INTERNATIONAL STANDARD

ISO/IEC 27010

Second edition
2015-11-15

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

Technologies de l'information — Techniques de sécurité — Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles

Reference number
ISO/IEC 27010:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27010:2012), which has been revised for compatibility with ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Introduction

This International Standard is a sector-specific supplement to ISO/IEC 27001:2013 and ISO/IEC 27002:2013 for use by information sharing communities. The guidelines contained within this International Standard are in addition to, and complement, the generic guidance given within other members of the ISO/IEC 27000 family of standards.

ISO/IEC 27001:2013 and ISO/IEC 27002:2013 address information exchange between organizations, but they do so in a generic manner. When organizations wish to communicate sensitive information to multiple other organizations, the originator must have confidence that its use in those other organizations will be subject to adequate security controls implemented by the receiving organizations. This can be achieved through the establishment of an information sharing community where each member trusts the other members to protect the shared information, even though the organizations may otherwise be in competition with each other.

An information sharing community cannot work without trust. Those providing information must be able to trust the recipients not to disclose or to act upon the data inappropriately. Those receiving information must be able to trust that information is accurate, subject to any qualifications notified by the originator. Both aspects are important, and must be supported by demonstrably effective security policies and the use of good practice. To achieve this, the community members must all implement a common management system covering the security of the shared information. This is an information security management system (ISMS) for the information sharing community.

In addition, information sharing can take place between information sharing communities where not all recipients will be known to the originator. This will only work if there is adequate trust between the communities and their information sharing agreements. It is particularly relevant to the sharing of sensitive information between diverse communities, such as different industry or market sectors.

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

1 Scope

This International Standard provides guidelines in addition to the guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities.

This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications. It provides guidelines and general principles on how the specified requirements can be met using established messaging and other technical methods.

This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organization's or nation state's critical infrastructure. It is designed to support the creation of trust when exchanging and sharing sensitive information, thereby encouraging the international growth of information sharing communities.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000:2014 apply.

4 Concepts and justification

4.1 Introduction

ISMS guidance specific to inter-sector and inter-organizational communications has been identified in Clauses 5 to 18 of this International Standard.

ISO/IEC 27002:2013 defines controls that cover the exchange of information between organizations on a bilateral basis, and also controls for the general distribution of publicly available information. However, in some circumstances there exists a need to share information within a community of organizations where the information is sensitive in some way and cannot be made publicly available other than to

members of the community. Often the information can only be made available to certain individuals within each member organization, or may have other security requirements such as anonymization of information. This International Standard defines additional potential controls and provides additional guidance and interpretation of ISO/IEC 27001:2013 and ISO/IEC 27002:2013 in order to meet these requirements.

There are four informative annexes. Annex A describes the potential benefits from sharing sensitive information between organizations. Annex B provides guidance on how members of an information sharing community can assess the degree of trust that can be placed in information provided by other members. Annex C describes the Traffic Light Protocol, a mechanism widely used in information sharing communities to indicate the permitted distribution of information. Annex D contains some examples of models for organizing an information sharing community.

4.2 Information sharing communities

To be effective, information sharing communities must have some common interest or other relationship to define the scope of the shared sensitive information. For example, communities may be market sector specific, and limit membership to organizations within that one sector. Of course, there may be other bases for common interest, for example, geographical location or common ownership.

There must also be trust between members, in particular that all members will follow the information sharing agreement.

4.3 Community management

Information sharing communities will be created from independent organizations or parts of organizations. There may, therefore, not be clear or uniform organizational structures and management functions applying to all members. For information security management to be effective, management commitment is necessary. Therefore, the organizational structures and management functions applying to community information security management should be clearly defined.

Differences among member organizations of an information sharing community should also be considered. The differences could include:

— differing legal or regulatory environments,

— whether member organizations already operate their own ISMS, and

— member rules on protections of assets and information disclosure.

4.4 Supporting entities

Many information sharing communities will choose to establish or appoint a centralized supporting entity to organize and support information sharing. Such an entity can provide many supporting controls such as anonymization of source and recipients more easily and efficiently than where members communicate directly.

There are a number of different organizational models that can be used to create supporting entities. Annex D describes two common models, the Trusted Information Communication Entity (TICE) and the Warning, Advice and Reporting Point (WARP).

4.5 Inter-sector communication

Many information sharing communities will be sector based, as this provides a natural scope of common interest. However, there may well be information shared by such communities that would be of interest to other information sharing communities established in other sectors. In such cases it may be possible to establish information sharing communities of information sharing communities, again based on some common interest, such as the nature of the shared information. We refer to this as inter-sector communication.

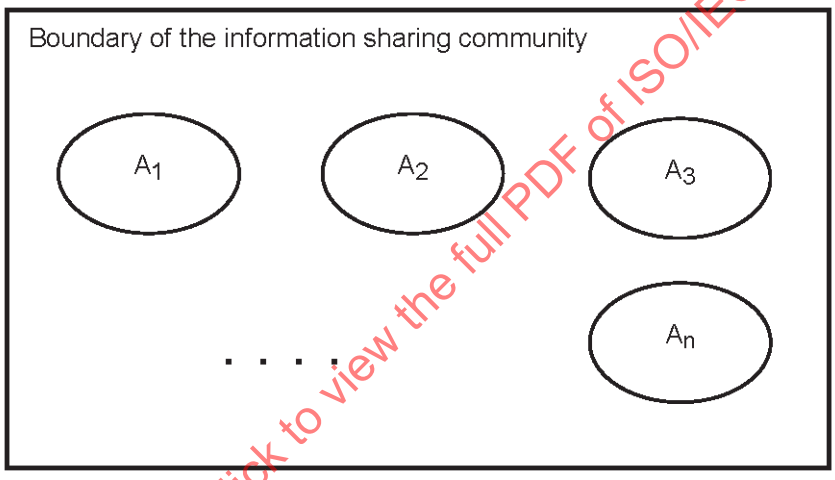
Inter-sector communication is greatly facilitated where supporting entities exist within each information sharing community, as the necessary information exchange agreements and controls can then be established between the supporting entities, rather than between all members of all communities. Some inter-sector communities will require anonymization of the source or recipient organizations; this also can be achieved by use of supporting entities.

