Finally, we constructed a portfolio to identify priorities for the proposed risk measures in terms of practical applicability and to identify the appropriate stepwise introduction of them. The results should contribute to the safe and secure utilization of telework in the new normal era.

Keywords: Telework, Work Style Reform, Risk Assessment, Risk Management Portfolio

1 Introduction

Telework is a working style that enables people to work regardless of time or place through the use of Information and Communication Technology (ICT). In general, there are three major types of telework: telecommuting, in which work is performed at home without going to the office; mobile work, in which work is performed on the road or in cafes; and satellite work, in which work is performed in offices other than the workplace [1].

Telework has undeniable advantages for both employees and companies. The benefits for employees include an improved work-life balance and a reduction in commuting fatigue, while the

[*] Faculty of Social System Science, Chiba Institute of Technology, Chiba, Japan
[†] Faculty of Liberal Arts, Osaka Shoin Women's University, Osaka, Japan
[‡] NTT Social Informatics Laboratories, Musashino, Japan
[§] Faculty of Science and Engineering, Hosei University, Koganei, Japan

benefits for companies are the assurance of business continuity in the event of a disaster or pandemic and a reduction in the number of employees who take time off due to childcare or nursing care [2]. The need for telework as a measure to prevent the spread of COVID-19 infection has also increased in recent years and is spreading rapidly.

However, as telework was hastily promoted even though companies were not yet ready for it in terms of their systems, various risks that have been postponed or overlooked are now becoming more apparent.

In this paper, we report the risk assessment we conducted from the perspectives of both the company and the employees in order to utilize telework in a safe and secure manner on a permanent basis in the new normal era. Specifically, using past literature and case studies as a basis, we first comprehensively extracted risk factors in teleworking using the Risk Breakdown Structure (RBS) method. Next, we analyzed the extracted risk factors using the risk matrix method and came up with countermeasures for them. We then evaluated the proposed countermeasures using the risk values and clarified their effectiveness. Finally, we created a portfolio of proposed risk countermeasures from the viewpoint of practical applicability and developed guidelines for their gradual introduction. This work will contribute to the safe and secure operation of telework in the new normal era with a view to the post-corona era.

Section 2 of this paper describes the current status and issues of telework, Section 3 presents related studies, Section 4 describes the assessment of telework risk based on the results of Sections 2 and 3, Section 5 describes the portfolio of proposed risk countermeasures, and Section 6 concludes the paper and mentions future work.

2 Current Status and Issues of Telework

2.1 Current Status of Telework

In recent years, government-led "work style reforms" have been promoted in Japan, which has led to the requirement of more flexible work styles. Among these, teleworking has been attracting the most attention because it enables people to work without being restricted by time or location through the use of ICT. For example, it can be used to secure the labor force in an aging society with a declining birthrate by reducing job turnover due to childcare and nursing care and by increasing job opportunities for the elderly and physically challenged people who may have difficulty commuting to work. According to a survey by the Ministry of Internal Affairs and Communications (MIC), the number of companies responding that they have already introduced telework has been increasing over the past 15 years—from 8.5% in 2004 to 21.1% in 2019—but it is not yet widespread [3].

As for other countries, the United States has the highest percentage of companies that have already introduced telework (85.0%), followed by the United Kingdom (38.2%) and Germany (21.9%) [4]. In the United States, the federal government has been promoting telework since the early 1990s, and in 2010 it enacted the Telework Enhancement Act. Telework is being actively promoted not only by private companies but also by government employees, including the employees of ministries and state governments [5].

The number of companies in Japan that are trying to introduce teleworking has been rapidly increasing since the advent of COVID-19. In a survey on the introduction rate of telework conducted by the Tokyo Metropolitan Government in March and April 2020, 24.0% of respondents answered that they had introduced it in March, and this number leapt to 62.7% by April. The percentage of employees who were implementing telework was about 20% as of December 2019, but about 50% of employees had started implementing telework as of April 2020.

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

2.2 Issues of Telework

While telework has undeniable advantages, there are also many challenges that complicate its widespread adoption. One example is found in the "White Paper on Information and Communications 2018" published by the MIC, where the largest number of respondents indicated that the development of a telework environment is an issue. In addition, according to the answers to a questionnaire administered to companies that have introduced telework, communication among employees and system design during telework can also be considered issues, as evidenced by the introduction of web conferencing, chat, etc. along with the planning necessary to introduce a new telework system that meets the needs of the new normal era [6]. In the telework work environment, it is important for employers to educate and advise employees to create an environment that takes health and safety into consideration, and to consider improving the environment or using satellite offices and other work locations outside the home. In addition, because teleworkers work in an environment where there are no supervisors or coworkers around, they cannot communicate as easily as in the traditional workplace, and mental health issues may emerge, such as a sense of loneliness and difficulties in noticing mental or physical changes in employees.

3 Related Work

There have been numerous studies of the risks associated with telework, both before and during the outbreak of the COVID-19 pandemic.

