Contents

فهرست

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electro technical 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 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

پیشگفتار

ISO (سازمان بین‌المللی استانداردسازی) و IEC (کمیسیون بین‌المللی الکتروتکنیک) در کنار هم سیستم تخصصی را برای استانداردسازی جهانی تشکیل می‌دهند. بنابراین آن‌دسته از موسسات ملی که از اعضای ISO یا IEC به شمار می‌روند، از طریق کمیته‌های فنی که توسط سازمان‌های مرتبط تشکیل شده‌اند، در تدوین استانداردهای بین‌المللی مشارکت نموده و فیلدهای خاص فعالیت‌های فنی را مورد بررسی قرار می‌دهند. کمیته‌های فنی ISO یا IEC در فیلدهایی که مورد علاقه طرفین می‌باشد، با یکدیگر همکاری می‌نمایند. در این میان سایر سازمان‌های بین المللی، سازمان‌های دولتی و غیر دولتی در کنار ISO یا IEC در این‌گونه فعالیت‌ها شرکت می‌کنند. ISO و IEC در زمینه فناوری اطلاعات، یک کمیته فنی مشترک را تأسیس نموده‌اند که اصطلاحاً ISO/IEC JTC 1 نام دارد.

پیش‌نویس استانداردهای بین‌المللی بر اساس مقررات بیان شده در دستورالعمل‌های ISO/IEC تهیه می‌شوند. بخش ۲.

تهیه استانداردهای بین‌المللی از مهمترین وظیفه کمیته فنی مشترک به شمار می‌آید. پیش‌نویس استانداردهای بین‌المللی که توسط کمیته فنی مشترک برگزیده شده است، جهت رأی‌گیری به هیأت‌ها و مجامع ملی به جریان می‌افتد. انتشار استاندارد به صورت استاندارد بین‌المللی نیازمند تایید از سوی حداقل ۷۵ % از آراء هیأت‌ها و سازمان‌های ملی می‌باشد.

در ادامه توجه فرمائید که برخی از بخش‌های این سند ممکن است مشمول حقوق ثبت اختراع باشد و لذا ISO و IEC در قبال تعیین تمام یا بخشی از این حقوق مسئول شناخته نخواهد شد.

ISO/IEC 27001 توسط کمیته فنی مشترک ISO/IEC JTC1، فناوری اطلاعات، کمیته فرعی SC 27، تکنیک‌های امنیتی فناوری اطلاعات تهیه شده است.

0. Introduction

0. 1.General

This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

This International Standard can be used in order to assess conformance by interested internal and external parties.

0. 2. Process approach

This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

۰. مقدمه

۰. ۱. کلیات

هدف از تهیه این استاندارد بین‌المللی، ارائه مدلی است که بر اساس آن بتوان یک سیستم مدیریت امنیت اطلاعات را ایجاد، اجرا، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود و ارتقاء بخشید. پیاده‌سازی چنین سیستمی می‌بایست برای یک سازمان به عنوان یک تصمیم استراتژیک تلقی گردد. در این میان عواملی مانند نیازها و اهداف سازمان‌ها، الزامات امنیتی، فرآیندهای به کار گرفته شده و اندازه و ساختار سازمان بر طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان تاثیر خواهند گذاشت. لذا ایجاد تغییر در این سیستم و سیستم‌های پشتیبان به مرور زمان چندان دور از انتظار نخواهد بود. در این میان انتظار می‌رود که پیاده‌سازی چنین سیستمی را بتوان بر اساس نیازهای سازمان رتبه‌بندی نمود. به عنوان مثال یک موقعیت ساده، یقیناً به یک راه حل ساده سیستم مدیریت امنیت اطلاعات نیاز خواهد داشت.

این استاندارد بین‌المللی می‌تواند توسط اشخاص درون سازمانی و برون سازمانی به منظور ارزشیابی میزان انطباق مورد استفاده قرار گیرد.

۰. ۲. رویکرد فرآیندی

در این استاندارد بین‌المللی به منظور ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات یک سازمان از رویکرد فرآیندی استفاده شده است.

