TC 68

TECHNICAL REPORT

ISO/TR 13569

First edition
1996-11-15

Banking, securities and other financial services — Information security guidelines

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Banque, valeurs mobilières et autres services financiers — Lignes directrices pour la sécurité de l'information

ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-10977ef8a5df/iso-tr-13569-1996

Reference number
ISO/TR 13569:1996(E)

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-1097e18a5df/iso-tr-13569-1996

© ISO 1996
All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.
International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-1097c8a5dfac/iso-tr-13569-1996

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-10977ef8a5df/iso-tr-13569-1996

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 13569, which is a Technical Report of type 3, was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 2, *Strategy, security and general operations*.

ISO/TR 13569:1996
10977ef8a5df/iso-tr-13569-1996

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-10977ef8a5df/iso-tr-13569-1996

Banking, securities and other financial services — Information security guidelines

1 Introduction

Financial institutions increasingly rely on Information Technology (IT) for the efficient conduct of business.

Management of risk is central to the financial service sector. Financial institutions manage risk through prudent business practice, careful contracting, insurance, and use of appropriate security mechanisms.

There is a need to manage information security within financial institutions in a comprehensive manner.

This Technical Report is not intended to provide a generic solution for all situations. Each case must be examined on its own merits and appropriate actions selected. This Technical Report is to provide guidance, not solutions.

The objectives of this Technical Report are:

- to present an information security programme structure.
- to present a selection guide to security controls that represent accepted prudent business practice.
- to be consistent with existing standards, as well as emerging work in objective and accreditable security criteria.

This Technical Report is intended for use by financial institutions of all sizes and types that wish to employ a prudent and commercially reasonable information security programme. It is also useful to providers of service to financial institutions. This Technical Report may also serve as a source document for educators and publishers serving the financial industry.

2 References

NOTE — Annex C contains references to national regulations, standards and codes. The list below includes only those documents referenced in the main body of this Technical Report.

International Standards:
ISO 8730:1990, *Banking - Requirements for message authentication (wholesale).*

ISO 8732:1988, *Banking - Key management (wholesale).*

ISO 9564-1:1991, *Personal Identification Number management and security - Part 1: PIN protection principles and techniques.*

ISO 9564-2:1991, *Personal Identification Number management and security - Part 2: Approved algorithm(s) for PIN encipherment.*

ISO 10126-1:1991, *Banking - Procedures for message encipherment (wholesale) - Part 1: General principles.*

ISO 10126-2:1991, *Banking - Procedures for message encipherment (wholesale) - Part 2: DEA algorithm.*

ISO 10202:1991-1996, *Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards* (all parts).

National Standards:
ANSI X9/TG-2, *Understanding and Designing Checks* (USA).

Regulations:
US Office of the Comptroller of the Currency, Banking Circular BC-226 Policy Statement.

Other documents:
Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing.

Code of Practice for Information Security Management.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9134-10977ef8a5ff/iso-tr-13569-1996

3 Executive summary

Financial institutions and their senior management have always been accountable for the implementation of effective controls for protecting information assets. The confidentiality, integrity, authenticity, and availability of that information are paramount to the business. As such, it is imperative that these assets be available and protected from disclosure, modification, fabrication, replication, and destruction, whether accidental or intentional. It is imperative for a financial institution to protect the transfer of its assets which are encoded in the form of trusted information.

Business depends more and more on computerized information systems. It is becoming impossible to separate technology from the business of finance. There is increasing use of personal computers and networks, and a greater need than ever for these to work together. In many institutions, more work is

done on personal computers and local area networks than on the large mainframes. Security controls for these local computers are not as well developed as controls over mainframes. The security needed for all information systems is growing dramatically. Image systems, digital voice/data systems, distributed processing systems, and other new technologies are being used increasingly by financial institutions. This makes information security even more important to the commercial success or even the survival of an institution.

