SVENSK STANDARD
SS-ISO/IEC 27035:2012

Fastställd/Approved: 2012-03-29
Publicerad/Published: 2012-04-03
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 01.140.30; 03.100.01; 04.050; 33.040.40; 35.020; 35.040; 35.080

Informationsteknik – Säkerhetstekniker – Styrning och hantering av informationssäkerhetsincidenter (ISO/IEC 27035:2011, IDT)

Information technology – Security techniques – Information security incident management (ISO/IEC 27035:2011, IDT)

Provläsningsexemplar / Preview

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Provläsningsexemplar / Preview

Den internationella standarden ISO/IEC 27035:2011 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO/IEC 27035:2011.

The International Standard ISO/IEC 27035:2011 has the status of a Swedish Standard. This document contains the official version of ISO/IEC 27035:2011.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Informationssäkerhet, SIS/TK 318.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Provläsningsexemplar / Preview

Provläsningsexemplar / Preview

Contents

Page

Provläsningsexemplar / Preview

Provläsningsexemplar / Preview

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27035 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035 cancels and replaces ISO/IEC TR 18044:2004, which has been technically revised.

Provläsningsexemplar / Preview

Introduction

In general, information security policies or controls alone will not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can make information security ineffective and thus information security incidents possible. This can potentially have both direct and indirect adverse impacts on an organization's business operations. Further, it is inevitable that new instances of previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any response less effective, and increase the degree of potential adverse business impact. Therefore, it is essential for any organization serious about information security to have a structured and planned approach to:

- detect, report and assess information security incidents;
- respond to information security incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas);
- report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

This International Standard provides guidance on information security incident management in Clause 4 to Clause 9. These clauses consist of several subclauses, which include a detailed description of each phase.

The term ‘information security incident management’ is used in this International Standard to encompass the management of not just information security incidents but also information security vulnerabilities.

Provläsningsexemplar / Preview

Information technology — Security techniques — Information security incident management

1 Scope

This International Standard provides a structured and planned approach to:

a) detect, report and assess information security incidents;

b) respond to and manage information security incidents;

c) detect, assess and manage information security vulnerabilities; and

d) continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

This International Standard provides guidance on information security incident management for large and medium-sized organizations. Smaller organizations can use a basic set of documents, processes and routines described in this International Standard, depending on their size and type of business in relation to the information security risk situation. It also provides guidance for external organizations providing information security incident management services.

2 Normative references

The following referenced documents are indispensable for the application of this document. 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

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

3.1
information security forensics
application of investigation and analysis techniques to capture, record and analyse information security incidents

3.2
information security incident response team
ISIRT
team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle

Provläsningsexemplar / Preview

NOTE The ISIRT as described in this International Standard is an organizational function that covers the process for information security incidents and is focused mainly on IT related incidents. Other common functions (with similar abbreviations) within the incident handling may have a slightly different scope and purpose. The following commonly used abbreviations have a meaning similar to that of ISIRT, though not exactly the same:

- CERT: A Computer Emergency Response Team mainly focuses on Information and Communications Technology (ICT) incidents. There may be other specific national definitions for CERT.
- CSIRT: A Computer Security Incident Response Team is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. These services are usually performed for a defined constituency, which could be a parent entity such as a corporation, governmental organization, or educational organization; a region or country; a research network; or a paid client.

3.3
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant

[ISO/IEC 27000:2009]

3.4
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[ISO/IEC 27000:2009]

4 Overview

4.1 Basic concepts

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

The occurrence of an information security event does not necessarily mean that an attempt has been successful or that there are any implications on confidentiality, integrity and/or availability, i.e. not all information security events are classified as information security incidents.

A threat acts in unwanted ways to exploit the vulnerabilities (weaknesses) of information systems, services or networks, which is the occurrence of information security events and potentially causes unwanted incidents to information assets exposed by the vulnerabilities. Figure 1 shows this relationship of objects in an information security incident chain. The shaded objects are pre-existing, affected by the unshaded objects in the chain that results in an information security incident.