4.6 Conformity

There are a number of places where ISO/IEC 27001:2013 will need to be interpreted when applied to an information sharing community (or, for inter-sector communication, a community of communities).

The first area where interpretation is required is the definition of the organization concerned.

ISO/IEC 27001:2013 requires that an ISMS is established, implemented, maintained and continually improved by an organization (ISO/IEC 27001:2013, 4.4). In this context, the relevant organization is the information sharing community. However, the members of the information sharing community will themselves be organizations – see Figure 1.



Key

A_k Member organization k of the community (k = 1 ... n), including any supporting entity.

Figure 1 — Communities and organizations

Secondly, in many information sharing communities, not all persons within the member organizations will be permitted access to the sensitive information shared between members. In this case, part of the member organization will be within scope of the community ISMS and part will be outside. The part outside the community scope will only have access to community information if it is marked for wider release – see Figure 2.

It is possible that members of the information sharing community may have their own information security management systems and, in consequence, some processes might fall within scope of both the community and members' management systems. In this case, there is at least a theoretical possibility that there might be conflicting and incompatible requirements upon those processes. This might be an issue justifying exclusion from the scope of the member's ISMS – see ISO/IEC 27001:2013, 4.3.

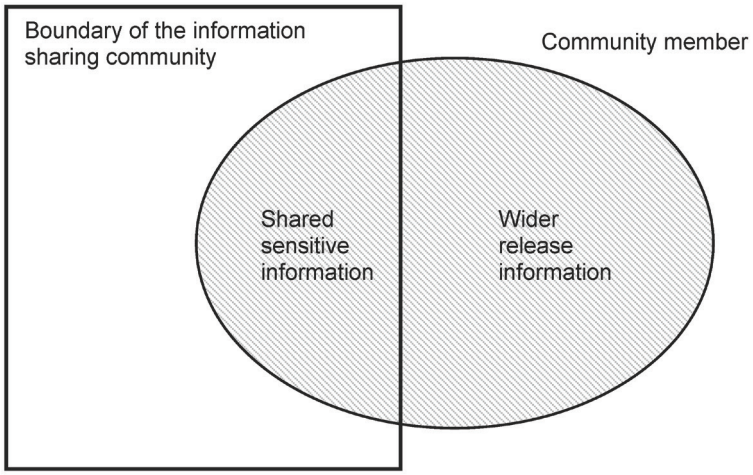


Figure 2 — Member ISMS partially in scope

When defining its risk assessment process (ISO/IEC 27001:2013, 6.1.2), the information sharing community will need to recognize that the impact of risks may be different on different members of the community. The community will, therefore, need to choose a risk assessment methodology that can handle non-uniform impact, and similarly for its risk assessment criteria.

4.7 Communications model

Communications of sensitive information as covered by this International Standard can take any form – written, verbal or electronic – provided that the selected control requirements are met.

In the remainder of this International Standard, individual sensitive communications are described in terms of the following participants:

— The *source* of an item of information is the person or organization that originates an item of information; the source does not need to be a member of the community.

— The *originator* is the member of an information sharing community that initiates its distribution within the community. The originator may distribute the information directly, or send it to a supporting entity for distribution. The originator may, but need not be, the same as the source of the information; the originator may conceal the identity of the source. Communities may provide facilities to enable a member to conceal its own identity as the originator.

— A *recipient* is a receiver of information distributed within the community. Recipients need not be members of the community if the information is identified as available for wider distribution. Communities may provide facilities to enable recipients to conceal their identities from the originators of information.

5 Information security policies

5.1 Management direction for information security

5.1.1 Policies for information security

ISO/IEC 27002:2013, control 5.1.1 is augmented as follows:

Implementation guidance

An information sharing policy should define how the community members will work together to set security management policies and direction for the information sharing community. It should be made

available to all employees involved in information sharing within the community. The policy may restrict its dissemination to other employees of community members.

The information sharing policy should define the information marking and distribution rules used within the community.

5.1.2 Review of the policies for information security

ISO/IEC 27002:2013, control 5.1.2 is augmented as follows:

Implementation guidance

The review should include information on significant changes to membership of the information sharing community.

6 Organization of information security

No additional information specific to inter-sector or inter-organizational communications.

7 Human resource security

7.1 Prior to employment

7.1.1 Screening

ISO/IEC 27002:2013, control 7.1.1 is augmented as follows:

Implementation guidance

Screening rules are unlikely to be consistent across all members of an information sharing community. Communities should consider defining minimum levels of verification checks to be applied to all employees or contractors of members who will be given access to shared community information.

7.1.2 Terms and conditions of employment

No additional information specific to inter-sector or inter-organizational communications.

7.2 During employment

No additional information specific to inter-sector or inter-organizational communications.

7.3 Termination and change of employment

No additional information specific to inter-sector or inter-organizational communications.

8 Asset management

8.1 Responsibility for assets

8.1.1 Inventory of assets

No additional information specific to inter-sector or inter-organizational communications.

8.1.2 Ownership of assets

No additional information specific to inter-sector or inter-organizational communications.

8.1.3 Acceptable use of assets

ISO/IEC 27002:2013, control 8.1.3 is augmented as follows:

Implementation guidance

Information provided by other members of an information sharing community is an asset and should be protected, used and disseminated in accordance with any rules set by the information sharing community or by the originator.

8.1.4 Return of assets

No additional information specific to inter-sector or inter-organizational communications.

8.2 Information classification

8.2.1 Classification of information

ISO/IEC 27002:2013, control 8.2.1 is modified as follows:

Control

Information should be classified in terms of legal requirements, value, credibility, priority, criticality and sensitivity to unauthorized disclosure or modification.

Implementation guidance

As well as the criteria given in ISO/IEC 27002:2013, information should be classified in terms of its credibility and priority. Credibility should be assessed in terms of the reputation of its source, technical content, and quality of description. Priority should indicate the need for urgent or immediate action, such as further distribution.