یک سازمان برای این که عملکرد اثربخشی داشته باشد، باید فعالیت‌های متعددی را شناسایی و مدیریت کند. هرگونه فعالیت که در آن از منابع استفاده می‌شود و برای تبدیل ورودی‌ها به خروجی‌ها مورد مدیریت قرار می‌گیرد را می‌توان به عنوان یک فرآیند در نظر گرفت. در اغلب اوقات، خروجی یک فرآیند مستقیماً و بدون هیچ گونه واسطه‌ای ورودی فرآیند بعدی را تشکیل می‌دهد.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a “process approach”.

The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) understanding an organization’s information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks;

c) monitoring and reviewing the performance and effectiveness of the ISMS; and

d) continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)[1]governing the security of information systems and networks.

1 OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

به کاربرد سیستم فرآیندها در یک سازمان و همچنین شناسایی و تعامل این فرآیندها و مدیریت آن‌ها اصطلاحاً "رویکرد فرآیندی" گفته می‌شود.

رویکرد فرآیندی در مدیریت امنیت اطلاعات به نحوی که در این استاندارد بین‌المللی آورده شده است، کاربران را برای تأکید بر اهمیت موارد زیر تشویق می‌کند:

الف) شناخت الزامات امنیت اطلاعات و نیاز به سیاست‌گذاری و هدف‌گذاری برای امنیت اطلاعات؛

ب) پیاده‌سازی و بهره‌برداری از موارد کنترلی به منظور مدیریت مخاطره‌های امنیت اطلاعات یک سازمان در چارچوب مجموعه مخاطره‌های کسب‌وکار سازمان؛

پ) پایش و بازنگری اجرا و اثربخشی سیستم مدیریت امنیت اطلاعات ؛ و

ت) بهبود مستمر بر اساس اندازه‌گیری هدف.

در استاندارد بین‌المللی حاضر از مدل PDCA (برنامه‌ریزی، اجرا، کنترل، اقدام) استفاده شده‌است. از این مدل برای تعیین ساختار تمامی فرآیندهای سیستم مدیریت امنیت اطلاعات استفاده می‌شود. شکل ۱ نشان می‌دهد که یک سیستم مدیریت امنیت اطلاعات چگونه الزامات و انتظارات امنیت اطلاعات طرف‌های ذینفع را به عنوان ورودی دریافت می‌کند، و از طریق اقدامات لازم و فرآیندها، خروجی‌های امنیت اطلاعات را به نحوی تولید می‌نماید که آن نیازمندی‌ها، الزامات و انتظارات را برآورده نماید. شکل ۱ همچنین روابط موجود در فرآیندهای ارائه شده در بند ۴، ۵، ۶، ۷ و ۸ را نشان می‌دهد.

پذیرش مدل PDCA همچنین بیانگر اصول حاکم بر امنیت شبکه‌ها و سیستم‌های اطلاعاتی می‌باشد، اصولی که در رهنمودهای OECD[1](2002) بیان شده است.

۱راهنمای OECD برای امنیت سیستم‌های اطلاعاتی و شبکه‌ها –به سوی فرهنگ امنیت. پاریس OECD، جولای ۲۰۰۲، www.oecd.org

This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

EXAMPLE 1
A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2
An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

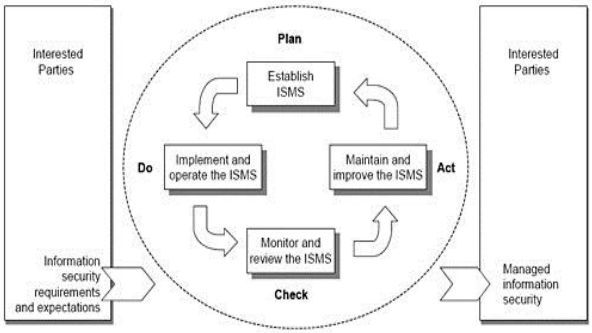
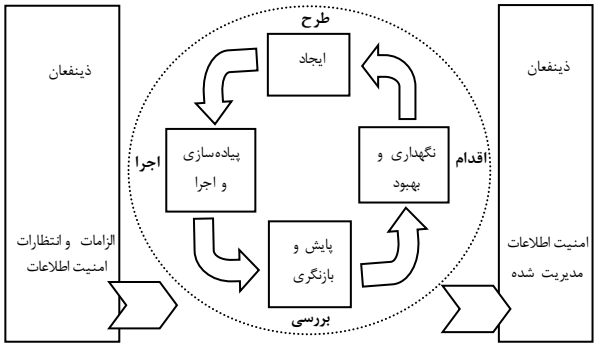


Figure 1 – PDCA model applied to ISMS processes

استاندارد بین‌المللی حاضر مدل کامل و جامعی را ارائه می‌نماید، که به کمک آن می‌توان اصول مندرج در رهنمودهای حاکم بر ارزیابی مخاطره، طراحی و پیاده‌سازی امنیت، مدیریت امنیت و ارزیابی مجدد را اجرا نمود.

