ICRC

INFORMATION SECURITY FRAMEWORK (ISF)

Security Management

October 2017

Approved by:
The ICRC Directorate
on 19 September 2017

Document Typology and Limitation

Document History

Version	Release date	Change summary
0.1	21.02. 2017	Information Security Framework was submitted and approved by the Information Security Board
0.2	June 2017	Information Security Framework new version is submitted and approved by the Director of Communication and Information Management
0.3	September 2017	Information Security Framework new version is submitted to the Directorate
1.0	October 2017	Information Security Framework final version is revised following recommendations from the Directorate

Executive summary

The Directorate of the International Committee of the Red Cross (ICRC) is fully aware that the security of the information and the information systems of the ICRC is essential to ensure the success of its operation around the world and to protect people's life, their physical and mental integrity, and their dignity.

To protect the information and the information systems against the multiple new threats appearing regularly, while complying with the interwoven mesh of regulations, the Directorate establishes a systematic and consistent approach which allows managing appropriately the related risks.

The Directorate fully endorses the Information Security Framework, as the organization's answer on top of which the ICRC builds and develops its informatiom security environment, taking in account three guiding principles:

- Confidentiality, to ensure that information is classified and handled in accordance with the Information Handling Typology rules and that no information is disclosed to unauthorized individuals or entities;
- Integrity, to maintain the accuracy and completeness of data over its entire life-cycle;
- Availability, to guarantee that authorized parties are able to access the information when needed.

These guiding principles constitute the heart of all the information security reference texts (policies, standards, etc.) which the ICRC implements and makes use of to manage effectively the information security in its activities.

The security of information and the information systems is not only granted by technologies or processes, it also includes people and their behavior. This document's purpose gives the opportunity to remind that:

- it is each and every staff member's responsibility to apply and abide to the ICRC existing rules;
- it is each and every manager's responsibility to make sure that ICRC staff adhere and act accordingly to the rules.

The Directorate delegates to the Information Security Board the mandate to ensure and improve the implementation of the Information Security Framework and all its related documents. The Information Security Board is responsible to escalate to the Directorate any decisions on security commitments impacting globally the institution.

Information Security Framework

Contents

Commitment and Rationale

Information is a key asset for the ICRC. It enables the ICRC to fulfill its mandate and accomplish its goals. It is vital to the smooth running of the organization.

The ICRC thus commits to protect ICRC information and information systems in order to protect its staff, beneficiaries, interlocutors and partners, to fulfill its mandate, to ensure business continuity, to guarantee the ICRC's confidential approach, and to comply with the ICRC Rules on Personal Data Protection, in the interest of the organization, the beneficiaries of its humanitarian services, its employees and partners.

While the ICRC cannot avoid information security incidents from occurring, it will take all reasonable measures to manage this risk, and ensure the confidentiality, integrity and availability of information and information systems, with the aim of preventing the occurrence of serious incidents and minimizing their impact on the organization. The Information Security Framework defines how the ICRC manages information security risks.

Information security is of everyone's responsibility. All staff are required to behave appropriately and comply with the existing rules and guidelines regarding information and information systems security

The management of information security risks is vital to protect internal staff, beneficiaries, interlocutors and partners. It is a key foundation to support ICRC operational activities and reputation, and notably the implementation of the ICRC policy on confidentiality (Doctrine 58) and ICRC Rules on Personal Data Protection.

The ICRC's confidential way of working is part of its identity[1] and implies the necessity to protect and secure to the extent possible all information relating to its activities. The ICRC Rules on Personal Data

[1] See the ICRC's confidential approach (DOCT 58), International Review of the Red Cross, No 887. The international community has recognized that the ICRC needs to protect its information relating to its activities to be able to fulfil its mandate (see article "Tools to do the job: The ICRC's legal status, privileges and immunities privileges and immunities of the ICRC", International Review of The Red Cross, No 897/898)

Protection[2] require an appropriate degree of security for the processing of personal data[3]. This relates in particular to access rights to databases, physical security, computer security or cybersecurity, the duty of discretion and the conduct of staff.