Likewise, sensitivity can depend on many aspects of information beyond a need for maintaining its confidentiality, such as the impact of disclosure or potential to compromise the anonymity of its source.

Care should be taken in interpreting classification markings assigned by other members of an information sharing community.

EXAMPLE One well-known email client displays the message “Please treat this as Confidential” when displaying emails where the sensitivity header field has been set to “company confidential” (RFC 4021[1]). It is not clear in this case if the originator intended “company confidential” (and the message has been sent in error) or intended “confidential to you, the recipient”.

8.2.2 Labelling of information

No additional information specific to inter-sector or inter-organizational communications.

8.2.3 Handling of assets

No additional information specific to inter-sector or inter-organizational communications.

8.3 Media handling

No additional information specific to inter-sector or inter-organizational communications.

8.4 Information exchanges protection

A control objective additional to ISO/IEC 27002:2013, Clause 8, asset management, is:

Objective: To ensure adequate protection of information exchanges within an information sharing community.
Information exchanged between members of an information sharing community should be protected in a consistent manner, even though the members are independent entities or parts of entities that may mark, distribute and protect their own information in different ways.
Where anonymity is requested, any information identifying the source of the information exchange should be removed. Likewise, it should be possible to receive shared information without revealing the recipient's identity.
Release of shared information outside the community should be controlled.

8.4.1 Information dissemination

Control

Information dissemination within the receiving member should be limited, based on pre-defined dissemination markings defined by the community.

Implementation guidance

Information which has no assigned dissemination marking should be given a default dissemination defined by the information sharing community. If in doubt or where there is no generally accepted agreement on default dissemination, information should be treated conservatively. If possible, the recipient should request the originator to re-transmit with an explicit dissemination marking.

Dissemination restrictions may include limitations on use such as controlling electronic copy and paste, preventing screen shots being taken, or preventing printing and export.

Other information

Different attributes or components of shared information may have different sensitivities. In particular, knowledge of the existence of a message or other shared information may have a different sensitivity to its contents.

Information rights management functionality is often used to enforce in-use limitations. If so, a clear user rights policy or model is needed so that users understand what their system will allow them to do and where they will be blocked.

8.4.2 Information disclaimers

Control

Each information exchange should begin with a disclaimer, listing any special requirements to follow by the recipients in addition to the normal information markings.

Implementation guidance

A recipient should request clarification from the originator if the disclaimer is not fully understood, or cannot be implemented.

8.4.3 Information credibility

Control

Each information exchange should indicate the originator's degree of confidence in the transmitted information's credibility and accuracy.

Implementation guidance

Based on urgency, potential consequences and technical constraints, it may not be possible to validate all information before transmission. Where limitations exist, these should be indicated as part of the message.

Indicating reservations on credibility of information is particularly important where the source is anonymous or unknown. It is also important to indicate where the originator has been able to validate the information given directly, and can vouch for its authenticity.

8.4.4 Information sensitivity reduction

Control

The originator of an information exchange should indicate if the sensitivity of the information supplied will reduce after some external event, or the passage of time.

Implementation guidance

Even if the sensitivity of supplied information reduces with time, it may still need protection. Classification guidelines (see 8.2.1) may need to include defaults for sensitivity reduction.

8.4.5 Anonymous source protection

Control

A community member should remove any source identification information in any communication it originates or receives where anonymity is requested.

Implementation guidance

The originator of information is responsible for obtaining approval from the source (if different) before communicating the information to other members of the information sharing community. The originator should also ask the source if it can be identified as the original provider of the information.

It is important that the source protection process looks at message content as well as message origin, because analysis of the content may reveal the identity of the source. Where possible, the originator of the message should ask the source to review the anonymized information and the list of intended recipients before it is distributed.

EXAMPLE A message such as "our ATMs were disabled today by a new virus that was not detected by our firewall but was detected by our policy server" could reveal the source if only one bank suffered public service disruption on the day in question.

There are technical mechanisms that can be used to provide authenticity without compromising anonymity. For example, shared cryptographic secrets could be used to confirm that a communication originated from a member of the community without revealing the actual identity of the originator.

8.4.6 Anonymous recipient protection

Control

With the approval of the originator, members of a community should be able to receive communications without revealing their own identities.

Implementation guidance

Anonymous receipt can be implemented by both technical means (e.g. cryptography) and procedural means (e.g. routing through a supporting entity). Care must be taken to ensure anonymity does not breach legal constraints or reduce the overall level of trust within the community.

Other information

Anonymous receipt is often necessary for effective inter-sector communications because sector communities will wish to keep their membership details private.

8.4.7 Onwards release authority

Control

Unless it is marked for wider release, information should not be distributed beyond the information sharing community without formal approval from the originator.

Implementation guidance

Each recipient should be responsible for obtaining any necessary authorizations for wider release from the originator prior to onwards distribution.

In inter-sector communications, the originator cannot know who all the organizations that receive the information will be. In such a case, a general or specific sector release approval will need to be granted.

Other information

The Traffic Light Protocol (see Annex C) is often used to indicate how information can be further distributed without seeking additional approval.

9 Access control

No additional information specific to inter-sector or inter-organizational communications.

10 Cryptography

10.1 Cryptographic controls

10.1.1 Policy on the use of cryptographic controls

ISO/IEC 27002:2013, control 10.1.1 is augmented as follows:

Implementation guidance

Cryptographic techniques can also be used to implement the dissemination rules of information sharing, e.g. through information rights management.

10.1.2 Key management

No additional information specific to inter-sector or inter-organizational communications.

11 Physical and environmental security

No additional information specific to inter-sector or inter-organizational communications.

12 Operations security

12.1 Operational procedures and responsibilities

No additional information specific to inter-sector or inter-organizational communications.

12.2 Protection from malware

12.2.1 Controls against malware

ISO/IEC 27002:2013, control 12.2.1 is augmented as follows:

Implementation guidance

Information received from other members of an information sharing community should be scanned for the presence of malware, regardless of whether the communications service between members of the community provides message scanning or not.