مثال ۱:
یک الزام می‌تواند این باشد که نقض امنیت اطلاعات، خسارات مالی جدی را برای یک سازمان به دنبال نداشته باشد، و یا موجب ایجاد مشکل برای سازمان نشود.

مثال ۲:
یک انتظار می‌تواند این باشد که در صورت بروز یک رویداد جدی به عنوان مثال هک شدن وب سایت تجارت الکترونیکی سازمان افرادی با سطح دانش کافی باید در سازمان حضور داشته باشند تا طبق رویه‌های مناسب اثر این رویداد را به حداقل کاهش دهند.



شکل ۱- مدل PDCA بکار برده شده در فرایندهای سیستم مدیریت امنیت اطلاعات

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

0. 3. Compatibility with other management systems

This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management systemcan thus satisfy the requirements of all these standards. Table C.1 illustrates the relationship between the clauses of this International Standard, ISO 9001:2000 and ISO 14001:2004.

This International Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

طرح (ایجاد سیستم مدیریت امنیت اطلاعات)	ایجاد خط‌مشی سیستم مدیریت امنیت اطلاعات، اهداف، فرآیندها و رویه‌های متناسب با مدیریت مخاطره و بهبود امنیت اطلاعات به منظور حصول نتایج مطابق با خط مشی و اهداف کلان سازمان
اجرا (اجرا و راه-اندازی سیستم مدیریت امنیت اطلاعات)	پیاده‌سازی و اجرای خط مشی سیستم مدیریت امنیت اطلاعات، کنترل‌ها، فرآیندها و رویه‌ها.
کنترل (پایش و بازنگری سیستم مدیریت امنیت اطلاعات)	ارزیابی و در صورت امکان سنجش، عملکرد فرایند مطابق با خط‌مشی سیستم مدیریت امنیت اطلاعات، اهداف و تجربه عملی، و ارائه نتایج به مدیریت جهت بازنگری
اقدام (نگهداری و بهبود سیستم مدیریت امنیت اطلاعات)	اتخاذ اقدامات اصلاحی یا پیشگیرانه براساس نتایج ممیزی داخلی سیستم مدیریت امنیت اطلاعات و بازنگری مدیریت یا سایر اطلاعات مرتبط، برای تحقق بهبود مستمر سیستم مدیریت امنیت اطلاعات

۰. ۳. سازگاری با سایر سیستم‌های مدیریت

استاندارد بین‌المللی حاضر به منظور پشتیبانی از اجرای سازگار و یکپارچه و عملکرد هماهنگ با استانداردهای مدیریت مرتبط، از هر نظر با استاندارد ایزو ۹۰۰۱:۲۰۰۰ و ایزو ۱۴۰۰۱:۲۰۰۴ مطابقت و سازگاری دارد؛ بنابراین یک سیستم مدیریت که به درستی طراحی شده باشد می‌تواند الزامات تمامی این استانداردها را برآورده و تامین نماید. جدول شماره پ.۱ روابط حاکم بین بندهای استاندارد حاضر، ایزو ۹۰۰۱:۲۰۰۰ و ایزو ۱۴۰۰۱:۲۰۰۴ را نشان می‌دهد.

استاندارد بین‌المللی حاضر به‌گونه‌ای طراحی شده است که سازمان را قادر نماید تا سیستم مدیریت امنیت اطلاعات خود را با الزامات سیستم مدیریت مربوطه هماهنگ و سازگار و یا ادغام نماید.

Information technology — Security techniques — Information security management systems — Requirements

IMPORTANT — This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with an International Standard does not in itself confer immunity from legal obligations.

1. Scope

1.1. General

This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

NOTE1: References to 'business' in this International Standard should be interpreted broadly to mean those activities that are core to the purposes for the organization's existence.

