GB

GUIDANCE TECHNICAL DOCUMENTS ON

STANDARDIZATION OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/Z 24364-2009

Information security technology - Guidelines for information security risk management

信息安全技术 信息安全风险管理指南

Issued on: September 30, 2009 **Implemented on: December 01, 2009**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine of PRC;

Standardization Administration of PRC.

Table of Contents

Information security technology - Guidelines for information security risk management

1 Scope

This guidance technical document defines the content and process of information security risk management, provides guidance for the information security risk management at different stages of the information system's life cycle.

This guidance technical document is intended to guide organizations in the management of information security risks.

2 Normative references

The provisions in following documents become the provisions of this guidance technical document through reference in this guidance technical document. For the dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this guidance technical document; however, parties who reach an agreement based on this guidance technical document are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB 17859-1999 Classified criteria for security protection of computer information system

GB/T 18336.2-2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements (ISO/IEC 15408-2:2005, IDT)

GB/T 20984-2007 Information security technology-Risk assessment specification for information security

GB/T 22081-2008 Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005, IDT)

3 Terms and definitions

The following terms and definitions apply to this guidance document.

3.1

uncertainties that may affect system resources.

3.7

Risk treatment

The process of selecting and implementing actions to change the risk.

[GB/T 22081]

4 Overview of information security risk management

4.1 Scope and objects of information security risk management

The concept of information security covers the security of information, information carriers, information environment. Information refers to the data and files as collected, processed, stored in the information system. The information carrier refers to the medium that carries the information, that is, the entity used to record, transmit, accumulate, save information. The information environment refers to the environment in which information and information carriers are located, including hard environments and soft environments such as physical platforms, system platforms, network platforms, application platforms.

Information security risk management is risk-based information security management, that is, information security management is always based on risk. Conceptually, information security risk management shall address all relevant objects contained in the above three aspects of information security (information, information carrier, information environment). However, for a specific information system, information security risk management may mainly involve the key and sensitive parts of the information system. Therefore, according to the actual information system, the focus of information security risk management, that is, the scope of risk management selection and the focus of the object shall be different.

4.2 Content and process of information security risk management

Information security risk management includes six aspects: background establishment, risk assessment, risk management, approval supervision, monitoring review, communication-consultation. Background establishment, risk assessment, risk management, approval supervision are the 4 basic steps of information security risk management. Monitoring review and communication-consultation are carried out in these 4 basic steps, as shown in

environmental changes.

In clauses 5 ~ 10 of this guidance technical document, it describes the concepts, processes, work contents, output documents of the above 6 steps of the implementation process of information security risk management.

4.3 Relationship between information security risk management and information system's life cycle and information security objectives

4.3.1 Information system's life cycle

The information system's life cycle is the whole process of an information system growing from nothing to developed, then to abandonment, which includes 5 basic stages of planning, design, implementation, operation-maintenance, abandonment.

In the planning stage, it determines the purpose, scope, needs of the information system, analyzes and demonstrates the feasibility, propose an overall plan. In the design stage, according to the overall plan, it designs the implementation structure of the information system (including functional division, interface protocol, performance indicators, etc.) and implementation plan (including implementation technology, equipment type selection, system integration, etc.). In the implementation stage, according to the implementation plan, it purchases and tests equipment, develops custom functions, integrates, deploys, configures, tests the systems, trains personnel and so on. In the operation-maintenance stage, the operation and maintenance system ensures that the information system can always work and continuously upgrade during the change of its own and its environment. In the abandonment stage, it scraps the entire information system or the outdated or useless parts of the information system. When the business objectives and needs of the information system change, or otherwise when the technology and management environment change, it is necessary to re-enter the above 5 stages to form a new cycle. Therefore, planning, design, implementation, operation-maintenance, abandonment constitute a spiral-rising cycle that allows information systems to adapt to changes in themselves and the environment.

4.3.2 Information security objectives

The objective of information security is to achieve the basic security features of information systems (i.e., the basic attributes of information security) and to achieve the required level of assurance. The basic attributes of information security include confidentiality, integrity, availability, authenticity, non-

5 Background establishment

5.1 Overview of background establishment

5.1.1 Concept of background establishment

Background establishment is the first step of information security risk management. It determines the object and scope of risk management, establishes the preparation for implementing risk management, conducts investigation and analysis of relevant information.