Being able to rely on available and relevant information is also one of the seven security pillars that allows the ICRC to reduce to the extent possible the inherent security risks it faces in its daily work.

The importance of protecting information and information systems is thus vital to avoid misuse, unauthorized access or disclosure of sensitive personal data and confidential information that can threaten the security of internal staff, beneficiaries or other persons to whom the information relates.

Information security incidents can have other far-reaching consequences for the organization such as disruption of operations and support functions affecting business continuity, financial losses in case of fraud or lawsuits by affected individuals and companies, failure to comply with the ICRC's legal obligations, as well as reputational damage and loss of trust among its staff, beneficiaries, interlocutors and donors in the ICRC capacity to manage information and fulfill its mandate in a responsible and professional manner.

Information security incidents can pose significant risks to business continuity and reputation as people and things are increasingly interconnected, and as:

- Information and communication technologies become ubiquitous and key to support all business processes, services and physical infrastructure;
- The organization's activities depend on information and information systems that are highly dependent on external systems and services, such as cloud computing services.
- Information becomes the main source of value and profit for private and public entities. Information and information systems thus drive competition, but they also may be taken advantage of by criminal groups and individuals, and may be the object of surveillance, spying and cyber-attacks by organized groups and states.

[2] See ICRC Rules on Personal Data Protection. Information security has a wider scope and a different objective to data protection. Information security covers all information (including personal data) processed by ICRC, while data protection only covers personal data. Information security is a set of measures to manage the information security risk, while data protection is a rights based approach that affords rights to individuals related to the use of their personal data and legal obligations for organizations, like the ICRC, in the processing of their personal data. Personal Data Protection rules require the application of the adequate level of security to the processing of Personal Data. Information security shall provide this adequate level of security and is therefore a prerequisite for the implementation of ICRC Personal Data Protection rules. The Information Security Framework and other policies related to information security shall apply to personal data, unless such application is not compatible with the ICRC Rules on Data Protection, in which case the latter (that strikes a balance between ICRC interests and individual rights) shall prevail.

[3] Article 21, Data Security, ICRC Rules on Personal Data Protection.

Purpose and Scope

Information Security

Information security is defined as all organizational, legal and technical measures aiming to protect the information and information systems managed by the ICRC against loss of confidentiality, integrity and availability, regardless of the form the information takes (e.g., electronic, physical, or oral). Data security has a narrower scope than information security and can be considered as one layer of information security. It is primarily concerned with the protection of digital data and the encryption of data in storage.

Information Security Framework

The **Information Security Framework (ISF)** defines the approach, guiding principles, roles and responsibilities set forth by the ICRC to manage an information security risk, in order to protect ICRC information and information systems against loss of confidentiality, integrity and availability.

All technical, organizational and legal rules and measures aiming to ensure the security of information and information systems shall be guided by the Information Security Framework.

The Information Security Framework applies to all information managed by the ICRC and to all information systems managed or approved by ICRC and used by internal staff, partners and beneficiaries.

It does not apply to the use by beneficiaries or partners of systems that are neither managed, nor approved by the ICRC. As an example, operational guidelines, advices and sharing of best practices by the ICRC to raise the awareness of beneficiaries and partners on the responsible use of systems which are neither approved nor managed by the ICRC are outside the scope of the Information Security Framework.

Audience

All **internal staff** (all individuals working for the ICRC under an employment contract) should familiarize themselves with, and must respect the Information Security Framework principles and other relevant information security policies and guidelines, enabling them to meet their obligations under the ICRC's Code of Conduct signed by all staff.

The Information Security Framework, the ICRC Rules on Personal Data Protection, the Framework for the management of documents and information at the ICRC, the Information Handling Typology Rules and other specific guidelines on the security of ICRC information and information systems are mandatory as well.

In its relationships with **third parties or external staff**, in particular, contractual partners or consultants, the ICRC shall ensure that the principles and rules contained in the Information Security Framework and any other policy related to information security are implemented through adequate safeguards, such as the inclusion and enforcement of appropriate contractual provisions. Where necessary, such contractual provisions may require compliance by third parties with ICRC information security policies and guidelines in addition to the Rules on Discretion.