NOTE 2: ISO/IEC 17799 provides implementation guidance that can be used when designing controls.

فناوری اطلاعات – فنون امنیتی – سیستم مدیریت امنیت اطلاعات – الزامات

مهم : سندی که در مقابل شما قرار دارد دربردارنده تمام مفاد لازم و ضروری یک قرارداد نمی‌باشد مسئولیت استفاده صحیح از این سند بر عهده کاربران قرار دارد. انطباق با استاندارد بین‌المللی به خودی خود به معنای مصونیت در برابر مسئولیت‌های قانونی نخواهد بود.

۱. دامنه کاربرد

۱.۱. کلیات

استاندارد بین‌المللی حاضر تمام سازمان‌ها (به عنوان مثال موسسات کسب‌وکار، موسسات دولتی و سازمان‌های غیرانتفاعی) را شامل می‌گردد. این استاندارد بین‌المللی الزامات مربوط به ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود یک سیستم مدیریت امنیت اطلاعات مستندسازی شده در قالب مخاطره‌های کسب‌وکار کلی سازمان را تعیین و بیان می‌نماید. استاندارد حاضر، الزامات مربوط به پیاده‌سازی کنترل‌های امنیتی که بر اساس نیازهای هر یک از سازمان‌ها یا بخش‌های مربوط به آن‌ها اختصاص داده شده‌اند را تعیین و بیان می‌نماید.

سیستم مدیریت امنیت اطلاعات به‌گونه‌ای طراحی شده است که انتخاب کنترل‌های امنیتی کافی و متناسب را تضمین می‌نماید و با استفاده از همین کنترل‌های امنیتی خواهد بود که دارایی‌های اطلاعاتی محافظت شده و به این ترتیب به طرفین ذینفع اطمینان خاطر داده می‌شود.

یادآوری ۱ : منظـور از " کسب‌وکار"در متن اسـتـاندارد بین‌المللی حاضر، آن‌دسته از فعالیت‌هایی هستند که برای اهدافی که سازمان بر آن اساس ایجاد شده است اهمیت اساسی دارند.

یادآوری ۲ : ISO/IEC17799 در بردارنده رهنمودهایی برای پیاده‌سازی است و لذا در زمان طراحی کنترل‌ها می‌توان از آن استفاده نمود.

1.2. Application

The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard.

Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons. Where any controls are excluded, claims of conformity to this International Standard are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable legal or regulatory requirements.

NOTE: If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system.

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 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

۱.۲. کاربرد

الزامات بیان شده در استاندارد بین‌المللی حاضر، الزاماتی کلی و عمومی هستند و به‌گونه‌ای در نظر گرفته شده‌اند که در تمامی سازمان‌ها علی‌رغم نوع، اندازه و ماهیتی که دارند کاربرد داشته باشند. در صورت اقامه هر گونه ادعا از سوی یک سازمان در خصوص مطابقت با استاندارد بین‌المللی حاضر، به جز الزامات بیان شده در ماده ۴، ۵، ۶، ۷ و ۸ قابل پذیرش نخواهد بود.

در صورتی که حذف هر یک از کنترل‌ها برای برآورده شدن معیارهای پذیرش مخاطره ضروری تشخیص داده شود، می بایست توجیه شده و مدارک و شواهد لازم ارائه گردد به‌گونه‌ای که مخاطره‌های وارد بر آن از سوی افراد مسئول مورد پذیرش قرار گیرد.

در صورت حذف هر یک از کنترل‌ها، هر گونه ادعا در خصوص مطابقت با استاندارد بین‌المللی حاضر پذیرفته نخواهد بود، مگر آن که چنین حذفی بر توانایی سازمان و یا مسئولیت سازمان تاثیری نداشته باشد و امنیت اطلاعات نیز باید به‌گونه‌ای باشد که الزامات امنیتی تعیین شده بر اساس ارزشیابی مخاطره و الزامات قانونی و انتظامی را برآورده نماید.

یادآوری : چنانچه سازمانی از قبل دارای یک سیستم مدیریت فرایند کسب‌وکار در حال اجرا باشد (به عنوان مثال در ارتباط با ایزو ۹۰۰۱ یا ایزو ۱۴۰۰۱)، بهتر است که در اغلب موارد الزامات استاندارد بین‌المللی حاضر را در قالب سیستم مدیریت فعلی برآورده نماید.