Security controls are required to limit the vulnerability of information and information processing systems. The level of protective control must be cost effective, i.e., consistent with the degree of exposure and the impact of loss to the institution. Exposures include financial loss, competitive disadvantage, damaged reputation, improper disclosure, lawsuit, or regulator sanctions. Well thought out security standards, policies and guidelines are the foundation for good information security.

Work is ongoing within the US, Canada and the European Community to establish a Common Criteria for the evaluation of information technology products. These criteria coupled with financial sector pre-defined functionality classes will enable financial institutions to achieve uniform, trusted, security facilities. This guideline should be used as an input to that process.

With the continuing expansion of distributed information there is growing interest and pressure to provide reasonable assurance that financial institutions have adequate controls in place. This interest is demonstrated in laws and regulations. An excerpt from the US Office of the Comptroller of the Currency, Banking Circular BC-226 Policy Statement illustrates this concern.

> "It is the responsibility of the Board of Directors to ensure that appropriate corporate policies, which identify management responsibilities and control practices for all areas of information processing activities, have been established. The existence of such a 'corporate information security policy,' the adequacy of its standards, and the management supervision of such activities will be evaluated by the examiners during the regular supervisory reviews of the institution."

This Technical Report includes a guideline for building a comprehensive information security programme.

4 How to use this Technical Report

This Technical Report was designed to serve many purposes. This clause provides a "road map" to the remainder of the Technical Report.

Clause 5: Requirements: This clause defines a starting point in building a security programme. It sets out minimum requirements for an adequate information security programme. It may also serve as a measure against which an institution can evaluate the state of its information security programme.

Clause 6: Information security programme components: This clause contains more specific information on how an Information Security Programme should operate. Specific responsibilities are suggested for various officers and functions of an institution. Lines of communication between functions, that are considered helpful for sound security practice are identified. This clause can be used by senior officials to ensure that structural impediments to sound security practice are minimized. Information security personnel may also use this clause to evaluate the effectiveness of the information security programme.

Clause 7: Control Objectives and Suggested Solutions: This clause is the heart of this Technical Report. It discusses threats to information in terms specific enough to enable financial personnel to ascertain if a problem exists at their institution, without educating criminals. The first four subclauses address controls common to many delivery platforms: classification, logical access control, change control, and audit trails. Subsequent subclauses address security concerns for information processing equipment, human resources, and those specific to the delivery platform used. Electronic fund transfers and cheque processing subclauses finish this clause.

Clause 8: Sources of further help: This clause lists the types of organisations which may be of assistance to information security professionals. It is intended that this clause be used with Annex C.

Annex A: Sample Documents: This Annex is a collection of ready-to-use sample forms for a variety of information security related purposes.

Annex B: Privacy Principles: This Annex presents a sample set of Privacy Principles.

Annex C: Sources of Further Assistance: This annex lists the names and contact information for national organisations which can be of assistance to Information Security personnel.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-10977ef8a5df/iso-tr-13569-1996

5 Requirements

At the highest level, the acceptance of ethical values and control imperatives must be communicated and periodically reinforced with management and staff. Information is an asset that requires a system of control, just as do other assets more readily reducible to monetary terms. Prudent control over the information assets of the institution is good business practice.

The protection of information should be centred around the protection of key business processes. The notion of information and its attributes change within the context of a business process and security requirements should be examined at each stage of that process.

Developing, maintaining, and monitoring of an information security programme requires participation by multiple disciplines in the organisation. Close coordination is required between the business manager and the information security staff. Disciplines such as audit, insurance, regulatory compliance, physical security, training, personnel, legal, and others should be used to support the information security programme. Information security is a team effort and an individual responsibility.