According to T. Gentle [7], while the transition to telework has been rapidly progressing in the United States due to the influence of COVID-19, many companies still use the same tools and techniques as in the traditional workplace and assume that these will continues to work. Moreover, it is not enough for companies to ensure protection from the outside: they also need to deal with internal threats. The risks of remote work environments need to be mitigated through employee education, virtual applications and desktops, communication, security enhancements, and user behavior analysis.

Y. Huiyi et al. [8] clarified that technological advances create both new risks and solutions for telework. He pointed out that, as with the responses to other security risks, they need to be constantly updated. While telework has many advantages, it can lead to security risks such as data leakage and falsification. However, these risks can be controlled, and several methods for doing so have been proposed, including those for establishing policies, training employees, securing networks and devices, and encrypting information.

P. Pyoria [9] attributed the slow diffusion of telework to the fact that businesses are concentrated in certain regions where a telework culture and contractual framework have not been established. He also stated that success is more likely to occur if the benefits and risks associated with telework are prepared for from the outset.

S. Desio et al. [10] evaluated the impact of teleworking as a response to COVID-19 on organizations, with a particular focus on psychological distress and well-being. Their findings showed that employees may be exposed to psychosocial risks such as loneliness, stress, and overwork, and are at risk for unhealthy eating and increased smoking, especially if they live alone.

A. M. Luchena et al. [11] analyzed teleworking form a social welfare point of view under a declared state of emergency in Spain and found that teleworking allowed for a more flexible response to COVID-19 and a more flexible work-life balance, but they pointed out that it is also necessary to consider psychological risks such as working long hours, switching between work

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

and private life, the impact of law amendments, and technological advances. In particular, disparities with older workers and gender considerations were noted.

While these previous studies have described external and internal security risks and psychological risks, not enough research has been done on the risks of telework work environments and internal systems. In addition, in individual studies, risks on the company side, such as legal changes, and risks on the employee side, such as internal fraud and psychological risks, have not been studied in an integrated manner. Ultimately, as some studies have stated, risk analysis by COVID-19 impact is useful because risks need to be constantly reviewed and updated according to technological advances and the current times.

4 Risk Assessment in Telework

4.1 Risk Assessment Process

Risk assessment is one of the most important steps in any risk management process. How well risks are managed depends on anticipating them and taking measures to avoid them in advance. After referring to papers by S. Frosdick [12] and others, we decided to proceed with risk assessment in the following process: (1) risk identification, (2) risk analysis, and (3) risk evaluation.

4.2 Identification of Risk Factors

Typical methods of risk analysis include the Delphi method [13], FTA (Fault Tree Analysis) [14], and RBS [15], [16]. The Delphi method is a method of aggregating opinions by repeating the process of multiple experts sharing their opinions, checking each other's opinions, and then sharing their opinions further. FTA is a method to identify all possible paths for undesirable events to occur, and is mainly used as an analysis related to machine and software failures. RBS is a method for extracting risk factors by decomposing and structuring the elements subject to risk analysis. Here, we decided to use RBS, which can comprehensively extract risk factors of telework from the viewpoint of promoting safe and secure telework.

Specific risk factors based on the RBS were extracted from three representative case studies by public and private organizations and multiple reviews by the authors under the MECE (Mutually Exclusive, Collectively Exhaustive) perspective. The first case study is the "Telework Implementation Issues (n=232)" survey conducted by the Ministry of Internal Affairs and Communications in 2018 before the start of COVID-19 [6], the second is the "Telework Awareness Survey (n=400)" conducted by the private company Sky Corporation in August 2020 after the start of COVID-19 [17], the third case referred to "Issues that arose when implementing telework (n=732)" within the "Results of an Urgent Questionnaire Survey by Telework Implementation Status" conducted by the Tokyo Chamber of Commerce and Industry in May 2020 [18]. Based on these three representative case studies by public and private organizations, the data was used to survey the actual conditions of teleworking before and after the start of COVID-19. These data were systematically extracted based on discussions by the authors (researchers from universities and companies) and from the MECE perspective.

Table 1 (1) shows the risk factor extraction results, where we categorized the risk factors of teleworking into both company and employee aspects in the first level and into environmental, security, and institutional aspects in the next level. Through this hierarchical and exhaustive study, we ultimately identified 28 risk factors. On the employee side, risk factors include the telework environment (such as the tools used in telework, the network, and the work environment) as well

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

as psychological aspects (such as internal fraud and security, including privacy). The risk factors on the company side include internal rules (such as the cost of building the work environment, provision of utilities during work, and rules for teleworking) as well as internal systems including attendance management [19] - [20].

Table 1: Risk specification results by RBS and risk analysis results by risk matrix method.