۲. مراجع الزامی

مستنداتی که در ذیل از آنها نامبرده شده است برای استفاده از سند حاضر ضروری هستند. در مورد مراجع دارای تاریخ، تنها نسخه‌های نامبرده شده قابل استفاده خواهند بود. در مورد مراجع بدون تاریخ، جدیدترین نسخه سند ارجاع شده (شامل هر گونه اصلاحیه) معتبر و قابل استفاده خواهد بود.

ISO/IEC 17799:2005، فناوری اطلاعات- تکنیک‌های امنیت- آیین نامه اجرایی مدیریت امنیت اطلاعات.

3. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1. asset

anything that has value to the organization
[ISO/IEC 13335-1:2004]

3.2. availability

the property of being accessible and usable upon demand by an authorized entity
[ISO/IEC 13335-1:2004]

3.3. confidentiality

the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
[ISO/IEC 13335-1:2004]

3.4. information security

preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
[ISO/IEC 17799:2005]

3.5. information security event

an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
[ISO/IEC TR 18044:2004]

۳. اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود.

۳.۱. دارایی

هر چیزی که از نظر سازمان ارزشمند باشد.
[ISO/IEC 13335-1:2004]

۳.۲. دسترس پذیری

به محض درخواست از سوی یک موجودیت مجاز، دارایی در دسترس و قابل استفاده باشد.
[ISO/IEC 13335-1:2004]

۳.۳. محرمانگی

به این معنا خواهد بود که اطلاعات در دسترس افراد، موسسات یا فرآیندهای غیرمجاز قرار نخواهد گرفت و برای ایشان افشا نخواهد شد.
[ISO/IEC 13335-1:2004]

۳.۴. امنیت اطلاعات

حفظ محرمانگی، یکپارچگی و در دسترس بودن اطلاعات و همچنین سایر دارایی‌ها مانند سندیت، مسئولیت‌پذیری، عدم انکار و قابلیت اطمینان را شامل می‌گردد.
[ISO/IEC 17799:2005]

۳.۵. رویداد امنیت اطلاعات

یک واقعه مشخص از یک حالت سیستم، سرویس یا شبکه که نشان‌دهنده نقض احتمالی خط‌مشی امنیت اطلاعات یا ***نقض تامین*** حفاظتی بوده یا نشان‌دهنده یک موقعیت ناشناخته درگذشته می‌باشد که ممکن است به‌نحوی با امنیت در ارتباط باشد.
[ISO/IEC TR 18044:2004]

3.6. information security incident

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
[ISO/IEC TR 18044:2004]

3.7. information security management system(ISMS)

that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.8. integrity

the property of safeguarding the accuracy and completeness of assets
[ISO/IEC 13335-1:2004]

3.9. residual risk

the risk remaining after risk treatment
[ISO/IEC Guide 73:2002]

3.10. risk acceptance

decision to accept a risk
[ISO/IEC Guide 73:2002]

3.11. risk analysis

systematic use of information to identify sources and to estimate the risk
[ISO/IEC Guide 73:2002]

۳. ۶ حادثه امنیت اطلاعات

یک یا مجموعه‌ای از رویدادهای ناخواسته یا پیش‌بینی نشده امنیت اطلاعات که به احتمال بسیار بالا فعالیت‌های کسب‌وکار را به مخاطره می‌اندازد و امنیت اطلاعات را تهدید می‌نماید.
[ISO/IEC TR 18044:2004]

۳. ۷ سیستم مدیریت امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات بخشی از سیستم کلی مدیریت به‌شمار می‌رود و مبتنی بر رویکرد مخاطره کسب‌وکار بوده و هدف از آن ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات می‌باشد.
یادآوری : سیستم مدیریت شامل ساختار سازمانی، سیاست‌ها، خط‌مشی‌ها، فعالیت‌های برنامه‌ریزی، مسئولیت‌ها، روش‌ها، رویه‌ها، فرآیندها و منابع می‌شود.