5.1.2 Purpose of background establishment

The background establishment is to clarify the scope and objects of information security risk management, as well as the characteristics and security requirements of the objects, to plan and prepare the items of information security risk management, to ensure the smooth implementation of subsequent risk management activities.

5.1.3 Basis for background establishment

Relevant national, regional, industrial policies, laws, regulations, standards, as well as the business objectives and characteristics of information systems are essential for background establishment.

5.2 Process of background establishment

The process of background establishment includes 4 stages: risk management preparation, information system investigation, information system analysis, information security analysis. In the process of information security risk management, the process of background establishment is the beginning of a main cycle of information security risk management, which provides input for risk assessment, monitoring review, communication-consultation throughout its 4 stages, as shown in Figure 3.

6 Risk assessment

6.1 Overview of risk assessment

6.1.1 Concept of risk assessment

Risk assessment is the second step in information security risk management. It identifies, analyzes, evaluates the risks faced by established risk management objects.

This clause only provides a framework description for risk assessment. The details may be found in GB/T 20984.

6.1.2 Purpose of risk assessment

Information security risk management relies on the results of risk assessment to determine subsequent risk management and approval supervision activities. Risk assessment enables organizations to pinpoint risk management strategies, practices, tools, focuses security activities on important issues, selects cost-effective and applicable security countermeasures. Risk management methods based on risk assessment have proven to be effective and practical, which have been widely used in various fields.

6.1.3 Scope of risk assessment

Risk assessment only provides a direction for information security activities, it does not lead to significant improvements on information security. Regardless of how detailed and multi-disciplined the assessment method is, it can only describe the risk status, without improving the security status of the organization. Only by using the assessment results to continuously perform improvement activities and achieve effective risk management, can the organization improve the security status.

6.2 Risk assessment process

The risk assessment process includes 4 stages: risk assessment preparation, risk factor identification, risk analysis, risk outcome determination. In the process of information security risk management, accepting the output of the background establishment, providing input for risk processing, monitoring review, communication-consultation are throughout its 4 stages, as shown in Figure 8.

The main risk treatment methods include 4 types: avoidance, transfer, reduction, acceptance.

a) Avoidance method: Avoid risks by not using assets at risk. For example, in an information system that does not have sufficient security, it does not process particularly sensitive information, thus preventing the leakage of sensitive information. For another example, for an information system that only processes internal businesses, the Internet is not used, thereby avoiding external harmful intrusions and bad attacks.

b) Transfer method: Avoid or reduce risk by transferring assets at risk or their value to a secure place. For example, when the organization does not have sufficient technical capability for security assurance, the technical system of the information system (i.e., the information carrier part) is outsourced to a third-party organization that meets the security requirements, thereby avoiding technical risks. For another example, by insuring expensive equipment, transfer the risk of equipment loss to the insurance company, thereby reducing the loss of asset value.

c) Reduction method: Reduce risk by taking protective measures against assets at risk. Protection measures can reduce risk from 5 aspects that constitute a risk (i.e., threat sources, threat behavior, vulnerability, assets, impact). For example, use legal means to sanction computer crimes (including stealing confidential information; attacking critical information system infrastructure; spreading viruses, unhealthy information, spam, etc.), play a deterrent role of law, thereby effectively curbing the motives of threat sources. Use the ID certification measures to resist the ability of identity to impersonate this threatening behavior. Patch the system in time (especially for patch for security vulnerabilities); close useless network service ports, thereby reducing system vulnerability and reducing the possibility of being exploited. Take various protective measures to establish an asset security domain, to ensure that assets are not infringed and their value is maintained. Take measures such as disaster recovery backup, emergency response, business continuity planning, thereby reducing the impact of security incidents.

d) Acceptance method: Accepting the risk is to choose not to take further measures against the risk and accept the consequence of risk. The premise of not treat risks is to determine the risk level of the information system, assess the occurring possibility of the risk and the potential damage, analyze the feasibility of using each management measure, carry out more comprehensive cost-effectiveness analysis, thereby determining that some functions, services, information, or assets do not require further protection.