12.3 Backup

No additional information specific to inter-sector or inter-organizational communications.

12.4 Logging and monitoring

12.4.1 Event logging

ISO/IEC 27002:2013, control 12.4.1 is augmented as follows:

Implementation guidance

When required by the information sharing community, members should log the internal dissemination of shared information.

12.4.2 Protection of log information

No additional information specific to inter-sector or inter-organizational communications.

12.4.3 Administrator and operator logs

No additional information specific to inter-sector or inter-organizational communications.

12.4.4 Clock synchronization

No additional information specific to inter-sector or inter-organizational communications.

12.5 Control of operational software

No additional information specific to inter-sector or inter-organizational communications.

12.6 Technical vulnerability management

No additional information specific to inter-sector or inter-organizational communications.

12.7 Information systems audit considerations

12.7.1 Information systems audit controls

No additional information specific to inter-sector or inter-organizational communications.

12.7.2 Community audit rights

A control additional to ISO/IEC 27002:2013, 12.7, information systems audit considerations, is:

Control

Every information sharing community should specify the rights of members to audit the systems of other members and of any trusted service providers.

Implementation guidance

The authority to audit member systems could be limited to a trusted third party, such as a TICE or WARP.

13 Communications security

13.1 Network security management

No additional information specific to inter-sector or inter-organizational communications.

13.2 Information transfer

13.2.1 Information transfer policies and procedures

No additional information specific to inter-sector or inter-organizational communications.

13.2.2 Agreements on information transfer

ISO/IEC 27002:2013, control 13.2.2 is augmented as follows:

Implementation guidance

All information sharing communities should define information transfer agreements, and should only permit members to join the community if such agreements are signed and accepted.

13.2.3 Electronic messaging

ISO/IEC 27002:2013, control 13.2.3 is augmented as follows:

Implementation guidance

All information sharing communities should define rules for the protection of information in transit, and only permit members to join the community if such rules are accepted and implemented by the prospective member. Any supporting entity should implement such rules internally.

Information sharing communities should consider implementing alternative mechanisms for information sharing that do not rely on electronic messaging, and enabling members to specify that specific messages are distributed by such other routes.

13.2.4 Confidentiality or non-disclosure agreements

No additional information specific to inter-sector or inter-organizational communications.

14 System acquisition, development and maintenance

No additional information specific to inter-sector or inter-organizational communications.

15 Supplier relationships

15.1 Information security in supplier relationships

15.1.1 Information security policy for supplier relationships

No additional information specific to inter-sector or inter-organizational communications.

15.1.2 Addressing security within supplier agreements

ISO/IEC 27002:2013, control 15.1.2 is augmented as follows:

Implementation guidance

All community members should be made aware of the identities of all third parties involved in the provision of community services, in case they have objections to particular parties being involved in the handling of information that they provide.

The agreements with suppliers associated with provision of community services should enable security reviews and audits of their services to be performed on a regular basis.

15.1.3 Information and communication technology supply chain

No additional information specific to inter-sector or inter-organizational communications.

15.2 Supplier service delivery management

No additional information specific to inter-sector or inter-organizational communications.

16 Information security incident management

16.1 Management of information security incidents and improvements

16.1.1 Responsibilities and procedures

No additional information specific to inter-sector or inter-organizational communications.

16.1.2 Reporting information security events

ISO/IEC 27002:2013, control 16.1.2 is augmented as follows:

Implementation guidance

Members of an information sharing community should consider whether detected events should be reported to other members of the community. The community should agree and publish guidance on the types of incident that will be of interest to other members. Members should exercise judgement to ensure only events potentially of interest to other members are reported.

There is a strong tendency for incidents to be kept confidential and for a community member not to disclose incident information in order to protect the originator's reputation. However, communicating incident information to others will foster future cooperation and coordination in incident prevention, prompt rapid reaction to incidents and improve overall security within the community. Events and incidents can be reported without necessarily revealing all of their consequences.

Likewise, members should examine all reported events promptly to see if they will have an impact upon their own operations. For example, a routine announcement by a member providing a shared service of a planned maintenance operation might require other members to review the reliability of alternative providers before the maintenance activity starts.

16.1.3 Reporting information security weaknesses

No additional information specific to inter-sector or inter-organizational communications.

16.1.4 Assessment of, and decision on, information security events

No additional information specific to inter-sector or inter-organizational communications.

16.1.5 Response to information security incidents

No additional information specific to inter-sector or inter-organizational communications.

16.1.6 Learning from information security incidents

ISO/IEC 27002:2013, control 16.1.6 is augmented as follows:

Implementation guidance

Investigations based on information distributed by an information sharing community should be performed, to reduce the risks of similar incidents and develop a better understanding of the risks facing the community and any related significant information infrastructures. Such investigations could be performed by the community members involved, or by a supporting entity, if one exists.

Following reported incidents, post incident reviews should be performed by members of the information sharing community to trigger updates to security incident response plans, related procedures and the business risk profile, even if the member was not affected by the incident in question. Each member should ensure that reported incident responses are assessed, and any lessons or possible improvements to the member's own processes are identified and acted upon to continuously improve its own response processes.

16.1.7 Collection of evidence

No additional information specific to inter-sector or inter-organizational communications.

16.1.8 Early warning system

A control additional to ISO/IEC 27002:2013, 16.1, management of information security incidents and improvements, is:

Control

An early warning system should be deployed within the information sharing community to effectively communicate priority information as soon as it is available.

Implementation guidance

Priority information is information that may enable other community members to avoid or minimize similar undesirable events. It is important that such information is shared urgently, even if it is not fully analysed or confirmed.

17 Information security aspects of business continuity management

17.1 Information security continuity

17.1.1 Planning information security continuity

ISO/IEC 27002:2013, control 17.1.1 is augmented as follows:

Implementation guidance

Business continuity and disaster recovery plans developed by members of an information sharing community should address the need to exchange sensitive information with other members in a secure manner as part of the recovery process.