The basic requirement of this technical guideline is the establishment of an information security programme that:

a. includes an institution-wide information security policy and statement, containing:

i. a statement that the institution considers information in any form to be an asset of the institution,

ii. an identification of risks and the requirement for implementation of controls to provide assurance that information assets are protected. Clause 7 of this Technical Report discusses suitable controls,

iii. a definition of information security position responsibilities for each manager, employee and contractor. Clause 6 of this Technical Report lists suggested responsibilities.

iv. a commitment to security awareness and education.

b. establishes one or more officer(s) responsible for the information security programme,

c. provides for the designation of individuals responsible for the protection of information assets and the specification of appropriate levels of security,

d. includes an awareness or education programme to ensure that employees and contractors are aware of their information security responsibilities,

e. provides for the resolution and reporting of information security incidents,

f. establishes written plans for business resumption following disasters,

g. provides identification of, and procedures for addressing exceptions or deviations from the information security policy or derivative documents,

h. encourages coordination with appropriate parties, such as audit, insurance, and regulatory compliance officers,

i. establishes responsibility to measure compliance with, and soundness of, the security programme,

j. provides for the review and update of the programme in light of new threats and technology. For example, the emergence of IT evaluation criteria should assist security professionals in the selection and implementation of standardized security controls,

k. provides for the production of audit records where necessary and the monitoring of audit trails.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc3-4604-9154-10977ef8a5df/iso-tr-13569-1996

6 Information security programme components

Subclause 6.1 addresses the information security responsibilities within the institution. Subclauses 6.2 and beyond address functions related to information security. The controls suggested in this Technical Report are those which enforce or support protection of information and information processing resources. While some of these controls may address other areas of bank governance, this Technical Report should not be viewed as a complete checklist of managment controls.

6.1 General duties

6.1.1 Directors

Directors of financial institutions have a duty to the institution and its shareholders to oversee the management of the institution. Effective information security practices constitute prudent business practice, and demonstrates a concern for establishing

the public trust. Directors should communicate the idea that information security is an important objective and support an information security programme.

6.1.2 Chief Executive Officer

The Chief Executive Officer, as the most senior officer of the institution, has ultimate responsibility for the operation of the institution. The CEO should authorize the establishment of, and provide support for, an information security programme consistent with recognized standards, oversee major risk assessment decisions, and participate in communicating the importance of information security.

6.1.3 Managers

Managers serve as supervisory and monitoring agents for the institution and the employees. This makes them key players in information security programmes. Each manager should:

- understand, support, and abide by institution's information security policy, standards, and directives,
- ensure that employees, vendors, and contractors also understand, support and abide by information security policy, standards, and directives, for example, the Code of Practice for Inforamtion Security Management,
- implement information security controls consistent with the requirements of business and prudent business practice,
- create a positive atmosphere that encourages employees, vendors, and contractors to report information security concerns,
- report any information security concerns to the Information Security Officer immediately,
- participate in the information security communication and awareness programme,
- apply sound business and security principles in preparing exception requests,
- define realistic business "need-to-know" or "need-to-restrict" criteria to implement and maintain appropriate access control,
- identify and obtain resources necessary to implement these tasks,
- ensure that information security reviews are performed whenever required by internal policy, regulations, or information security concerns.

Examples of circumstances that should trigger such a review include:

- large loss from a security failure,
- preparation of an annual report to the Board of Directors and Audit Committee,
- acquisition of a financial institution,
- purchase or upgrade of computer systems or software,
- acquisition of new communications services,
- introduction of a new financial product,
- introduction of new out-source processing vendor,
- discovery of a new threat.

Additionally, managers who are "owners' of information should:

- be responsible for the classification of information or information processing systems he controls.
- define the security requirements for his information or information processing systems.
- authorize access to information or information processing systems under his control.
- inform the Information System Security Officer of access rights and keep such access information up-to-date.

NOTE — All business information should have an identified "owner." A procedure for establishing ownership is required to ensure that all business information will receive appropriate protection.