Guiding Principles

The ICRC shall ensure the level of protection required for each information asset through adequate organizational, legal and technical security measures, by following three information security guiding principles. These principles are based upon security best practices such as the ISO 27001 standard, applying to information security.[4]

Confidentiality

Confidentiality provides the assurance that information is shared only with authorized persons and/or organizations.[5]

Access rights to information[6] must adhere to the Information Handling Typology Rules, which establishes four levels of classification (public, internal, confidential and strictly confidential) and provides guidance on how to classify information and thus protect it against unauthorized disclosure.

Access rights to confidential and strictly confidential information are granted on the basis of the "**need-to-know" principle**, which requires that access to information is given only to individuals who need to know the information in order to perform their job function.

Integrity

Integrity provides the assurance that the information is authentic and complete. The information is not modified or destroyed without authorization and due process.

Availability

Availability provides the assurance that the information, information systems and services are available when needed by those authorized to use them.

[4] The International Organization for Standardization (ISO) has published the ISO/IEC 27001:2013 which specifies the requirements for establishing, implementing, maintaining and continually improving an organizational information security management system.
More information can be found at:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[5] NB this principle of confidentiality derives from international standards (ISO) applied to information security management. It should not be misunderstood with the ICRC policy on confidentiality, as defined in the ICRC Doctrine 58 (The International Committee of the Red Cross's (ICRC's) confidential approach: specific means employed by the ICRC to ensure respect for the law by State and non-State authorities).

[6] A Data Subject's right to access is determined pursuant to Article 8 of the ICRC Rules on Personal Data Protection, rather than by the category of classification.

Information Handling Typology Rules

All information must be classified by staff in accordance with the Information Handling Typology Rules, which provides a four-level classification model. This model supports the ICRC's confidential approach to its work and helps to ensure that information receives the appropriate level of protection throughout its lifecycle (from collection to archiving or deletion), in accordance with the consequences of disclosure for the organization.

Public

This category of information concerns the ICRC's official public communication and information that is made available in the public domain by authorized persons (official channels for public information).

Internal

Information which can be shared with internal and external staff and which must not be published in the public domain.

Confidential

Information which is limited to a group of authorized recipients (internal staff, external staff, beneficiaries or interlocutors) on a need-to-know basis.

The unauthorized disclosure, alteration or destruction of this information could have a **seriously adverse** impact on ICRC operations, assets or staff, external staff, beneficiaries or interlocutors.

Strictly Confidential

Information which is limited to specific members (authorized recipients) of internal staff on a need-to-know basis.

External staff, beneficiaries, interlocutors and other actors should not have access to strictly confidential information except in exceptional cases duly documented (by contract or by obligation, for a limited period of time and on a need-to-know basis).

The unauthorized disclosure, alteration or destruction of this information could have a **severely adverse** impact on ICRC operations, assets, internal staff, external staff, beneficiaries or interlocutors.

Details on ICRC classification and its implementation are available in documents related to the Information Handling Typology Rules.