(1) Results of risk factor extraction using RBS method					(2) Results of risk analysis using risk matrix method			
No.	Level1	Level2	Level3	Level4/Risk Factor	Risk Probability	Risk Impact	Risk Classification	Risk Countermeasures
1	Employee side	Telework environment	Telework tools	Lack of proficiency with tools such as Remote Desktop	High	Low	Risk Mitigation	Create procedures for work and communication tools based on the company's security policy, and educate employees about the rules on a regular basis.
2				Lack of proficiency with communication tools such as web conferencing				
3			Working environment	Insufficient bandwidth in the network environment				Data dieting (e.g., limiting video and audio for web conferencing when bandwidth is insufficient) is performed as necessary.
4				Lack of printers and other fixtures				Establish a system for companies to pay for the construction of telework environments.
5				Vulnerability of telecommunication devices for telework	Low	High	Risk Transfference	Keep telework communication device software up to date. Manage the access log.
6				Lack of independent telework environment	High	High	Risk Avoidance	Establish a system for companies to pay for the construction of telework environments.
7				Health hazards such as economy class syndrome				Companies should develop labor management for teleworkers and ensure that they have time for health care.
8		Security environment	Physical security	Shoulder hacking into PC screen in a telework environment	High	Low	Risk Mitigation	Create telework work standards based on the company's security policy and educate employees about the rules on a regular basis.
9				Loss of corporate terminal for telework	Low	High	Risk Transfference	MDM should be implemented for company-leased terminals, and encryption should be required when storing data; for non-company-leased terminals (e.r., BYOD), remote VPN and cloud computing should be required.
10				Use of shared home terminals				Based on the company's security policy, create telework work standards, such as prohibiting the use of terminals other than company-loaned terminals and authorized terminals, and educate employees about them.
11				Use of free Wi-Fi, etc.				Companies can set up a system to pay for the construction of a telework environment and lend mobile Wi-Fi to their employees.
12				No face-to-face surveillance possible	High	High	Risk Avoidance	Companies should establish a working environment for telework and require employees to report on the progress of their work on a regular basis.
13			Cyber security	File-sharing mistakes	Low	High	Risk Transfference	Create telework work standards based on the company's security policy, and educate employees about them. Specifically, prohibit the use of terminals other than those loaned by the company or those authorized (e.g., MDM-implemented terminals), and require the use of remote VPN or cloud computing for BYOD and other non-company loaned terminals.
14				Unauthorized access				
15				Computer virus				
16				Use of outdated security software				
17				Installation of unnecessary software				
18			Psychological security	Internal fraud				Create telework work standards based on the company's security policy, and educate employees on a regular basis.
19				Lack of a face-to-face partner (loneliness while working)	High	High	Risk Avoidance	Provide a virtual environment where companies can develop a labor environment for telework and enable employees to communicate with each other.
20			Privacy	Leakage of images and conversations of non-related parties during a web conference				Create telework work standards based on the company's security policy and educate employees about them.
21				Mirroring of work area during a web conference	Low	High	Risk Transfference	Establish a system in which companies pay for the construction of a telework environment.
22	Employer side	Internal legal system	Internal rule	Fees for telework environment				
23				Inadequate communication rules in telework environment	High	Low	Risk Mitigation	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
24				Increase in water and electricity costs due to working in telework environment	High	High	Risk Avoidance	Establish a system in which companies pay for the construction of telework environments.
25				Mail delivered to the office addressed to a teleworking employee	High	Low	Risk Mitigation	Create telework work standards based on the company's security policy and educate employees about them.
26			Labor management	Inadequate labor management in telework	High	High	Risk Avoidance	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
27				Increase in overtime hours in telework		High		Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.
28				Increase in web conferencing in telework	High	Low	Risk Mitigation	

4.3 Risk Analysis and Proposal of Countermeasures

In the risk analysis, we used the risk matrix method to capture the characteristics of telework risk as an initial study. This method is a qualitative analysis technique that classifies each risk factor into one of the four areas shown in Fig. 1. As shown in Table 1 (2), eight risk factors were classified as Risk Avoidance, 12 as Risk Transference, eight as Risk Mitigation, and zero as Risk Acceptance. Thus, measures based on Risk Transference accounted for about half of the total.

The following are the results of our analysis of the 28 risk factors listed in Table 1 using the risk matrix method.

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

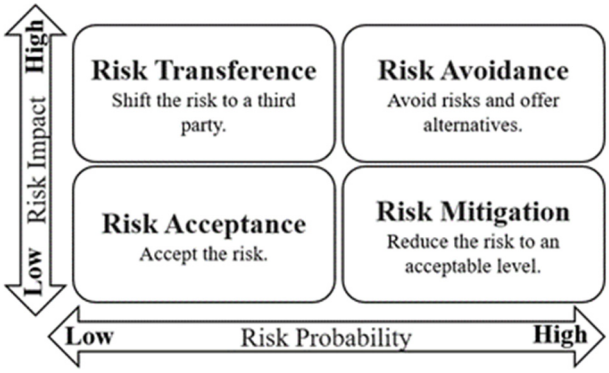

Figure 1 Risk matrix method.

4.3.1 Risk Transference

Table 2 lists the risk factors for which the risk classification was "Risk Transference". The main trends here include many of the security issues involved in teleworking, such as physical security, cybersecurity, and psychological security. The main countermeasures include the introduction of Mobile Device Management (MDM) for teleworking terminals, obligatory use of a Virtual Private Network (VPN) and cloud computing for Bring Your Own Device (BYOD) and other terminals not leased by the company, and teleworking based on the company's security policy. Clear standards should be developed and employees should be educated about them.