۳. ۸ یکپارچگی

مشخصه‌ی حفاظت از دقت و تمامیت دارایی‌ها می‌باشد.
[ISO/IEC 13335-1:2004]

۳. ۹ مخاطره باقیمانده

منظور از آن مخاطره‌ای است که پس از برطرف‌سازی مخاطره‌ها هم‌چنان باقیمانده است.
[ISO/IEC Guide 73:2002]

۳. ۱۰ پذیرش مخاطره

به معنای تصمیم‌گیری در خصوص پذیرش مخاطره می‌باشد.
[ISO/IEC Guide 73:2002]

۳. ۱۱ تجزیه و تحلیل مخاطره

به معنای استفاده سیستماتیک از اطلاعات جهت تعیین و شناسایی منابع و برآورد مخاطره می‌باشد.
[ISO/IEC Guide 73:2002]

3.12. risk assessment

overall process of risk analysis and risk evaluation
[ISO/IEC Guide 73:2002]

3.13. risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of the risk
[ISO/IEC Guide 73:2002]

3.14. risk management

coordinated activities to direct and control an organization with regard to risk
[ISO/IEC Guide 73:2002]

3.15. risk treatment

process of selection and implementation of measures to modify risk
[ISO/IEC Guide 73:2002]
NOTE: In this International Standard the term 'control' is used as a synonym for 'measure'.

3.16. statement of applicability

documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.
NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security.

۳. ۱۲. ارزشیابی مخاطره

منظور از آن، فرآیند کلی تجزیه و تحلیل وبررسی مخاطره می‌باشد.
[ISO/IEC Guide 73:2002]

۳. ۱۳. ارزیابی مخاطره

به فرآیند مقایسه مخاطره برآورد شده بر اساس معیارهای مخاطره تعیین شده اطلاق می‌شود که به منظور تعیین اهمیت مخاطره انجام می‌گردد.
[ISO/IEC Guide 73:2002]

۳. ۱۴. مدیریت مخاطره

به فعالیت‌های هماهنگ شده‌ای اطلاق می‌شود که با در نظر گرفتن مخاطره به منظور هدایت و کنترل یک سازمان انجام می‌شوند.
[ISO/IEC Guide 73:2002]

۳. ۱۵. برخورد با مخاطره

به فرآیند انتخاب و پیاده‌سازی معیارها جهت تعدیل مخاطره اطلاق می‌شود.
[ISO/IEC Guide 73:2002]
توجه : در این استاندارد بین المللی عبارت "اندازه‌گیری" معادل "کنترل" استفاده شده است.

۳. ۱۶. بیانیه کاربرد پذیری

به گزارش مستندی اطلاق می‌شود که مشخص‌کننده اهداف کنترلی و کنترل‌های مرتبط و قابل اجرا در سیستم مدیریت امنیت اطلاعات سازمان می‌باشد.
یادآوری : اهداف کنترلی و کنترل‌ها مبتنی بر نتایج ارزشیابی مخاطره و فرآیندهای اتخاذ تدبیر برای برخورد با مخاطره، الزامات قانونی، تعهدات قراردادی و الزامات کسب‌وکار سازمان در رابطه با امنیت اطلاعات می‌باشند.

4. Information security management system

4.1. General requirements

The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization's overall business activities and the risks it faces. For the purposes of this International Standard the process used is based on the PDCA model shown in Figure 1.

4.2. Establishing and managing the ISMS

4.2.1. Establish the ISMS

The organization shall do the following :

a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope (see 1.2).

b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

1) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;

2) takes into account business and legal or regulatory requirements, and contractual security obligations;

3) aligns with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place;

۴. سیستم مدیریت امنیت اطلاعات

۴.۱. الزامات عمومی

سازمان باید در چارچوب فعالیت‌های کلان کسب‌وکار خود و مخاطراتی که با آن‌ها مواجه است یک سیستم مدیریت امنیت اطلاعات مستند را ایجاد، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود بخشد. فرآیند به‌کار برده شده در راستای استاندارد بین‌المللی حاضر مبتنی بر مدل PDCA می‌باشدکه درشکل شماره ۱ نشان داده شده است.