Management Process and Principles

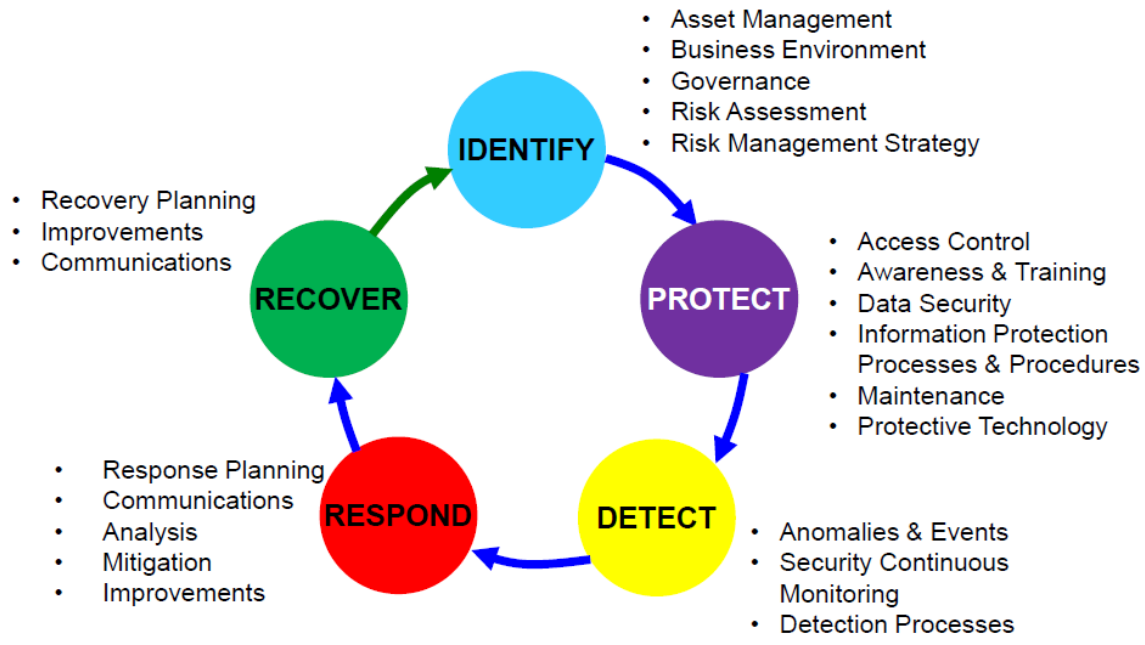
Internal staff, including managers responsible for managing information and information systems, must always adhere to the following processes and principles in a continuous, comprehensive and proactive manner in order to protect the information and information systems managed by ICRC.

Process

As security of information and information systems are continuously evolving, with new systems, technologies, processes, vulnerabilities and threats, the internal staff responsible for managing information and information systems must establish clear processes to secure ICRC information and systems, assess and mitigate any risks to the extent possible.

Given the constantly evolving information security landscape, such processes must be reviewed on a regular basis and revised as necessary.

Internal staff responsible for managing information and information systems must apply the following five core steps in a continuous process and cycle in any information and information systems management process:[7]



[7] These five core steps are based on those set out by the National Institute of Standards and Technology (NIST). See: https://www.nist.gov/cyberframework

1. Identify

"Identify" refers to the first step necessary to understand the business requirements and environment, as well as the risks, threats and vulnerabilities related to the management of information and information systems, in order to manage these risks. It is essential to understand risks in the context in which they arise, so that the most appropriate mitigation measures can be taken.

To identify means to:

- Understand the business context, purpose and requirements of the different métiers to use or develop information systems, processes, capabilities or services;
- Identify the ICRC's most critical information assets, and protect them in accordance with the level of risk they are exposed to;
- Undertake risk assessments on a regular basis in order to identify any risks and the appropriate legal, organizational and technical measures which must be taken in order to mitigate them.

2. Protect

"Protect" means implementing the appropriate safeguards to address the risks identified in step 1.

This step of the information and systems management process must take into account four safeguards: protective technologies (e.g. antivirus software, firewalls), organizational aspects (e.g. information and systems security procedures, formalized responsibilities), legal safeguards (e.g. Headquarters Status Agreements, contracts with suppliers, etc.) and people (e.g. training, awareness-raising).

These safeguards are implemented at different stages of the process:

- During the development of new projects, with controls at the project's gates;
- In response to specific initiatives and requests, such as innovation initiatives; or new processes involving internal data processing or data sharing with third parties;
- During normal operations and maintenance.

3. Detect

"Detect" refers to the appropriate activities required to identify the occurrence of an information security incident.

It includes the use of technical means to detect a suspicious activity and an information security incident in a timely manner and understand the potential risks they pose. This step of the management process demands continuous monitoring of activities with appropriate processes and means (e.g. tools and resources) of detection.