6.1.4 Employees, vendors, and contractors should:

- understand, support, and abide by organisational and business unit information security policies, standards and directives,
- be aware of the security implications of their actions,
- promptly report any suspicious behavior or circumstance that may threaten the integrity of information assets or processing resources,
- keep each institution's information confidential. This especially applies to contractors and vendors with several institutions as customers. This includes internal confidentiality requirements, e.g. Chinese Walls.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9fc5-4604-9154-fa977ddd5df1/iso-tr-13569-1996

NOTE — Security programme components should be incorporated into service agreements and employees' employment contracts.

6.1.5 Legal function

Institutions may wish to include the following responsibilities for the legal department or function:

- monitor changes in the law through legislation, regulation and court cases that may affect the information security programme of the institution.

- review contracts concerning employees, customers, service providers, contractors, and vendors to ensure that legal issues relating to information security are addressed adequately.

- render advice with respect to security incidents.

- develop and maintain procedures for handling follow-up to security incidents, such as preservation of evidence.

6.1.6 Information Security Officers

For the purpose of this Technical Report, we define an Information Security Officer as the senior official or group of officials charged with developing, implementing, and maintaining the programme for protecting the information assets of the institution.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9f65-4604-9154-10977ef8a5df/iso-tr-13569-1996

The Information Security Officers should:

- manage the overall information security programme,

- have responsibility for developing Information Security Policies and Standards for use throughout the organisation. These policies and standards should be kept up-to-date, reflecting changes in technology, business direction, and potential threats, whether accidental or intentional,

- assist business units in the development of specific standards or guidelines that meet information security policies for specific products within the business unit. This includes working with business managers to ensure that an effective process for implementing and maintaining controls is in place,

- ensure that when exceptions to policy are required, the risk acceptance process is completed, and the exception is reviewed and reassessed periodically,

- remain current on threats against financial information assets. Attending information security meetings, reading trade publications, and participation in work groups are some ways of staying current with new developments,

- understand the current information processing technologies and the most current information protection methods and controls by receiving internal education, attending information security seminars and through on-the-job training

- apply management and organisational skills, knowledge of the business, and where appropriate, professional society recognition, in the execution of their duties,

- encourage the participation of managers, auditors, insurance staff, legal staff, and other disciplines that can contribute to information protection programmes,

- review audit and examination reports dealing with information security issues, and ensure that they are understood by management. The officer should be involved in the formulation of management's response to the audit findings and follow-up periodically to ensure that controls and procedures required are implemented within the stipulated time frames,

- confirm that the key threats to information assets have been defined and understood by management,

- assume responsibility or assist in the preparation and distribution of an appropriate warning of potentially serious and imminent threats to an organisation's information assets, e.g., computer virus outbreak. See clause A.6 for a sample warning,

- coordinate or assist in the investigation of threats or other attacks on information assets,

- assist in the recovery from attacks,

- assist in responding to customer security issues, including letters of assurance and questions on security. Although a letter of assurance is sent from the institution to the customer, it will often reflect the customer's desires rather than the institution's security policy.

6.1.7 Information Systems Security Administration

Each business unit and system manager must determine the need-to-know access privileges for users within their business sectors and communicate these documented privileges to the administrator. These access privileges should be reviewed periodically and changes should be made when appropriate.

Each information access control system should have one or more Information Systems Security Administrator(s) appointed to ensure that access control procedures are being monitored and enforced. Administrators should operate under dual control, especially for higher level privileges. These access control procedures are described in detail in 7.2.

The Information System Security Administration should:

- be responsible for maintaining accurate and complete access control privileges based on instructions from the information resource owner and in accordance with any applicable internal policies, directives, and standards,
- remain informed by the appropriate manager whenever employees terminate, transfer, take a leave of absence, or when job responsibilities change,
- monitor closely users with high-level privileges and remove privileges immediately when no longer required,
- monitor daily access activity to determine if any unusual activity has taken place, such as repeated invalid access attempts, that may threaten the integrity, confidentiality, or availability of the system. These unusual activities, whether intentional or accidental in origin, must be brought to the attention of the information resource owner for investigation and resolution,
- ensure that each system user be identified by a unique identification sequence (USERID) associated only with that user. The process should require that the user identity be authenticated prior to gaining access to the information resource by utilizing a properly chosen authentication method,
- make periodic reports on access activity to the appropriate information owner,
- ensure that audit trail information is collected, protected, and available.