8 Approval supervision

8.1 Overview of approval supervision

8.1.1 Concept of approval supervision

Approval supervision is the fourth step of information security risk management, including approval and continuous supervision. Approval means that the decision-making level of the organization makes decision on whether to recognize the risk management activities based on whether the results of risk assessment and risk treatment meet the security requirements of the information system. The continuous supervision refers to the inspection on whether the organization, its information system, information security-related environment have change, as well as the supervision on whether the changing factors may induce new security potentials and affect the security assurance level of the information system.

Approval shall be carried out by the decision-making level of the competent authority within the organization or at a higher level. Continuous supervision is usually done by the internal management level and the executive level of the organization; if necessary, it may also entrust the external professional organizations at the support level to provide support, depending on the nature of the information system and the professional competence of the organization itself.

8.1.2 Principles for approval supervision

The approval and continuous supervision of the results of risk assessment and risk treatment are not based on the rigid comparison process based on relevant standards, but rather on the business carried by the information system. It carries out relevant work based on the importance of business and the effects after the business is subjected to loss. There are two grounds for approval:

a) The residual risk of the information system is acceptable;

b) Security measures (including risk assessment and risk treatment) meet the security needs of the current business of the information system.

8.2 Process of approval supervision

The process of approval supervision includes 3 stages: application of approval, treatment of approval, continuous supervision. In the process of information security risk management, accepting the output of risk treatment is the end of an information security risk management activity. Monitoring review and

9 Monitoring review

9.1 Overview of monitoring review

9.1.1 Concept of monitoring review

The monitoring review monitors and reviews the 4 main steps of the information security risk management cycle, namely background establishment, risk assessment, risk treatment, approval supervision. Monitoring is monitoring and control. One is to monitor and control the risk management process, that is, the process quality management, to ensure the effectiveness of the process; the second is to analyze and balance the cost-effectiveness, that is, the cost-effective management, to ensure cost effectiveness. The review tracks changes in the protected system itself or in its environment, to ensure the validity and compliance of the results.

9.1.2 Significance of monitoring review

There are also risks associated with information security risk management activities. Supervision and review can timely identify problems such as changes, deviations, delays that have occurred or are about to occur, so as to take appropriate measures to control and correct them, thereby reducing the losses caused and ensuring the effectiveness of the main loop of information security risk management.

9.1.3 Contents of monitoring review

The monitoring review includes the following aspects and content:

a) Effectiveness of monitoring process:

1) Whether the process is executed completely and effectively;

2) Whether the output document is complete and the content is thorough.

b) Effectiveness of monitoring cost: Whether the execution cost is reasonable as compared to the results obtained.

c) Validity and compliance of the review results:

1) Whether the output results meet the security requirements of the information system;

2) Whether the output results are outdated due to changes in the information system itself or the environment.

Communication-consultation provide communication and consultation for relevant personnel in the 4 steps of the main cycle of information security risk management (i.e., background establishment, risk assessment, risk treatment, approval supervision). Communication is to provide communication channels for direct participants, to maintain coordination and achieve security goals. Consultation provides a learning pathway for all relevant people to improve risk awareness, knowledge and skills to meet security goals.

10.1.2 Significance of communication-consultation

In order to ensure the smooth and effective implementation of information security risk management activities, the coordination and consistency of relevant personnel actions and the mastery of relevant knowledge and skills are critical factors. Through unimpeded communication and full communication, the coordination and consistency of actions are maintained. Through effective training and convenient consultation, ensure that the action personnel have sufficient knowledge and skill, which is the meaning of communication-consultation.

10.1.3 Objectives of communication-consultation

Communication-consultation includes the following aspects and objectives:

a) Participant-oriented communication:

1) Communicate with decision-makers for understanding and approval;

2) Communicate with management levels and executive levels for understanding and collaboration;

3) Communicate with the support level to gain understanding and support;

4) Communicate with the user level to get understanding and cooperation.

b) Consultation with relevant personnel: Provide consultation and training for relevant personnel at all levels to improve personnel security awareness, knowledge, skills.

10.1.4 Methods of communication-consultation

The roles of the two sides of the communication-consultation are different and the methods adopted are different. See Table 1 for the division of roles and responsibilities of personnel involved in information security risk management. Table 11 shows the methods in which communication between different levels of personnel is conducted.