4.3.2 Risk Avoidance

Table 3 shows the list of risk factors whose risk classification was "Risk Avoidance". The main trends here include problems with the telework environment and attendance management. Major measures include the development of support systems for companies to establish a telework environment and the development of labor management for telework.

4.3.3 Risk Mitigation

Table 4 shows the list of risk factors with a risk classification of "Risk Mitigation". The main trends here include problems with telework tools, telework environments, and internal company rules. The main measures include the development of a labor environment for telework, the creation of telework standards based on security policies by companies, and the implementation of training for employees.

4.3.4 Summary

On the basis of the above results, the main risk measures for the 28 risk factors are as follows.

a) Companies create telework standards based on their security policies.
b) MDM and data encryption are installed in company-rented terminals.
c) For terminals other than company-issued terminals (e.g., BYOD), VPN and cloud computing are obligatory [21].

The most important risk countermeasure for telework is the establishment of a telework system based on the basic company security policy, which includes strengthening the operational aspects of telework, i.e., working style, work environment (including tools), and security.

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

Table 2: Risk transference measure characteristics (risk probability: low, risk impact: high).

(1) Results of risk factor extraction using RBS method		(2) Results of risk analysis using risk matrix method
No.	Level4/Risk Factor	Risk Countermeasures
5	Vulnerability of telecommunication devices for telework	Keep telework communication device software up to date. Manage the access log.
9	Loss of corporate terminal for telework	MDM should be implemented for company-leased terminals, and encryption should be required when storing data; for non-company-leased terminals (e.g., BYOD), remote VPN and cloud computing should be required.
10	Use of shared home terminals	Based on the company's security policy, create telework work standards, such as prohibiting the use of terminals other than company-loaned terminals and authorized terminals, and educate employees about them.
11	Use of free Wi-Fi, etc.	Companies can set up a system to pay for the construction of a telework environment and lend mobile Wi-Fi to their employees.
13	File-sharing mistakes	Create telework work standards based on the company's security policy, and educate employees about them. Specifically, prohibit the use of terminals other than those loaned by the company or those authorized (e.g., MDM-implemented terminals), and require the use of remote VPN or cloud computing for BYOD and other non-company loaned terminals.
14	Unauthorized access	
15	Computer virus	
16	Use of outdated security software	
17	Installation of unnecessary software	
18	Internal fraud	Create telework work standards based on the company's security policy, and educate employees on a regular basis.
21	Mirroring of work area during a web conference	Establish a system in which companies pay for the construction of a telework environment.
22	Fees for telework environment	

Table 3: Risk avoidance measure characteristics (risk probability: high, risk impact: high).

(1) Results of risk factor extraction using RBS method		(2) Results of risk analysis using risk matrix method
No.	Level4/Risk Factor	Risk Countermeasures
6	Lack of independent telework environment	Establish a system for companies to pay for the construction of telework environments.
7	Health hazards such as economy class syndrome	Companies should develop labor management for teleworkers and ensure that they have time for health care.
12	No face-to-face surveillance possible	Companies should establish a working environment for telework and require employees to report on the progress of their work on a regular basis.
19	Lack of a face-to-face partner (loneliness while working)	Provide a virtual environment where companies can develop a labor environment for telework and enable employees to communicate with each other.
20	Leakage of images and conversations of non-related parties during a web conference	Create telework work standards based on the company's security policy and educate employees about them.
24	Increase in water and electricity costs due to working in a telework environment	Establish a system in which companies pay for the construction of telework environments.
26	Inadequate labor management in telework	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
27	Increase in overtime hours in telework	Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.

Table 4: Risk mitigation measure characteristics (risk probability: high, risk impact: low).

(1) Results of risk factor extraction using RBS method		(2) Results of risk analysis using risk matrix method
No.	Level4/Risk Factor	Risk Countermeasures
1	Lack of proficiency with tools such as Remote Desktop	Create procedures for work and communication tools based on the company's security policy, and educate employees about the rules on a regular basis.
2	Lack of proficiency with communication tools such as web conferencing	
3	Insufficient bandwidth in the network environment	Data dieting (e.g., limiting video and audio for web conferencing when bandwidth is insufficient) is performed as necessary.
4	Lack of printers and other fixtures	Establish a system for companies to pay for the construction of telework environments.
8	Shoulder hacking into PC screen in a telework environment	Create telework work standards based on the company's security policy and educate employees about the rules on a regular basis.
23	Inadequate communication rules in telework environment	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
25	Mail delivered to the office addressed to a teleworking employee	Create telework work standards based on the company's security policy and educate employees about them.
28	Increase in web conferencing in telework	Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.

4.4 Evaluation of Risk Countermeasures by Risk Values

Next, we evaluated the effectiveness of the proposed measures by quantifying the risk factors listed in Table 1. We used risk calculation formulas common in the field of ISMS to determine risk values based the qualitative results reported above. Finally, risk values were calculated using formulas and approximations [22].

1) Ordinary Risk Value Formula

Each risk value is quantified as follows.

Risk value = value of asset * value of threat * value of vulnerability (1)

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

In general, calculating the elements on the right-hand side of Eq, (1) is very difficult, so to simplify, we used the following approximate formulas [23] - [25].