4. Respond

"Respond" refers to all the appropriate activities to take following the detection of a security incident. It includes actions taken immediately to ensure timely response to detected security incidents and complementary activities such as communication (e.g. to inform relevant or affected stakeholders including managers and staff, partners, beneficiaries and law agencies), analysis (to ensure the appropriateness of the response), mitigation measures (to limit impact), improvements (e.g. following a 'lessons learned' exercise), and, when relevant, written/oral interventions towards a State party to the Geneva Conventions to recall their obligations and/or third party identified as implicated in the incident.

5. Recover

"Recover" includes all necessary activities and recovery plans to restore in a timely manner any capability or services that were impaired due to a security incident. In addition to recovery processes, improvements and communications may be also be appropriate.

Principles

Internal staff in charge of managing information and information systems must adhere to the following principles in order to ensure that information is only accessible to authorized persons and organizational processes are duly followed.

Segregation of duties

Segregation of Duties (or separation of duties) refers to the division of roles and responsibilities for the purposes of reducing the possibility for a single individual to compromise the security of information and information systems. It reinforces the level of control to prevent fraud or error. Segregation of duties requires that each important security function is divided into separate steps and that each step is assigned to a different person or entity.

Authentication, Access control and Accounting

Authentication, Access control and Accounting mechanisms shall ensure that:

- A user attempting to access ICRC information and information systems is identified as the one s/he claims to be;
- A user is authorized to access only information and information systems that s/he is entitled to in order to fulfil her or his function;

Information Security Roles & Responsibilities

The governance and escalation mechanism to manage an information security risk is based upon the following division of tasks and responsibilities.

All internal and external staff

It is the responsibility of internal and external staff to take all necessary measures to protect ICRC information and information systems.

Internal staff must comply with the Code of Conduct, the Information Security Framework, the Information Handling Typology Rules and other information security guidelines and policies, as well as with ICRC Rules on Personal Data Protection.

In its relationships with **third parties or external staff**, in particular contractual partners or consultants, the ICRC shall ensure that the principles and rules contained in the Information Security Framework and any other policy related to information security are implemented through adequate safeguards, such as the inclusion and enforcement of appropriate contractual provisions. Where necessary, such contractual provisions may require compliance by third parties with ICRC information security policies and guidelines.

Directorate

The Directorate validates the Information Security Framework. It delegates to the Information Security Board – led by the Department of Communication and Information management – the responsibility of managing information security risks at the global level, as well as approving institutional policies and guidelines related to information security.

The Directorate delegates as well to the Information Security Board the overall consistency of the Information Security Framework with global compliance mechanisms, including institutional risk management processes and the Institutional Strategy and priorities.

The Director of Communication and Information management will inform the Directorate of security issues that are considered as on watch or a top risk for the organization and of necessary mitigation or recovery measures. The Directorate will determine the level of risk that the organization is ready to assume and acceptable time period for implementation of mitigation or recovery measures. The Audit Committee and Assembly Council will be informed of serious security risks or issues.

Global Compliance Office

The Global Compliance Office, supervised by the Deputy Director General contributes to the strengthening of ICRC's management capacity in the area of risk management, internal control and Code of Conduct compliance.

The Global Compliance Office supports the department of Communication and Information Management and the Information Security Board in risk management and compliance with the Information Security Framework, as well as other information security policies and guidelines published by the Information Security Board.

The Code of Conduct Compliance Officer supports enforcement of rules and regulations when they complement the Code of Conduct and as soon as a complaint has been registered. It notifies the

Director of the Department of Communication and Information Management of information security issues and allegations of violation of the Information Security framework, policies and guidelines that come to its attention.

Complaints related to violations of ICRC rules on data protection are not in scope of the Global Compliance Office. Such complaints will be transferred to the Data Protection office for further handling. See the ICRC Rules on Personal Data Protection.

Information Security Board

The Information Security Board (ISB) manages institutional risks related to the security of information at the ICRC, acts as a compliance mechanism and a decision-making body on major information security issues, policies and guidelines, and validates institutional information security guidelines.