11 Information security risk management in the information system planning stage

11.1 Security objectives and security requirements

The security objective of the information system planning stage is to clarify the purpose of information system security construction, analyze and demonstrate the possibility of information system security construction, develop an overall security planning. In order to ensure the realization of the security objectives, it is necessary to conduct risk management on the links that may introduce security risks in the information system planning stage, thereby reducing the high cost of treating the same security risks in the later stages of the project.

The main security needs involved in the information system planning stage include:

a) Clarify the overall security policy;

b) Ensure that the overall security policy is derived from business expectations;

c) Clearly describe the security status of the systems involved;

d) Submit a clear security needs document;

e) Clarify and agree on risk assessment criteria;

f) Clearly describe the security implementation from which levels of the system;

g) Fully analyze and demonstrate the possibility of security implementation in system planning.

11.2 Process and activities of risk management

11.2.1 Overview of risk management process

According to the security objectives and security needs in the information system planning stage, the main risk management activities at this stage include: defining the overall policy on information system security, analysis of information system security needs, agreement on risk assessment criteria, argumentation analysis on the implementation of information system security, etc. Meanwhile in the above process, the monitoring review and communication-consultation are performed to ensure the realization of risk

3) Review the rationality of the monitoring review process.

c) Whether there is a special person to review and evaluate regularly according to a specific process:

1) Review the current risk management review process of the organization;

2) Review the re-inspection and adjustment plan;

3) Review whether it can ensure that any change of the security status of the system may enter into the review and assessment process, so as to modify the security policy in a timely manner and restore it to a security status which is acceptable by the organization.

d) Whether the scope of risk management is clear.

The above items need to be added or deleted according to the specific conditions of the information system. The review process for the overall security policy needs to be approved by the relevant departments of the information system.

11.2.3 Analysis of security needs

The security risks that may be introduced during the analysis process of security needs may be managed in the following ways:

a) It shall review the integrity, organization, clarity, etc. of the security needs analysis document;

b) It shall use the information security risk analysis methods to identify the shortcomings in the current security assurance system by conducting risk assessments on information systems.

In the above process, the lack of any process will bring a large deviation to the risk assessment results, so it shall pay attention to the comprehensiveness of the process and ensure the correct implementation of each process.

The review process for the security requirements analysis document needs to be approved and supervised by the relevant departments of the information system.

11.2.4 Agreement on risk assessment criteria

It may use the following methods to manage the security risks that may be introduced during the development process of risk assessment criteria:

a) It shall review the integrity, organization, clarity, etc. of the risk assessment criteria document.

12 Information security risk management in the design stage of information system

12.1 Security objectives and security needs

The security objective of the information system in the design stage is to design the implementation structure of information system security (including functional division, interface protocols, performance indicators, etc.) and implementation program (including realization technology, equipment type selection, system integration) according to the overall security planning program as output during the planning stage. When designing the realization structure and implementation program of the information system, it is easy to introduce security risks in many aspects such as technology selection, cooperation, management, etc. Therefore, for the critical links, it shall propose necessary security requirements and carry out pertinent security risk management.

The main security requirements for the information system in the design stage include:

a) The design scheme is in line with the system construction plan;

b) The security needs in the design scheme are in line with the security objectives in the planning stage;

c) Assess the effectiveness of the various technologies used to implement the security system;

d) The requirements for the level of security protection for the products used in the implementation program;

e) For self-developed software, security risks shall be fully considered during the design stage.

12.2 Processes and activities of risk management

12.2.1 Overview of risk management process

According to the security objectives and security needs of the information system in the design stage, the main risk management activities at this stage include: analysis and demonstration of security design scheme of information system, selection of security technology and security product, risk treatment of self-developed software, etc. Meanwhile in the above processes, use the

12.2.3 Selection of security technology

It may use the following methods to manage the security risks that may be introduced during the security technology selection process, to build a security assurance system which meets the requirements:

a) Refer to existing domestic and international security standards;

b) Refer to recognized security practices at home and abroad;

c) Refer to industry standards;

d) Expert committee's decision-making.