2) Approximate Risk Value Formula

2-a) Approximation of Asset Value

The asset value is approximated by the impact of the risk matrix, as shown in Fig. 2. In other words, the value of an asset is considered to be the impact of risk. Degrees of risk are defined as 1 (low) to 5 (high) [22]. The risk matrix is divided into two risk impact levels, where for the sake of simplicity, the higher impact is assumed to be 5 (the maximum risk level) and the lower impact is assumed to be 1 (the minimum risk level).

2-b) Approximation of Threat Value

The threat value in Eq. (1) is approximated by the risk occurrence probability in the risk matrix. In the reference literature, risk probability is defined in three levels [23]. These values are mapped to the risk occurrence probabilities in the risk matrix in Fig. 2 (as in 2-a) above), with the maximum value of the risk occurrence probability being 3 and the minimum value being 1.

2-c) Approximation of Value of Vulnerability

The vulnerability rating is defined as a three-level rating: 3 (high), 2 (medium), and 1 (low) [22]. Here, the four regions in Fig. 2 are classified into three categories according to risk probability and risk impact. Risk Avoidance is approximated as 3 (high), Risk Transference and Risk Mitigation as 2 (medium), and Risk Acceptance as 1 (low). As described above, Eq. (1) can be simplified to Eq. (2). Approximate values for each parameter in Eq. (2) are listed in Table 5.

$$\text{Risk value} \fallingdotseq \text{value of risk impact} * \text{value of risk probability} * \text{value of vulnerability} \quad (2)$$

3) Calculation of Risk Value Based on Eq. (2)

We calculated risk values for all risk factors using Eq. (2). Then, we implemented the proposed countermeasures and calculated the risk values again. The results are shown in Table 6.

Table 5: Approximate values of Eq. (2).

	Risk Impact	Risk Probability	Vulnerability	
High	3	5	Risk Avoidance	3
Low	1	1	Risk Transference and Mitigation	2
			Risk Acceptance	1

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

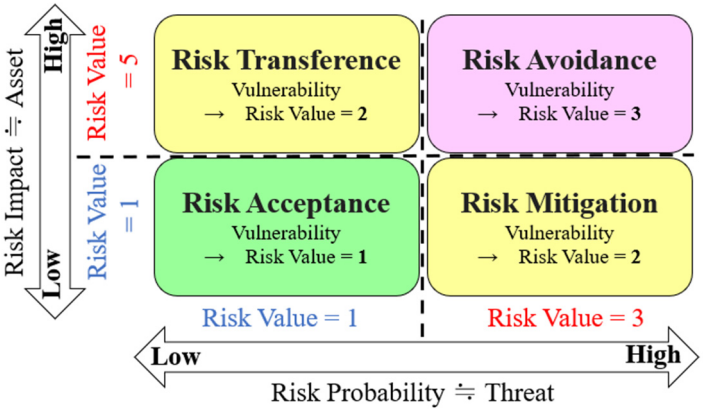

Figure 2 Risk value approximation of risk matrix.

Table 6: Risk analysis results.

No.	Risk Factor	Risk Probability	Risk Impact	Before risk countermeasures		After risk countermeasures	
				Vulnerability (Risk Classification)	Risk value	Vulnerability (Risk Classification)	Risk value
1	Lack of proficiency with tools such as Remote Desktop	3	1	2	6	1	3
2	Lack of proficiency with communication tools such as web conferencing	3	1	2	6	1	3
3	Insufficient bandwidth in the network environment	3	1	2	6	1	3
4	Lack of printers and other fixtures	3	1	2	6	1	3
5	Vulnerability of telecommunication devices for telework	3	5	2	30	1	15
6	Lack of independent telework work environment	3	5	3	45	1	15
7	Health hazards such as economy class syndrome	3	5	3	45	1	15
8	Shoulder hacking into the PC screen in a telework environment	3	1	2	6	1	3
9	Loss of corporate terminal for telework	1	5	2	10	1	5
10	Use of shared home terminals	1	5	2	10	1	5
11	Use of free Wi-Fi, etc.	1	5	2	10	1	5
12	No face-to-face surveillance possible	3	5	3	45	1	15
13	File sharing mistakes	1	5	2	10	1	5
14	Unauthorized access	1	5	2	10	1	5
15	Computer virus	1	5	2	10	1	5
16	Use of outdated security software	1	5	2	10	1	5
17	Install unnecessary software	1	5	2	10	1	5
18	Internal fraud	1	5	2	10	1	5
19	Lack of a face-to-face partner (loneliness while working)	3	5	3	45	1	15
20	Leakage of images and conversations of non-related parties during a web conference	3	5	3	45	1	15
21	Mirroring of the work area during a web conference	1	5	2	10	1	5
22	Fees for telework environment	1	5	2	10	1	5
23	Inadequate communication rules in a telework environment	3	1	2	6	1	3
24	Increase in water and electricity costs due to working in a telework environment	3	5	3	45	1	15
25	Mail delivered to the office addressed to a teleworking employee	3	1	2	6	1	3
26	Inadequate labor management in telework	3	5	3	45	1	15
27	Increase in overtime hours in telework	3	5	3	45	1	15
28	Increasing Web Conferencing in Telework	3	1	2	6	1	3
				Risk value (total)	**548**	Risk value (total)	**214**

Table 7 shows the percentage of reduction in risk values after implementing the countermeasures. As we can see, the overall risk reduction was about 61%. This demonstrates that the proposed measures are effective despite the fact that the risk value is a relative measure.