۴.۲. ایجاد و مدیریت بر سیستم مدیریت امنیت اطلاعات

۴.۲.۱. ایجاد سیستم‌مدیریت امنیت اطلاعات

سازمان باید نسبت به انجام آنچه که در ذیل آمده است اقدام نماید:

الف) تعیین دامنه، حدود و مرزهای سیستم مدیریت امنیت اطلاعات بر حسب مشخصات فعالیت کسب‌وکار، سازمان، مکان آن، دارایی‌ها و فناوری و جزئیات آن و توجیهات مربوط به هر یک از حذفیات از دامنه (۱-۲ را مشاهده کنید)

ب) تعیین خطمشی سیستم مدیریت امنیت اطلاعات بر حسب مشخصات فعالیت‌های کسب‌وکار، سازمان، مکان آن، دارایی‌ها و فناوری‌هایی که:

۱) شامل چارچوبی برای تعیین اهداف و مبنای درک کلان راهبری و اصولی برای اقدام با تمرکز به امنیت اطلاعات باشد.

۲) الزامات کسب‌وکار و الزامات قانونی یا آیین‌نامه‌ای، و تعهدات قراردادی امنیت را مد نظر قرار دهد.

۳) آن را با ساختار مدیریت راهبردی مخاطره سازمان همراستا نماید، ساختاری که ایجاد و نگهداری سیستم مدیریت امنیت اطلاعات در آن شکل خواهد گرفت.

4) establishes criteria against which risk will be evaluated (see 4.2.1c)); and

5) has been approved by management.

NOTE: For the purposes of this International Standard, the ISMS policy is considered as a superset of the information security policy. These policies can be described in one document.

c) Define the risk assessment approach of the organization.

1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

2) Develop criteria for accepting risks and identify the acceptable levels of risk. (see 5.1f)

The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

NOTE: There are different methodologies for risk assessment. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security.*

d) Identify the risks.

1) Identify the assets within the scope of the ISMS, and the owners [1]) of these assets.

2) Identify the threats to those assets.

3) Identify the vulnerabilities that might be exploited by the threats.

1 The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

۴) معیارهای پذیرش که مخاطره بر اساس آن‌ها مورد ارزیابی قرار خواهند گرفت را تعیین نماید (به بند ۴-۲-۱-پ مراجعه نمایید)

و

۵) توسط مدیریت تصویب شده باشد.

یادآوری : خط‌مشی سیستم مدیریت امنیت اطلاعات با توجه به استاندارد بین‌المللی حاضر به عنوان یک سند بالادستی خط‌مشی امنیت اطلاعات در نظر گرفته می‌شود. این خط‌مشی‌ها را می‌توان در یک سند توصیف نمود.

پ) تعیین رویکرد ارزشیابی مخاطره سازمان.

۱) متدولوژی ارزشیابی مخاطره که از هر حیث مناسب با سیستم مدیریت امنیت اطلاعات، امنیت اطلاعات کسب‌وکار شناسایی شده و الزامات قانونی و آیین‌نامه‌ای باشد را تعیین نماید.

۲) معیارهای پذیرش مخاطره را ایجاد نموده و سطوح قابل پذیرش مخاطره را مشخص سازد.(به بخش ۵-۱ مراجعه نمایید.)

متدولوژی ارزشیابی مخاطره انتخاب شده باید قابل مقایسه بودن و قابل تکرار بودن نتایج ناشی از ارزشیابی مخاطره را تضمین نماید.

یادآوری: متدولوژی‌های متفاوتی برای ارزشیابی مخاطره وجود دارد. مثال‌های مربوط به متدولوژی‌های ارزشیابی مخاطره در ISO/IEC TR 13335-3، *فن‌آوری اطلاعات - رهنمودهای مربوط به مدیریت امنیت فناوری اطلاعات – تکنیک‌های مدیریت امنیت فناوری اطلاعات* مورد بحث و بررسی قرارگرفته است.

ت) شناسایی مخاطره‌ها.

۱) شناسایی دارایی‌ها در چارچوب دامنه سیستم مدیریت امنیت اطلاعات و صاحبان[1] دارایی‌ها.

۲) شناسایی تهدیدهایی که متوجه دارایی‌ها است.

۳) شناسایی نقاط آسیب‌پذیر که ممکن است از سوی عوامل تهدیدکننده مورد استفاده قرار گیرند.

۱عبارت مالک اشاره به فرد یا موجودیتی دارد که مسئولیتش برای کنترل، تولید، توسعه، نگهداری، استفاده، و امنیت دارائی توسط مدیریت تائید شده است. عبارت مالک اشاره به فردی نیست که مستقیماً به دارایی دسترسی دارد

4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

e) Analyse and evaluate the risks.