In addition, the Information Security Board ensures the consistency of the Information Security Framework with global compliance mechanisms, top risk management frameworks and the Institutional Strategy and priorities. When appropriate, the Information Security Board is responsible to escalate to the Directorate decisions which have a significant impact on the institution.

The Information Security Board is chaired by the Deputy Director of the Communication and Information Management (CIM) Department. It is a multi-disciplinary board that appoints its permanent members and determines its own functioning rules.

The Information Security Board is the owner of the Information Security Framework and is responsible for reviewing, updating and promoting it.

ICRC Data Protection Office

The ICRC Data Protection Office (DPO) is the ICRC's supervisory body with regards to all personal data protection matters. The Data Protection Office monitors the application of the provisions of the ICRC Rules on Personal Data Protection and contributes to its consistent application throughout the ICRC, in order to protect natural persons in relation to the Processing of their Personal data.

In the case where a person considers that their rights have been infringed under the ICRC Rules on Personal Data Protection, the Data Protection Office may refer the matter to the ICRC Data Protection Commission which will examine the case and make a binding decision. The Directorate will be informed of such escalations via the Director of the Department managing the Data Protection Office.

ICT Security Officer

The ICT Security Officer, leading the Cyber Security Risks & Compliance office (CSRC) is responsible for managing the security of ICRC information systems and assets, based on risk analysis. The ICT Security Officer initializes and drafts for the Information Security Board the guidelines, concepts and instructions necessary to ensure information security. He or she determines the ICT security guidelines,

standards and measures to secure the information systems which are validated by the Director of the Department, further to their consultation at the Information Security Board.

Archives and Information Management Division

The Information Management Unit of the Archives and Information Management Division provides guidance and support to internal and external staff on how to apply the Information Handling Typology Rules and other information security guidelines and policies for collecting, managing, archiving and sharing information. It is also responsible for the implementation of the Information Handling Typology Rules.

Managers of Departments, Divisions and Units

The management of Departments, Divisions and Units are responsible for the promotion, implementation and enforcement of the Information Security Framework, the Information Handling Typology Rules, ICRC Rules on Personal Data Protection, as well as other institutional information security policies and guidelines.

Moreover, the management is responsible to define and implement more specific guidelines and processes for its specific services in order to protect the specific ICRC information and information systems under its métier's responsibility at HQ and in the field.

These specific guidelines and measures shall be in line with the ICRC's code of conduct, Information Security Framework, the Information Handling Typology Rules, ICRC Rules on Personal Data Protection and other institutional information security guidelines and policies.

Delegations

The management of the Delegation is responsible for promoting, implementing and enforcing the Information Security Framework, the Information Handling Typology Rules, the ICRC Rules on Personal Data Protection, as well as other institutional information security policies and guidelines, for its internal staff, as well as external staff engaged with the Delegation.

The management of the Delegation is responsible, for defining and implementing additional and more specific guidelines and measures to protect the information assets and systems used in the Delegation by internal and external staff.

These specific guidelines and measures must be in line with the ICRC's Code of Conduct, Information Security Framework, the Information Handling Typology Rules, the ICRC Rules on Personal Data Protection, security guidelines, and other institutional information security guidelines and policies.

Enforcement

Internal and external staff are responsible for managing and using information and information systems in a responsible way. They must comply with institutional rules, in particular with the rules of the ICRC's Code of Conduct related to the use of information technology, which constitute an integral part of the employment contract. Failure to comply with specific rules on information security described in ICRC's Code of Conduct can lead to sanctions, including the initiation of disciplinary proceedings.

The Directorate of the ICRC entrusts the Department of Communication and Information Management to ensure that proper compliance mechanisms are designed, implemented and enforced, with the support of the Global Compliance Office. This includes the enforcement of the Information Security Framework and staff compliance with information security rules.

Enforcement includes:

a) All measures led by the respective bodies, as defined above in the Information Security Roles & Responsibilities, to manage information security risks;

b) Regular controls, in the form of
    a. internal assessments; and
    b. external audits

c) Response mechanisms, such as inquiries or investigations that can lead to corrective measures or sanction.