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

Table 7: Percentage of reduction in risk value.

	Before risk countermeasures (1)	After risk countermeasures (2)
Risk value (total)	548	214
Risk value reduction rate = ((1)-(2))/ (1)	—	0.61

5 PORTFOLIO OF RISK COUNTERMEASURES FOR TELEWORK

In this section, the risk measures for teleworking presented in Section 4 (Tables 2-4) are evaluated from a practical perspective. In general, from a practical perspective, prioritization of risk measures should be considered from a cost perspective. In this paper, we apply a portfolio approach to prioritization, as a portfolio of risk countermeasures for teleworking allows for stepwise risk countermeasures.

5.1 Application of Portfolio Management

It is generally reasonable to implement risk countermeasures in stages, taking cost-effectiveness into consideration. This paper proposes a portfolio of risk countermeasures (priorities) based on the Computer Security Incident Response Team (CSIRT) risk countermeasure classification [26], [27]. For example, Proactive Service and Security Quality Management Service are categorized as proactive measures and have a higher priority than Reactive Service. In the proposed risk countermeasure portfolio, Proactive Service, Security Quality Management Service, and Reactive Service are clearly identified for each countermeasure so that countermeasures can be introduced step by step.

We reorganized the risk measures in Tables 2–4 on the basis of the hierarchical perspective shown in Table 1. Specifically, the portfolios were classified into 1) environmental aspects on the employee side, 2) cybersecurity aspects on the employee side, 3) non-cybersecurity aspects on the employee side, and 4) internal institutional aspects on the company side. The results are presented below.

5.2 Risk Countermeasure Portfolio of Employee Side

5.2.1 Environmental Aspect

In the portfolio of proposed risk countermeasures for environmental aspects on the employee side, Nos. 1 and 2 in Table 8 were countermeasures for the creation of procedure manuals and employee education to combat the lack of proficiency in telework tools (e.g., remote desktop and web conferencing tools), and since these measures are continuous, they were classified as Security Quality Management Service. Nos. 3 and 5 were classified as Proactive Service because they are proactive measures for the maintenance of the network environment, which is indispensable for teleworkers. As for Nos. 4, 6, and 7, they were classified as Reactive Service, which are post-measures, because they are factors that are not essential for some people (e.g., a lack of fixtures such as printers and an independent telework environment).

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

Table 8: Environmental aspects on employee side.

No.	Risk Factor	Risk Countermeasures	Pre	Post	Quality
1	Lack of proficiency with tools such as Remote Desktop	Create procedures for work and communication tools based on the company's security policy, and educate employees about the rules on a regular basis.			○
2	Lack of proficiency with communication tools such as web conferencing				○
3	Insufficient bandwidth in the network environment	Data dieting (e.g., limiting video and audio for web conferencing when bandwidth is insufficient) is performed as necessary.	○		
4	Lack of printers and other fixtures	Establish a system for companies to pay for the construction of telework environments.		○	
5	Vulnerability of telecommunication devices for telework	Keep telework communication device software up to date. Manage the access log.	○		
6	Lack of independent telework environment	Establish a system for companies to pay for the construction of telework environments.		○	
7	Health hazards such as economy class syndrome	Companies should develop labor management for teleworkers and ensure that they have time for health care.		○	

5.2.2 Cybersecurity Aspects

In the portfolio of proposed risk countermeasures in terms of cybersecurity on the employee side, which is shown in Table 9, all the proposed risk countermeasures (Nos. 13–17) were classified as Security Quality Management Service, since they require continuous countermeasures such as employee training, the introduction of MDM to company-rented terminals, VPN, and use of cloud computing.

Table 9: Cybersecurity aspects on employee side.

No.	Risk Factor	Risk Countermeasures	Pre	Post	Quality
13	File-sharing mistakes	Create telework work standards based on the company's security policy, and educate employees about them. Specifically, prohibit the use of terminals other than those loaned by the company or those authorized (e.g., MDM-implemented terminals), and require the use of remote VPN or cloud computing for BYOD and other non-company loaned terminals.			○
14	Unauthorized access				○
15	Computer virus				○
16	Use of outdated security software				○
17	Installation of unnecessary software				○

5.2.3 Non-Cybersecurity Aspects

In the portfolio of proposed risk countermeasures for non-cybersecurity aspects on the employee side, as shown in Table 10, Nos. 8, 10, 12, 18, 20, and 21 are risk countermeasures such as the creation of telework work standards based on the company's security policy and training for employees based on these standards. Therefore, they were classified as Security Quality Management Service. Numbers 9 and 11 were classified as Proactive Service because they are risk countermeasures against the loss of company-issued terminals and the provision of mobile Wi-Fi, which are essential for telework. As for No. 19, it is a countermeasure against loneliness during work, and was classified as a Reactive Service because it depends on the personality of the employee; an example here is the construction of a communication environment to mitigate loneliness during work due to the lack of a face-to-face partner.