Provläsningsexemplar / Preview

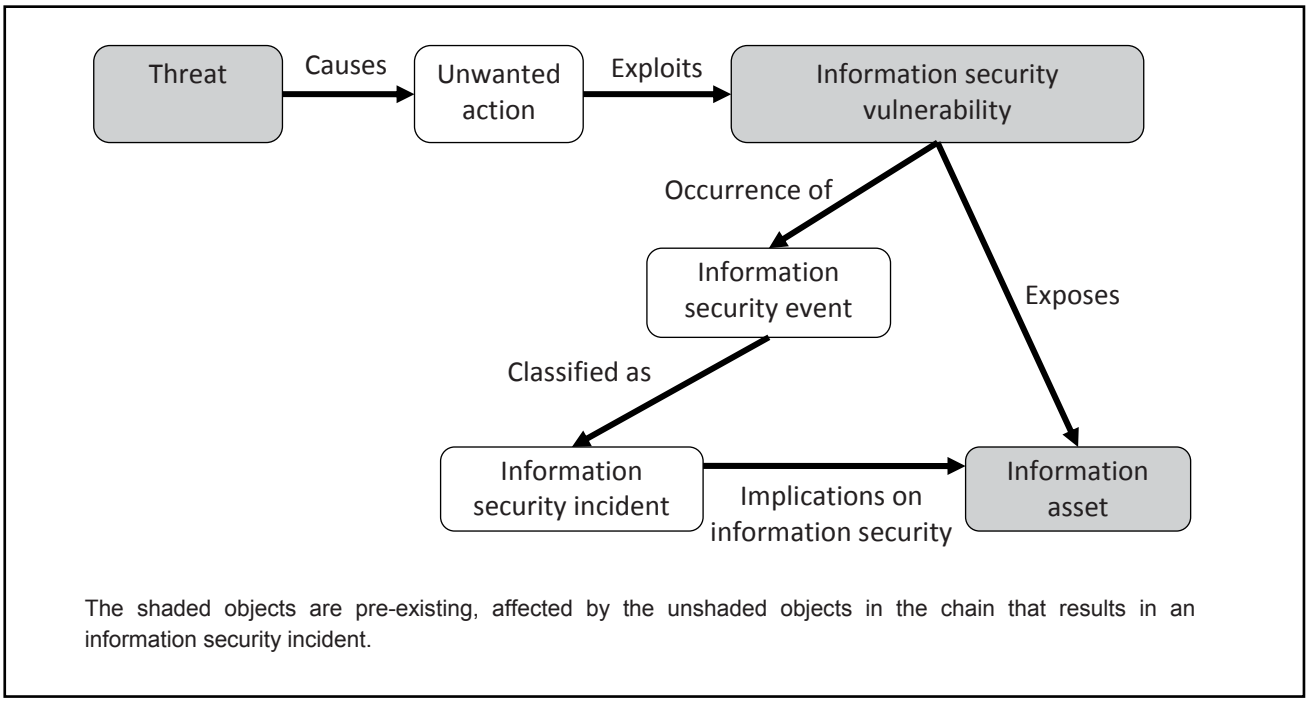

Figure 1 — The relationship of objects in an information security incident chain

4.2 Objectives

As a key part of an organization's overall information security strategy, the organization should put controls and procedures in place to enable a structured well-planned approach to the management of information security incidents. From a business perspective, the prime objective is to avoid or contain the impact of information security incidents to reduce the direct and indirect costs caused by the incidents.

The primary steps to minimize the direct negative impact of information security incidents are the following:

- stop and contain,
- eradicate,
- analyse and report, and
- follow up.

The objectives of a structured well-planned approach are more refined and should ensure the following:

a) Information security events are detected and dealt with efficiently, in particular in identifying whether they need to be categorized and classified as information security incidents or not.

b) Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.

c) The adverse effects of information security incidents on the organization and its business operations are minimized by appropriate controls as part of the incident response, possibly in conjunction with relevant elements from a crisis management plan or plans.

d) Reported information security vulnerabilities are assessed and dealt with appropriately.

e) Lessons are learnt quickly from information security incidents, vulnerabilities and associated management. This is to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management scheme.