17.1.2 Implementing information security continuity

No additional information specific to inter-sector or inter-organizational communications.

17.1.3 Verify, review and evaluate information security continuity

No additional information specific to inter-sector or inter-organizational communications.

17.2 Redundancies

No additional information specific to inter-sector or inter-organizational communications.

18 Compliance

18.1 Compliance with legal and contractual requirements

18.1.1 Identification of applicable legislation and contractual requirements

ISO/IEC 27002:2013, control 18.1.1 is augmented as follows:

Implementation guidance

The information sharing community should take due account of any relevant agreements, laws and regulations relating to information sharing, such as anti-cartel legislation or regulations. This could prevent certain organizations joining the community, or place restrictions upon their representation.

18.1.2 Intellectual property rights

No additional information specific to inter-sector or inter-organizational communications.

18.1.3 Protection of records

No additional information specific to inter-sector or inter-organizational communications.

18.1.4 Privacy and protection of personally identifiable information

No additional information specific to inter-sector or inter-organizational communications.

18.1.5 Regulation of cryptographic controls

No additional information specific to inter-sector or inter-organizational communications.

18.1.6 Liability to the information sharing community

A control additional to ISO/IEC 27002:2013, 18.1, compliance with legal and contractual requirements, is:

Control

Liability issues and remediation should be clarified, understood and approved by all members of an information sharing community, to address situations in which information is intentionally or unintentionally disclosed.

Implementation guidance

Remediation should include, at a minimum, notification of any unauthorized disclosure back to the originator, with sufficient detail to identify the information disclosed.

Where possible, notification should be provided back to the source, even if the information has been sanitized and does not reveal its origin. This could be achieved by the intermediary of a trusted third party, such as a TICE.

Unauthorized disclosure consequences could affect directly the responsible parties and might involve eliminating or restricting access to some members for some period of time to re-establish community trust.

18.2 Information security reviews

No additional information specific to inter-sector or inter-organizational communications.

Annex A
(informative)

Sharing sensitive information

A.1 Introduction

Sensitive information is an asset of important value that must be securely managed when shared between organizations. It must be delivered in time to address business issues and to make better decisions, even more so if it is critical to the organization.

Information sharing communities may represent many types of organization and even individual people. Communities may be extraordinarily diverse in their membership, or be aligned very closely with a form of business activity, such as a particular industry or market sector. Communities may be located in both the public and private sectors, or may contain members of both kinds. The requirement is a common wish to share sensitive information of some type, and to accept agreed controls and processes governing the use of that information.

To securely exchange sensitive information within an information sharing community, it is necessary to design, implement and monitor processes to provide a secured flow of information on a timely basis. The processes should ensure that information is disseminated to the appropriate persons, whilst providing reasonable assurance that the information cannot be used for malicious purposes and is not indiscriminately re-distributed so as to become essentially public information.

The effectiveness of distribution will be determined by the degree of trust that members hold in the relationships established by the information sharing community. At the same time, the security mechanisms relating to communications should prevent distributing information to persons or organizations that would likely:

— use or accumulate the data to perform malicious acts;

— publicly disseminate information without permission of the information originator;

— provide information that has not been sufficiently analysed and, therefore, induces inappropriate actions which could waste or mislead resources and the impact on organizations.

For information sharing communities to function effectively, recipients of information must be empowered by their member organizations to act upon the information received, and must not be encouraged to misuse that information, for example for commercial advantage.

A.2 Challenges

Adequate information security management for inter-sector and inter-organizational communications is strongly recommended to face the following challenges; failure to do so could impact normal business conditions and cause disruptions during incidents:

— New security threats and vulnerabilities.

— System and network increased dependencies.

— Contractual, legal, regulatory and business evolution and limits.

— Adequate communications models establishment.

— Attack and reaction processes coordination.

— Ongoing governance.

Secured and resilient communications between community members should include the following elements:

— Risk knowledge and management.

— Dissemination and communication.

— Monitoring.

While these three elements should be taken for their specific value, they are closely linked and complement each other.

It is difficult to develop trust between members of an information sharing community without personal relationships with the representatives of other members. People need to meet face to face, in order to build relationships and create confidence in each other's credibility and discretion. It is difficult to create trust using only remote communications technologies. It is also difficult to establish mechanisms which give confidence in the credibility of the source of information whilst retaining the anonymity of that source. People will often speak more freely if they have confidence that their identity will be kept confidential.

An information sharing community can be effective even if not all members share all information with all other members. Distribution mechanisms must be flexible enough to enable distribution to be limited to specific members of the community, or to be limited by topic.

Finally, when sharing information between communities (for example, in inter-sector communications), the gatekeepers between the communities face special difficulties. Sources of information will not necessarily have knowledge of the membership of other communities and must rely on the interfaces to protect anonymity and other conditions of release. The gatekeepers may lack the specialist knowledge to realize when certain community communications should not be passed further. These problems are typically even worse in inter-national rather than inter-sector communications.

A.3 Potential benefits

Sharing sensitive information with others inevitably increases the potential risk of inappropriate disclosure. For a community to be effective, these risks must be managed and minimized, and the benefits seen as outweighing the accepted residual risks.

The potential benefits of sharing sensitive information include:

— Early warning of any significant change in the risk situation, like new threats, updated likelihood of attack, newly discovered vulnerabilities, etc.

— Improved security through shared best practice.

— Access to useful information not available from any public source.

— Cost savings through elimination of duplicated effort.

— Better risk assessments through greater understanding of threats and vulnerabilities.

— Better organization of maintenance and intervention from information concerning similar activities at other organizations.

— Better preparedness for security incidents.

— Benchmarking of security measures against similar organizations.

— Corporate social responsibility.

— Compliance with legal requirements or corporate policy.

It is essential that the community monitoring and review processes identify concrete benefits (and drawbacks) from community membership for use by members in assessing their continued membership of the community.