The activities of the ISSA should be reviewed by an independent party on a routine basis.

6.2 Risk acceptance

Business Managers are expected to follow the institution's information security policy, standards and directives whenever possible. If the manager believes that circumstances of his particular situation prevent him from operating within that guidance, he should either:

- undertake a plan to come into compliance as soon as possible, or
- seek an exception based upon a risk assessment of the special circumstances involved.

The Information Security Officer should participate in the preparation of the compliance plan or exception request for presentation to appropriate levels of management for decision.

The Information Security Officer should consider changes to the information security programme whenever the exception procedure reveals situations not previously addressed.

While a complete treatment of risk management is far beyond the scope of this Technical Report, clause A.7 provides a sample risk acceptance form that identifies relevant factors in making risk acceptance decisions.

6.3 Insurance

In planning the information security programme, the Information Security Officer and business manager should consult with the insurance department and, if possible, the insurance carrier. Doing so can result in a more effective information security programme and better use of insurance premiums.

Insurance carriers may require that certain controls, called Conditions Prior to Liability or conditions precedent, be met before a claim is honored. Conditions Prior to Liability often deal with information security controls. Since these controls must be in place for insurance purposes, they should be incorporated into the institution's information security programme. Some controls may also be required to be warranted, i.e., shown to have been in place continuously since inception of the policy.

Business Interruption coverage and Errors and Omissions coverage, in particular, should be integrated with information security planning.

6.4 Audit

The following quotation from the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing defines the auditor's role as follows:

"Internal auditing is an independent appraisal function established within an organisation to examine and evaluate its activities as a service to the organisation. The objective of internal auditing is to assist members of the organisation in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analyses, appraisals, recommendations, counsel,

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/3055b978-9f65-4604-9154-10977ef8a5df/iso-tr-13569-1996

and information concerning the activities reviewed."

More specifically, in the area of information security, auditors should:

- evaluate and test controls over the information assets of a financial institution.
- engage in an on-going dialogue with Information Security Officers and others to bring appropriate perspectives to the identification of threats, risks, and the adequacy of controls for both existing and new products.
- provide management with objective reports on the condition of the control environment and recommend improvements that can be justified by need and cost benefit.
- specify retention and review of audit trail information.

Where the audit review function is combined with other functions, management attention is required to minimize conflict of interest potential.

6.5 Regulatory compliance

Regulatory authorities concern themselves principally with issues of safety, soundness, and compliance with laws and regulations. One element of safety and soundness is the institution's system of control that protect information from unavailability, and unauthorized modification, disclosure, and destruction.

Regulatory Compliance Officers should work with the Information Security Officer, business managers, risk managers, and auditors to ensure that information security requirements of regulations are understood and implemented. Regulatory Compliance Officers should also remain current on new technologies or methodologies which may become subject of regulation. For example, compliance with pre-defined functionality classes for Information Technology products.

6.6 Disaster recovery planning

An important part of an Information Security Programme is a plan to continue critical business in the event of a disruption. A disaster recovery plan outlines roles and responsibilities under those conditions.

Disaster recovery is that part of business resumption planning that ensures that information and information processing facilities are restored as soon as possible after interruption.

The disaster recovery plan should include the following:

- listing of business activities considered critical, preferably with priority rankings, including time frames adequate to meet business commitments,
- identification of the range of disasters that must be protected against,
- identification of processing resources and locations available to replace those supporting critical activities,
- identification of personnel available to operate processing resources or to replace personnel unable to report to the institution,
- identification of information to be backed up and the location for storage, as well as the requirement that the information will be saved for back-up on a stated schedule,
- information back-up systems capable of locating and retrieving critical information in a timely fashion,
- agreements with service suppliers for priority resumption of services, when possible.