Table 10: Non-cybersecurity aspects on employee side.

No.	Risk Factor	Risk Countermeasures	Pre	Post	Quality
8	Shoulder hacking into PC screen in a telework environment	Create telework work standards based on the company's security policy and educate employees about the rules on a regular basis.			○
9	Loss of corporate terminal for telework	MDM should be implemented for company-leased terminals, and encryption should be required when storing data; for non-company-leased terminals (e.r., BYOD), remote VPN and cloud computing should be required.	○		
10	Use of shared home terminals	Based on the company's security policy, create telework work standards, such as prohibiting the use of terminals other than company-loaned terminals and authorized terminals, and educate employees about them.			○
11	Use of free Wi-Fi, etc.	Companies can set up a system to pay for the construction of a telework environment and lend mobile Wi-Fi to their employees.	○		
12	No face-to-face surveillance possible	Companies should establish a working environment for telework and require employees to report on the progress of their work on a regular basis.			○
18	Internal fraud	Create telework work standards based on the company's security policy, and educate employees on a regular basis.			○
19	Lack of a face-to-face partner (loneliness while working)	Provide a virtual environment where companies can develop a labor environment for telework and enable employees to communicate with each other.		○	
20	Leakage of images and conversations of non-related parties during a web conference	Create telework work standards based on the company's security policy and educate employees about them.			○
21	Mirroring of work area during a web conference	Establish a system in which companies pay for the construction of a telework environment.			○

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

5.3 Risk Countermeasure Portfolio of Company Side

5.3.1 Internal Institutional Aspects

In the portfolio of proposed risk countermeasures in terms of the company's internal systems, all of the proposed risk countermeasures (Nos. 22–28 in Table 11) include training for employees and formulation of systems, which are essential for telework, so they were classified as proactive measures in the Security Quality Management Service.

Table 11: Internal institutional aspects on company side.

No.	Risk Factor	Risk Countermeasures	Pre	Post	Quality
22	Fees for telework environment	Establish a system in which companies pay for the construction of a telework environment.			○
23	Inadequate communication rules in telework environment	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.			○
24	Increase in water and electricity costs due to working in telework environment	Establish a system in which companies pay for the construction of telework environments.			○
25	Mail delivered to the office addressed to a teleworking employee	Create telework work standards based on the company's security policy and educate employees about them.			○
26	Inadequate labor management in telework	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.			○
27	Increase in overtime hours in telework	Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.			○
28	Increase in web conferencing in telework				○

5.4 Summary

To form the portfolio of risk countermeasures for telework, the countermeasures were hierarchically reorganized and clustered into four categories: 1) environmental aspects on the employee side, 2) cybersecurity aspects on the employee side, 3) non-cybersecurity aspects on the employee side, and 4) internal institutional aspects on the company side. Using the classification of CSIRTs as a basis, we examined the proposed phased introduction of risk countermeasures.

As a result, 24 out of the 28 countermeasure proposals were classified as proactive service and security quality management service, which demonstrates the importance of proactive measures in the introduction of telework. In particular, we clarified which measures are essential when introducing telework, such as the construction of an Internet environment, the introduction of MDM for company-rented terminals, and the use of VPNs and cloud computing. We also demonstrated the necessity of continuing the use of teleworking tools, security education, and the development of in-house systems even after the introduction of teleworking.

6 CONCLUSION AND FUTURE WORK

In this paper, we conducted a risk assessment of telework based on the perspectives of both companies and employees in order to utilize telework permanently, safely, and securely in the new normal era. Specifically, we comprehensively extracted 28 risk factors using the RBS method, analyzed them, and proposed countermeasures. Our analysis revealed eight risk factors in the Risk Avoidance category, 12 in Risk Transference, eight in Risk Mitigation, and zero in Risk Acceptance. Thus, measures based on Risk Transference accounted for about half of the total. Our findings clarified that the most important thing is to strengthen the operational aspect of telework, i.e., to establish a telework system based on the company's security policy. The effectiveness of the proposed risk countermeasures was also demonstrated through an evaluation by risk values, where we found that the risk value after implementation of the countermeasures

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

was reduced by approximately 61%. Finally, we created a portfolio to identify the priorities of the proposed risk countermeasures in terms of practical applicability. We also clarified the advantages of the phased introduction of the proposed risk countermeasures with reference to the classification of CSIRTs. Overall, our findings should contribute to the safe and secure operation of telework from the viewpoint of practical operability.

Our future work will investigate the implementation of risk assessment based on the management's viewpoint, in contrast to the risk assessment based on the employee's viewpoint in the present study.

Acknowledgement

This work was supported by JSPS KAKENHI Grant Number JP 19H04098.