A.4 Applicability

Information can be exchanged between many types of organization, large or small, government or private, similar or diverse. However, the greatest benefits may often be experienced by organizations operating within the same sector or with the same corporate objectives, which share sector-specific categories of information security risk. ISO/IEC 27006[2] identifies some such sectors.

There may also be great benefits in sharing information across sectors, either by defining communities based upon other characteristics (such as geographical location) or by sharing information with other sector-based information sharing communities in a hierarchical structure of communities.

A.5 Defining and operating an information sharing community

The information sharing community should define the rules and conditions governing its operation. Such rules and conditions should include:

— the rules and conditions governing membership of the information sharing community and its internal organization;

— the objectives of the information sharing community and intended benefits to members;

— the procedures for members joining or leaving the information sharing community;

— the rules and conditions governing any centralized community processes or entities such as a TICE or WARP;

— the rules and conditions regarding obligations of community members, disciplinary and expulsion processes and criteria;

— clear rules for how members may use and pass on shared information;

— the other legal and financial obligations and conditions of community membership.

The rules and conditions of the information sharing community should also:

— ensure that information is communicated in an efficient and secure manner that ensures that its target audience properly receives the data in good time;

— specify and prioritize potential and selected communication channels, in terms of priority usage to communicate the data for each identified information type;

— specify the permitted circumstances under which information is transmitted to members of the community;

— specify the mandatory and optional data protection and distribution attributes associated with community communications;

— specify clear rules for interpreting the data protection and distribution attributes concerning information dissemination;

— require members to provide feedback on the relevance, timeliness and accuracy of the information received;

— where possible, specify or adapt existing messaging standards for the exchange of information.

The communication rules should define the frequency of communication, any requirements for confirmation of receipt, and any priority or escalation criteria. The rules should recognize that

members of the information sharing community may have varying levels of trust in other members of the community. That degree of trust may vary over time and situation.

Appropriate communication channels should be selected by assessing their strengths and weaknesses when delivering the identified information types supported by the community, based on criteria such as: target audience; attributes of the information to be delivered; channel reach; and frequency, and cost. Examples of possible communication channels are: electronic messaging; public or member-only sites; conference or two-way phone calls; letters sent by public postal services; or face-to-face meetings. The influence a communication has on its target audience depends on the effectiveness of the channel in reaching the audience, its credibility with the audience and its appropriateness to the issue or the information subject.

Not all information needs to be communicated in real-time; some information can best be shared through routine contact.

Possible examples of when information will be transmitted to members of the community are immediate reporting of detected incidents fitting predefined profiles, routine reporting on a time basis, or responses to requests for information from other members. Possible examples of data protection and distribution attributes are a requirement to conceal the origin of the information, the sensitivity of the information or the originator's assessment of the trustworthiness of the information. An example of a set of rules for interpreting data protection and distribution attributes is the Traffic Light Protocol – see Annex C. Attributes may vary depending on the communications channel used. For example, the mandatory attributes for postal distribution may well be different from those for Internet email.

Whatever technical solutions are selected and implemented, they should be appropriate for the types of information shared within the community and consistent with the defined objectives of the community. Face to face contact builds trust and may be a necessary way to grow communities by inviting new members. However, the existence of a trusted platform or other sharing infrastructure may itself encourage membership.

A.6 Information exchange agreements

The information sharing community should define (in an information exchange agreement) the mechanisms and processes governing community communications. Information can be exchanged by letter, or orally at face-to-face meetings, as well as electronically. Information can be exchanged formally, using predefined formats and protocols, or informally, in an unstructured way. Information could be exchanged on a routine or ad-hoc basis. Information can be exchanged by peer-to-peer communications, hierarchically or through a centralized supporting entity such as a TICE or WARP.

The information exchange agreement may permit information to be shared with only selected members of the information sharing community, or only to be made shared anonymously. Likewise, even where centralized reporting facilities exist, it may permit information to be passed between members directly.

The information exchange agreement should specify the types of information that may be exchanged between members of the community. This is in order to ensure a common understanding by the community members of the communicated information and to ensure that members design and implement appropriate security measures for the sensitivity level of the shared information.

Examples of possible information types are:

— "announcements", which correspond to informative explained events;

— "alerts and warnings", which correspond to unexplained physical or IT-related events, denial of service attacks, scanning or spoofing;

— "incident handling", which correspond to analysis, response support and response coordination relating to actual incidents;

— "information requests", which correspond to requests for information from one member of the community addressed to all or some other community members;

— "quality of service predictions", which provide information on the predicted effectiveness and reliability of the various community communications channels.

Too much information sharing can be as bad as too little, unless a suitable method of filtering the data is included. If building trend information is seen as a main benefit of sharing, there must be a method for differentiating high priority "act now" information from low priority "for the record" information.

A.7 Success factors

Effective communities will have genuine shared interests, although not all members may be interested in all aspects. For example, fixed line telecom companies will not be interested in wireless problems, but will interested as interested as mobile companies in identifying hoax calls.

Members of effective communities will use empowered representatives that can make things happen internally.

Effective communities may limit or otherwise constrain membership, for example to ensure fair representation in decision making.

A.8 Scope of the ISMS for an information sharing community

The scope of the ISMS for an information sharing community should include:

— all processes used for the communication of information between community members, including intermediaries;

— the storage of information as relevant during the communication;

— the processes implemented by the relevant members to send and receive shared information;

— the processes implemented by community members for the destruction of shared information.

The scope should not include information security management processes implemented by the relevant community members to manage their own information security, and possibly covered by other information security management systems, apart from restrictions placed on the nature of the information to be shared and the interfaces to the information sharing system. The ISMS could be managed centrally by a supporting entity such as a TICE or WARP, or it could be managed collaboratively by the members of the community.

Annex B
(informative)

Establishing trust in information exchanges

B.1 Statement of trust

A recipient's degree of trust in a received statement is largely predicated on the degree to which the source of the message is trusted, and the source's own trust in the statement.

This is perhaps best encapsulated in the "5 by 5" model used within the law enforcement and intelligence communities:

— {A – E} Decreasing degree of trust in source;

— {1 – 5} Decreasing degree of trust placed by source in information.