The disaster recovery plan should be tested as frequently as necessary to find problems and to keep personnel trained in its operation. A periodic re-evaluation of the recovery plan to ascertain that it is still appropriate for its purposes should be undertaken periodically. A minimal frequency for both tests and reevaluations should be specified by the institution.

6.7 Information security awareness

The goal of a Security Awareness Programme is to promote information security. The programme is meant to influence, in a positive way, employees' attitudes towards Information Security. Security awareness should be addressed on an on-going basis. The success of any Information Security Programme is directly related to the Information Security Officer's ability to gain support and commitment from all levels of staff within the organisation. Failure to gain this support reduces the programme's effectiveness.

Without Management support, the information security programme cannot survive. Different levels of management and staff have different concerns. These concerns should be emphasized when addressing those various levels. Furthermore, presentations must be made in such a way that people of all levels and skills will be able to understand.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39550978-9f65-4604-9154-10977ef8a5df/iso-tr-13569-1996

Managers should be made aware of the exposure, risks and loss potential, as well as regulatory and audit requirements. This should be presented both in business terms and with examples pertinent to the manager's area of responsibility; positive messages being the most effective. Subclause 7.8 of this guideline examines these areas in more detail.

To function properly, the Information Security Programme must achieve a balance of control and accessibility. Both staff and management must be made aware of this. Users must be given access sufficient to perform their required job functions. They should never be given unrestricted access.

The Information Security Programme must support the work environment in which it exists. The Information Security staff must not operate in a vacuum. They must understand the business objectives as well as the internal operation and organisation of the institution to better protect and advise the institution. By acting in concert with other groups within the organisation, a cooperative spirit can evolve that will benefit everyone. In this way, security awareness will be promoted daily.

Lastly, to promote goodwill and support for the programme, Information Security staff members must be available to assist at all times.

6.8 External Service Providers

Financial institutions require that externally provided critical services, such as data processing, transaction handling, network service, and software generation, receive the same levels of control and information protection as those activities processed within the institution itself. The contract should include the elements necessary to satisfy the financial institution that:

- external service provider should in all cases abide by the security policies and standards of the financial institution.
- third party reports, i.e., the reports prepared by the service provider's own public accounting firm are made available.
- internal auditors from the financial institution be accorded the right to conduct an audit at the service provider relating to procedures and controls specific to the financial institution.
- the external service provider should be subject to Escrow agreements of delivered systems, products or services.

In addition to the above, an independent financial review of the provider should be conducted by specialists within the financial institution before engaging in a contract with a service provider.

No business should be transacted with a service provider unless a letter of assurance is obtained stating information security controls are in place. The Information Security Officer should examine the service provider's security programme to determine if it is in concert with the institution's. Any shortfall should be resolved either by negotiations with the provider or by the risk acceptance process within the institution.

In addition to information security requirements, contracts with service providers should include a non-disclosure clause and clear assignment of liability for losses resulting from information security lapses.

6.9 Cryptographic operations

Threats against confidentiality and integrity of information can be countered by appropriate cryptographic controls. Cryptographic controls such as encryption and authentication require that certain material, e.g., cryptographic keys, remain secret.

One or more facilities that generate, distribute, and account for cryptographic material may be required to support cryptographic controls. ISO standards on banking key management should be used wherever possible.

The facilities providing cryptographic material management should be subject to the highest level of physical protection and access control. Key management must be performed under split knowledge to preserve the security of the system.

Sound cryptographic practices and effective disaster recovery planning foster conflicting objectives. Close consultation between those responsible for disaster recovery and cryptographic support is imperative to ensure that neither function compromises the other.

Supply of cryptographic materials to customers should be done in a manner that minimizes the possibility of compromise. The customer should be made aware of the importance of security measures for cryptographic material. Interoperation with a customer's, correspondent's or service provider's cryptographic system should only be allowed under a fully documented letter of assurance.