References

[1] Y. Ide, "A case of office work (Telework)", Ergonomics, Vol. 55 Supplement Issue, S2F2-4, Japan Human Factors and Ergonomics Society, 2019(Japanese Edition)

[2] T. Kamei, et al., "Challenges and prescriptions for reforming work styles through telework", Knowledge of Asset Creation, July 2017 issue, pp.36-49, NRI, 2017, (Japanese Edition)

[3] Ministry of Internal Affairs and Communications, "2019 Report on the Survey of Telecommunications Usage Trends (Enterprise Edition)", 2019, https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201900_002.pdf, (accessed 2022/05/26), (Japanese Edition)

[4] Ministry of Health, Labor and Welfare, "Telework Portal Site Overseas Initiatives", https://telework.mhlw.go.jp/telework/abr/, (accessed 2021/03/04) , (Japanese Edition)

[5] M. Furuya, "World telework situation 2012", Japan Telework Society, The 13th Academic Salon, https://www.mlit.go.jp/crd/daisei/telework/docs/H24b_06.pdf, (accessed 2021/03/04), (Japanese Edition)

[6] Ministry of Internal Affairs and Communications, "Realizing a comfortable workplace through telework", 2021, https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201900_002.pdf, (accessed 2022/05/26), (Japanese Edition)

[7] T. Gentle, "Insider Threat Risk Assessment and Telework", ED-520: Foundations of Insider Threat Management, https://securityawareness.usalearning.gov/cdse/itawareness/documents/TorielloK-NITAM-Essay.pdf, (accessed 2022/05/26), 2021

[8] Y. Huiyi, et al., "Security Risks in Teleworking: A Review and Analysis", The University of Melbourne, https://minerva-access.unimelb.edu.au/items/c37178db-9b3c-5ff6-89b9-8f264b789555, (accessed 2022/05/26), 2013

[9] P. Pyoria, "Managing telework: risks, fears and rules", Management Research Review, Vol. 34 No. 4, pp. 386-399.,2011

[10] S.Desio, et al., "Telework and its effects on mental health during the COVID-19 lockdown", European Review for Medical and Pharmacological Sciences, 25, pp.3914-3922, 2021

[11] A. M. Luchena, et al., "Telework and Social Services in Spain during the COVID-19 Pandemic", Int. J. Environ. Res. Public Health 2021, 18, 725, 2021

[12] S. Frosdick, "The techniques of risk analysis are insufficient in themselves", Disaster Prevention and Management, Disaster Prevention and Management, Vol. 6, No. 3, pp. 165–

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.

177, 1997
[13] Project Risk Coach, How to Use the Delphi Technique, https://projectriskcoach.com/delphi-technique/, (accessed 2023/09/04)
[14] RRC Training, Fault Tree Analysis (FTA) and Event Tree Analysis (ETA), https://www.icao.int/sam/documents/2014-adsafass/fault%20tree%20analysis%20and%20event%20tree%20analysis.pdf, (accessed 2023/09/04).
[15] Manick, "Risk Breakdown Structure", http://www.justgetpmp.com/2011/12/risk-breakdown-structure-rbs.html, (accessed 2022/05/22)
[16] M. Rasool, et al., Methodology and tools for risk evaluation in construction projects using Risk Breakdown Structure, European Journal of Environmental and Civil Engineering, 16:sup1, s78-s98, DOI: 10.1080/19648189.2012.681959, 2012
[17] Sky , "Awareness Survey on Telework", https://www.skygroup.jp/news/201019_01/, (accessed 2021/03/04) , (Japanese Edition)
[18] The Tokyo Chamber of Commerce and Industry, Issues that arose when implementing telework, 2021, (Japanese Edition)
[19] H. Koyama, et al., "Risk Assessment of Telework for the New Normal Era", 2021 IEEE 10th Global Conference on Consumer Electronics, pp.573-574, 2021
[20] H. Koyama, et al., "A Study of Risk Assessment Quantification for Secure Telework," 2022 11th International Congress on Advanced Applied Informatics (IIAI-AAI), pp.574-580, 2022
[21] S. Tanimoto, et al., "Risk Assessment of BYOD: Bring Your Own Device", 2016 IEEE 5th Global Conference on Consumer Electronics, pp.511-514, 2016
[22] SCRIBD, "ISMS Risk Assessment Manual v1.4", https://www.scribd.com/document/202271054/ISMS-Risk-Assessment-Manual-v1-4, 2015
[23] H. Sato, et al., "Information Security Infrastructure", Kyoritsu Shuppan Co., Ltd., pp.29-32, 2010, (Japanese Edition)
[24] S. Tanimoto, et al., "A Study of Risk Assessment Quantification in Cloud Computing", 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp. 426-431, 2014
[25] S. Tanimoto, et al.," Risk Assessment Quantification of Ambient Service", ICDS 2015 : The Ninth International Conference on Digital Society, pp. 70-75, 2015
[26] J. Wiik, et al., Effectiveness of Proactive CSIRT Services, In 18th Annual FIRST Conference on Computer Security Incident Handling, 2006
[27] Y. Kenmoku, et al., A Study of Assurance Level in Information Security Management - LoA Introducing Method for CSIRT Deployment -, 6th International Conference on Project Management (ProMAC 2012), 2012

Copyright © by IIAI. Unauthorized reproduction of this article is prohibited.