In the design stage of the project, it shall make full consideration of the degree to which the selected security technology can solve the problem, that is, the effectiveness of the technology selection. If the selection of technology is unreasonable, it will directly lead to the exposure of the corresponding security weaknesses, then the occurrence of security risks will be obvious.

The review process for the technology selection document needs to be approved and supervised by the relevant departments of the organization to which the information system belongs.

12.2.4 Type selection of security product

It may use the following methods to manage the security risks that may be introduced during the type selection process of security product:

a) Review whether it complies with relevant security standards;

b) Review whether it passes the certification of the relevant certification authority;

c) Review whether it meets the current level of security assurance;

d) Review the usefulness of the product;

e) Centralized testing;

f) Decision-making by expert meeting.

The reasonable degree of type selection of security products will directly affect the security defense effect required by the original design. Therefore, it must do a good job in the type selection of security products during the project design stage.

The review process for the product's type selection document needs to be approved and supervised by the relevant departments of the organization to

A system security test is a test of a specific part of a system that is developed or purchased and a test of the entire system, including:

a) Testing of security functions and security features of the purchased equipment and software, customized software and various parts of the system;

b) The overall security testing of the entire system after integration;

c) Testing of security management, physical facilities, personnel, processes, business or internal services (such as network services), contingency plans.

If new treatment measures are added during the development or procurement stage, they shall be retested. The security test can be implemented internally by the organization to which the information system belongs, or otherwise it may be implemented by hiring a third-party professional organization.

A test plan shall be developed prior to testing; it shall make records for the test process and test results.

13.2.3 Inspection and configuration

The purchased equipment, software, custom-developed software and systems shall be inspected and properly configured, including:

a) Check whether the purchased equipment and software have the production and sales licenses of the national authorities, whether they have passed the evaluation and certification by the relevant national authorities;

b) Check the security functions and security features of the purchased equipment and software, customized software and systems;

c) Follow the product specifications and design specifications to properly configure equipment, software, systems, to ensure compliance with design requirements.

If new security measures are added during the implementation of the system, it shall also analyze the risks brought to the original system by the newly added measures, to ensure that the added measures are coordinated and consistent with the original design.

13.2.4 Personnel training

The training targets include system users, system maintenance personnel, security management personnel. The training process is an important manifestation of communication-consultation. The training contents include:

then the approval of the information system is denied. For systems that are denied for operation, the information system's owner shall communicate with the authorized administrators and other related parties, to re-establish risk treatment measures and improvement plans, to reduce the security risk of the information system to an acceptable level, then conduct authorization of approval.

14 Information security risk management in the operation-maintenance stage of information systems

14.1 Security objectives and security needs

The security objective of the information system in the operation-maintenance stage is, after the information system is authorized to put into operation, to ensure the normal operation and security of the system during the operation and when the information system or its operating environment changes.

The security needs of the information system in the operation-maintenance stage include:

a) Without any change in the information system, maintain the normal operation of the system and perform daily security operation and security management;

b) In the event of changes in the information system and its operating environment, conduct risk assessment and develop risk treatment measures;

c) Conduct risk reassessment on a regular basis, to maintain the continued security of the system;

d) Regular re-approval of the information system, to ensure the time validity of the system authorization.

In the operation-maintenance stage, the main objective of risk management is to ensure that the above security needs have been achieved.

14.2 Processes and activities of risk management

14.2.1 Overview of risk management process

According to the security objectives and security requirements in the operation-maintenance stage of the information system, the main risk management

operations shall also be carried out on a regular basis, to ensure that the system authorization maintains time validity.

14.2.2 Security operation and management

After the information system starts to operate, it shall, according to the system operating requirements, operation requirements, management requirements as defined by the treatment measures, perform security operation and security management, to ensure the realization of the security functions of the system. Examples of security operations and management include performing backups, conducting training sessions, managing keys, updating user management and access privileges, updating security software, etc.

14.2.3 Change management

When the information system and its operating environment change, it shall assess their risks, develop and implement appropriate measures to control the risk. Change management includes the following aspects:

a) Changes to information systems: including system upgrades, adding new functions, discovering new system threats and vulnerabilities;

b) Changes in system's operating environment: including the hard environment of the system, changes in the soft environment, changes in the legal and regulatory environment.