The quality of security delivered by cryptographic products depends on the continued integrity of those products. Both hardware and software cryptographic products require integrity protection consistent with the level of security they are intended to provide. Use of appropriately certified integrated circuits, and anti-tamper enclosures, and key zeroizing make hardware systems somewhat easier to protect than software. When circumstances allow, software cryptographic products may be used. Features that enhance system integrity, such as self-testing, should be employed to the maximum degree feasible.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/39530998-9fc3-4604-9154-1897e8baadf/iso-tr-13569-1996

Cryptographic products are subject to varying governmental regulations as to use, import, and export. Local regulations on the use, manufacture, sale, export, and import of cryptographic devices vary widely. Consultation with local counsel or authorities is advised.

6.10 Privacy

Financial institutions possess some of the most sensitive information about individuals and organisations. Laws and regulations require that this information be processed and retained under certain security and privacy rules. Certain technical and business developments, such as networks, document imaging, target marketing, and cross-departmental information sharing, have led to concerns about the adequacy of banks' privacy protection.

Financial institutions should review all privacy laws and regulations, such as those involving credit information. Consideration should also be given to keeping current on emerging privacy legislation, either through bank law offices, bank industry sources, or other independent information sources. In addition, banks that have international operations need to be aware of European and other privacy laws and regulations that apply.

Financial institutions should review their operations to determine whether information on their customers and employees are adequately protected. Specific policies and procedures should be developed concerning how information is gathered, used, and protected. These policies and procedures should be made known to relevant employees. Privacy policies and procedures should address:

- collection of information to ensure that only relevant and accurate information is collected;
- processing of information to provide appropriate restrictions over access, including determinations of who should have access to information, quality control to avoid errors in data entry or processing, and protection against inadvertent unauthorized access;
- sharing of information, so that it occurs only through pre-determined procedures, that information is used for purposes relevant to the reasons for its original collection, and that such sharing does not lead to new opportunities for unauthorized privacy invasion by other parties;
- storage of information to ensure that it occurs in protected fashion to disallow unauthorized access;
- notification of information use and the availability of procedures that allow the person whose information is being held, to correct errors and to raise objections over the use of this information; and
- secure destruction of information when no longer needed.

In addition, electronic and other forms of employee monitoring must meet legal requirements that vary by jurisdiction. Worker monitoring is increasingly being viewed as a privacy issue and is undergoing court and legislative review. Privacy protection and due process rights need to be considered in addition to employer rights.

Financial institutions might consider developing a privacy audit. This audit evaluates how well the institution is achieving privacy protection and considers ways by which information technology can address privacy problems.

See Annex 2 for Basic Principles for Data Protection from the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

7 Control Objectives and Suggested Solutions

The controls listed in this clause are measures to ensure the availability of information and information processing resources, and to prevent unauthorized modification, disclosure, or destruction of information, whether intentional or accidental.

Subclauses 7.1 through 7.4 discuss four recurrent themes, that support many other controls:

- information classification,
- access control,
- audit trails, and
- change control.

The remaining parts of the clause discuss controls and their applicability, organized beginning with computers, networks, and software, followed by human factors, then moving to specific service platforms. A subclause on electronic fund transfers and a note on cheques complete this clause.

Each control appears with a brief statement of the primary control objective. It should be noted that many controls which are intended to prevent intentional abuse, are also useful against accidental harms. When the objective is relevant to the institution's line of business, it is recommended that the control listed be implemented whenever feasible. The actual decision to implement or not implement a control listed here will depend on the size and type of the institution as well as the institution's tolerance to risk, and regulatory requirements.

It is most important that the institution address all threats it faces. Controls, insurance, or formal

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 13569:1996
https://standards.iteh.ai/catalog/standards/sist/29550978-9b5-4604-9154-1697f6b45df/iso-tr-13569-1996