Thus "A-1" information is expected to be implicitly trusted, whereas "E-5" information will typically be discarded.

But, of course, in the real world there is very little "A-1" information. Perhaps the best known examples where both the source and information are expected to be implicitly trusted, but for which occasional errors have to be expected, is the use of Global Positioning System (GPS) based satellite navigation systems, where instances of mapping or route planning system errors have been accidentally misleading, causing large vehicles to be misdirected down small tracks, which are often the basis of "light relief" items in the press.

A further issue with regard to trust in statements is the risk of specious reinforcement. There is an intrinsic tendency – or underlying assumption – that multiple instances of the same information from seemingly differing sources is confirmatory.

This, to some extent, is of course true, but such trust cannot be taken too literally, and, in particular, any mathematical model of such trust should not assign linear weighting to additional instances.

B.2 Technological support

B.2.1 Introduction

There are a number of technologies that have recently been developed to support trust in electronically supplied information generated by unknown or unfamiliar entities. Such technologies are closely associated with the concept of "Web 2.0"[3]. Web 2.0 is not a set of technologies – rather it is a philosophy/concept that relates to social media and incorporates ideas such as the use of the Web as a platform, harnessing collective intelligence, co-created (user generated) content, the social use of the Web etc.

Two facets of Web 2.0 are of particular relevance to this International Standard:

— pseudo anonymity;

— reputation systems, also called reputation engines.

B.2.2 Anonymity and pseudo-anonymity

Sources and recipients of information may wish to remain anonymous for a variety of reasons. The strength to which anonymity is actually achievable depends on the knowledge of the context i.e. how well

the entire messaging system is understood. In large, decentralized systems the messaging system may not be fully known to any participant, and in many cases the context of the message will change over time.

The concept of anonymity is tied to the concept of **unlinkability**, where items of interest are no more and no less related after any observation than they are related from a-priori knowledge.

Relationship anonymity implies a degree of untraceability as to who communicates with whom: thus, it is not possible to link an originator to the recipient or recipients.

Unobservability is being unable to observe when the originator sends and the recipient receives.

Relationship unobservability means it is not possible to observe the communication between the originator and the recipient.

Pseudonymity involves the replacing of a person's name and other identifying characteristics with a label, in order to prevent identification of the data subject or, at least, to make such identification substantially difficult. Being **pseudonymous** is the state of using a pseudonym as an identification label.

With respect to the degree of linkability, various types of pseudonyms may be possible:

a) *Person pseudonym*: A person pseudonym is a substitute for the holder's name which is regarded as representation for the holder's civil identity. It may be used in all contexts, e.g.: a number of an identity card; the social security number; DNA; a nickname; the pseudonym of an actor; or a mobile phone number.

b) *Role pseudonym:* The use of role pseudonyms is limited to specific roles, e.g., a customer pseudonym or an Internet account used for many instantiations of the same role "Internet user". The same role pseudonym may be used with different communication partners.

c) *Relationship pseudonym:* For each communication partner, a different pseudonym is used. This means that different communications partners cannot tell that they are communicating with the same user.

d) *Role-relationship pseudonym:* For each role and for each communication partner, a different role-relationship pseudonym is used. This means that the communication partner does not necessarily know whether two pseudonyms used in different roles belong to the same holder. On the other hand, two different communication partners who interact with a user in the same role do not know from the pseudonym alone whether it is the same user.

   EXAMPLE Suppose a source of information regularly uses the name "Wool" when communicating information not in the public domain to Bernstein, and uses the name "Touched" when communicating the same information to Woodward. Bernstein then receives information about a new subject from "Deep Throat" and Woodward from "Watergate". Bernstein and Woodward do not know if "Deep Throat" and "Watergate" are the same person and also do not know if "Deep Throat" is the same person as "Wool" or "Touched", or both.

e) *Transaction pseudonym:* For each transaction, a transaction pseudonym unlinkable to any other transaction pseudonyms (and at least initially unlinkable to any other transaction pseudonyms) is used, e.g., randomly generated transaction numbers for online-banking. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible.

In general, anonymity of both role pseudonyms and relationship pseudonyms is stronger than anonymity of person pseudonyms. The strength of anonymity increases with the application of role-relationship pseudonyms, the use of which is restricted to both the same role and the same relationship.

Anonymity is stronger if less personal data of the pseudonym holder can be linked to the pseudonym.

B.2.3 Reputation engines

The concept of a reputation engine forms the basis of many social media and social networks on the Web. Reputation engines are used to filter the most relevant information and they become more relevant as the quantity and variety of information increase dramatically.

A reputation engine can be defined as a formalized set of policies and procedures that are used to compute a reputation score for an individual based on their past activity. In the online world, a reputation engine is tied to the idea of a digital footprint. Digital footprints are traces of someone's activity in a digital environment.

Credit reports and other mechanisms have always provided a means to quantify reputation – but a comparison of the Web mechanisms of reputation (such as Internet auction ratings) to traditional credit reports is interesting. As we transact on the Web (buy, sell, borrow, repay) we create digital data. This data is captured by others (like credit rating agencies) and although it belongs to us – it is 'owned' by the credit rating agency (and indeed we may be charged for accessing it!).

There are more refined form of reputation engines such as the eBay reputation engine[1)]. The eBay engine differs from a credit score because it is transparent. Every piece of feedback (including negative feedback) is fed back to the person about whom the comment is made – thus giving an opportunity for appeal.

A reputation engine could be used to increase trust by incorporating insights from the wider community sources through tasks like: validating new information sources; validating content sources; real time alerts, such as Twitter search and Google alerts; reinforcing trust from unknown sources; complementing search by external insights; bringing in new/external ideas to the trusted sharing domain; forecasting opportunities and threats from external sources, etc. However, many current Web 2.0 technologies (e.g. wikis) have limitations for building trust since they do not have a robust trust model internally.