When the information system and its operating environment change, it shall implement the risk assessment process and risk treatment process in the risk management process, analyze the new risks that may arise, develop and implement the treatment measures to deal with the risks.

Change management is mainly used when the information system and its operating environment change little. Change management does not require re-authorization of system operation.

14.2.4 Risk reassessment

Risk reassessment is the process of reassessing the risk of the system. It shall carry out risk reassessment of the system at regular basis. When major changes occur in the information system and its operating environment, it shall also carry out risk reassessment at appropriate time. The cycle of regular risk assessment shall generally be one year and the maximum shall not exceed two years.

After the risk reassessment, it shall perform the risk treatment process, to develop and implement the treatment measures for the risks.

14.2.5 Re-approval

3	Risk assessment of obsolescence process	Risk treatment
4	Review after obsolescence	Approval supervision

15.2.2 Determination of obsolescence object

After the information system has been in operation and use for a period of time, some or all of the system may no longer be needed. At this point, the obsoleted parts need to be analyzed to determine which parts of the system need to be obsoleted. The consideration range of the obsoleted objects includes obsoleted information, hardware, software, entire system.

It shall develop a list of obsoleted objects and identify it.

15.2.3 Risk assessment of obsoleted objects

The risk assessment of an obsoleted system shall mainly consider the security requirements of the obsoleted information, hardware, software, analyze the threats and vulnerabilities caused by the obsoleted system, assess the possible impact and possibility of unsafe obsolescence.

The security requirements of the obsoleted system shall be based on the confidentiality, integrity, availability of the original system, focusing on considering the confidentiality requirements of the obsoleted information and system, to ensure that sensitive information will not be leaked.

15.2.4 Risk treatment in obsolescence process

The risk treatment of the obsolescence process shall consider establishing a safe disposal procedure for the obsoleted system. It may consider the following treatment measures:

a) Media which contains sensitive information shall be safely stored or disposed of in a secure manner, such as incineration or debris, or used for other purposes within the organization after data is cleared.

b) Collect all the media for secure disposal may be easier than trying to isolate sensitive items.

c) Many organizations provide services for the collection and disposal of documents, equipment, media. Care shall be taken to select an appropriate contractor with sufficient treatment measures and experience.

d) If possible, the disposal of sensitive items shall be recorded, in order to maintain an audit trail.

when stacked media are waiting for centralized disposal, it shall consider the aggregation effects, i.e., a large amount of unclassified information which is stacked together may be more sensitive than a small amount of classified

Appendix A

(Informative)

Risk treatment reference model and its needs and measures

A.1 Risk treatment reference model

Risk treatment may, according to the evolutionary route, make reference to the following models: the traditional security protection treatment model, the PDR model, the P2DR model, the P2DR2 model, which are described as follows:

a) Traditional security protection treatment model. The method performs audit analysis on the information system, formulates corresponding security policies, adopts certain security protection measures. The premise of adopting this model is to ensure the correct setting of information systems, relatively complete defense methods, relatively fixed threats and weaknesses. It is suitable for networks or information systems with small scale and relatively no dynamic changes in security elements, without the need for detection and response mechanisms.

b) PDR model. This risk treatment model includes three processes: protection, detection, response. The time requirements for the three are met: Dt + Rt < Pt, where Dt is the time it takes for the system to detect a network attack or intrusion, Rt is the time from the detection of intrusion of the information system to the point when the system makes sufficient response, Pt is the effective protection time for the system to set various protection measures, that is, the time required for the external intrusion to achieve the purpose of infringing the security target. This model emphasizes the time requirements for PDR behavior; it may not include the development of risk analysis and related security strategies.

c) P2DR model. On the basis of the PDR model, use the audit analysis of the system to obtain a security policy throughout the PDR process, to form a dynamic security treatment loop system of security audit, policy, protection, detection, response.

d) P2DR2 model. The PPDRR model is a typical, well-recognized security treatment model. It is a dynamic and self-adaptive security treatment model that adapts to continuous change of security risk and security needs, provides ongoing security assurance. The PPDRR model includes 5 main parts: policy, protection, detection, response, recovery. Protection, detection, response, recovery constitute a complete and dynamic security cycle, which, under the guidance of the security policy, jointly achieves

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------