B.3 Assessing trustworthiness of information

The concepts underpinning trust are intrinsically of a subjective rather than objective nature and, as such, are not necessarily amenable to mechanistic representation. Nonetheless, a Pareto approach[4] can be taken to the problem: a solution where the majority of the desired result can be achieved with a relatively small amount of effort, although any attempt to perfect the model would require a disproportionate amount of effort.

Possible components of such an approach are:

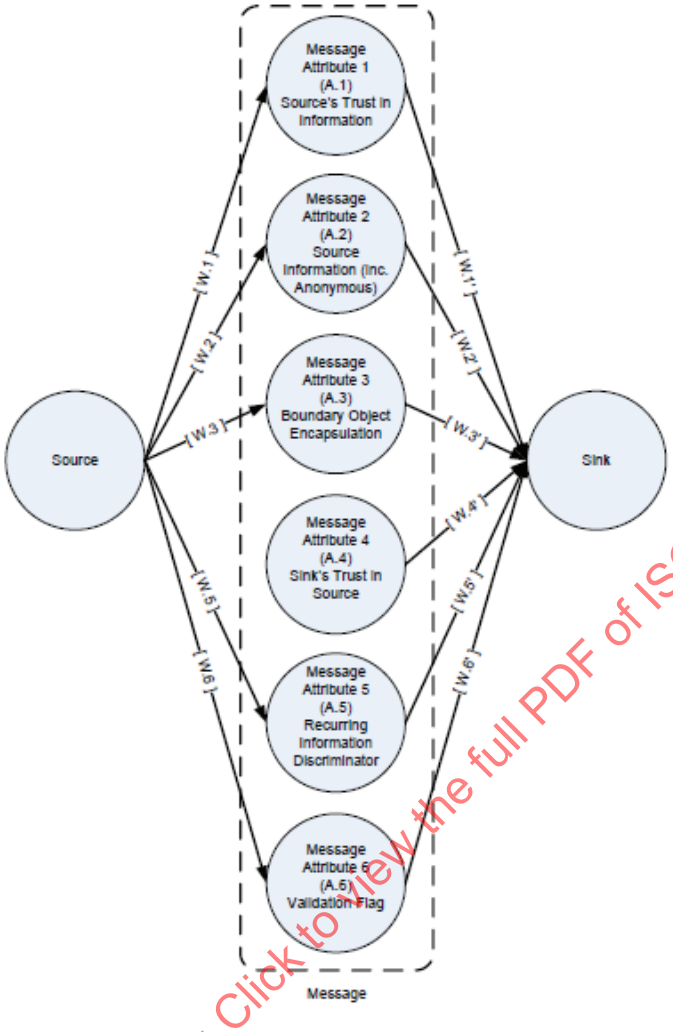
a) That originators of information should assign a degree of trust in information they publish. The usefulness of this approach has been validated by the United Kingdom's Centre for Protection of National Infrastructure, where it is used to automatically profile and disseminate warning information to a variety of information sharing communities.

b) That all information be clearly identified with its source, ideally using a structured data format.

c) Notwithstanding the concept of source identification, there should also be support for anonymous reporting, as experience from the safety world indicates that provision for anonymity significantly increases information sharing.

d) That the concept of a Boundary Object be used to encapsulate the substance of any information exchanged. Boundary Objects are structured assemblages of information that have a degree of mutual recognition within a community of interest, and as such both enable communication across linguistic and domain boundaries: the success of initiatives such as Mitre's Common Vulnerability Enumeration (CVE) notation is attributed in part to their de facto adoption as such Boundary Objects.

1) Names of products used in B.2.3 are examples of relevant products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of these products.



Key

W.n originator's judgement of trustworthiness of information in message

W.n' recipient's judgement of trustworthiness of information in message

Figure B.1 — Assessment of message content trustworthiness

e) That both originator and recipient of a trusted information exchange should provide an assessment as to whether, and how many times, the information is supportive of previously received content: although there is some scope for automated parsing of information for this purpose, it has to be recognized that automated parsing of messages for such purposes within the current state of the art is unreliable. To minimize the risks of specious reinforcement, a diminishing return Cumulative Distribution Function will need to be applied to the count of number of previous instances, which will therefore mean that the weighted value of additional information decreases as the count increases.

f) That the source or recipient assign a flag as to whether the information has been confirmed independently, to guard against enshrining so-called *urban legends* as useful information. This enshrines a further degree of critical scepticism about information received.

g) That recipients of information should assign a subjective rating of the source, based on the precepts of the "5 by 5" model (see B.1).

Suitably weighted, such criteria can enable members of an information sharing community to quantify the trust they can and should place in the information that they receive from other members of the community. This is represented pictorially in Figure B.1 above.

Annex C
(informative)

The Traffic Light Protocol

This annex describes the Traffic Light Protocol (TLP), a mechanism widely used in information sharing communities to indicate the permitted distribution of information. Although the basic concept is widely understood, there are a number of slightly different variations in use. This description is taken from the Good Practice Guide for Network Security Information Exchanges published by the European Network and Information Security Agency (ENISA).[5] The concept was originally developed by the UK's Centre for the Protection of National Infrastructure (CPNI).

The TLP was created in order to encourage greater sharing of sensitive information between organizations. The originator needs to signal how widely they want their information to be circulated beyond the immediate recipient, if at all.

The TLP is based on the concept of the originator labelling information with one of four colours to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required.

The four colours and their meanings are as follows:

— RED - Personal for Named Recipients Only. In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will be passed verbally or in person.

— AMBER - Limited Distribution. The recipient may share AMBER information with others within their organization, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.

— GREEN - Community Wide. Information in this category can be circulated widely within a particular community. However, the information may not be published or posted on the Internet, nor released outside of the community.

— WHITE – Unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

Sensitive information, howsoever provided by an originator, should be marked at the time of disclosure in accordance with the TLP. All sensitive information will be deemed to be AMBER unless otherwise stated or written. However, by default, and unless specifically stated otherwise at the time of disclosure, the identity of the source of the sensitive information will always be RED.

The TLP can also be adapted for use within an organization, for example, where only some individuals are granted full access to all shared information. See Figure 2.