1) Assess the business impacts upon the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risks are acceptable or require treatment using the criteria for accepting risks established in 4.2.1c)2).

f) Identify and evaluate options for the treatment of risks.

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies and the criteria for accepting risks (see 4.2.1c)2));

3) avoiding risks; and

4) transferring the associated business risks to other parties, e.g. insurers, suppliers

۴) شناسایی تاثیرات امکان از بین رفتن محرمانگی، یکپارچگی و در دسترس بودن دارایی‌ها.

ث) تجزیه و تحلیل و ارزیابی مخاطره‌ها .

۱) ارزشیابی اثرات کسب‌وکار بر سازمان با در نظرگرفتن پیامدهای از دست رفتن محرمانگی، یکپارچگی یا دسترس‌پذیری دارایی‌ها که ممکن است ناشی از نواقص امنیتی باشد.

۲) ارزشیابی واقع‌بینانه احتمال وقوع نواقص امنیتی در نتیجه تهدیدات و آسیب‌پذیری‌های متداول و تاثیرات آن بر دارایی‌ها و کنترل‌هایی که در حال حاضر انجام می‌شوند.

۳) برآورد سطوح مخاطره.

۴) تعیین اینکه مخاطره‌ها قابل پذیرش هستند یا نیازمند اتخاذ تدابیر لازم هستند با استفاده از معیارهای پذیرش مخاطره مندرج در بند ۴-۲-۱-پ-۲ .

ج) شناسایی و ارزیابی راهکارهایی برای برخورد با مخاطره‌ها.

اقدامات ممکن شامل موارد زیر هستند:

۱) بکار بردن کنترل‌های مناسب،

۲) پذیرش آگاهانه و هدفمند مخاطره‌ها، مشروط بر این که خط-مشی‌های سازمان و معیارهای پذیرش مخاطره بطور کامل بر آورده شوند. (۴-۲-۱-پ-۲ را مشاهده کنید)،

۳) اجتناب از مخاطره‌ها و

۴) انتقال مخاطره‌های وابسته و آمیخته به کسب‌وکار به سایر گروه-ها ازجمله بیمه‌گرها وتامین‌کنندگان.

g) Select control objectives and controls for the treatment of risks.

Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks (see 4.2.1c)2)) as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover the identified requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

NOTE: Annex A contains a comprehensive list of control objectives and controls that have been found to be commonly relevant in organizations. Users of this International Standard are directed to Annex A as a starting point for control selection to ensure that no important control options are overlooked.

h) Obtain management approval of the proposed residual risks.

i) Obtain management authorization to implement and operate the ISMS.

j) Prepare a Statement of Applicability.

A Statement of Applicability shall be prepared that includes the following:

1) the control objectives and controls selected in 4.2.1g) and the reasons for their selection;

2) the control objectives and controls currently implemented (see 4.2.1e)2)); and

چ) انتخاب اهداف کنترل و کنترل‌ها برای برخورد با مخاطره.

اهداف کنترل و کنترل‌ها باید با هدف برآورده شدن الزامات تعیین شده بر اساس ارزشیابی مخاطره و فرآیند برخورد با مخاطره انتخاب و به مورد اجرا گذاشته شوند. این انتخاب باید با در نظر گرفتن معیارهای پذیرش مخاطره(به (بند ۲)از ۴-۲-۱-پ مراجعه نمایید) همچنین الزامات قانون، آیین‌نامه و قرارداد باشد.

اهداف کنترل و کنترل‌های مندرج در پیوست الف به عنوان بخشی از این فرآیند باید انتخاب شود و از هر حیث برای برآورده شدن الزامات شناسایی شده مناسب می‌باشد.

اهداف کنترل و کنترل‌های مندرج در پیوست الف، جامع و کامل نیستند و لذا اهداف کنترل و کنترل‌های دیگر نیز ممکن است انتخاب شوند.

یادآوری : پیوست الف، متضمن فهرست کامل و جامعی از اهداف کنترل و کنترل‌ها است و در سازمان‌ها رایج و مرسوم می‌باشد. به کاربران استاندارد بین‌المللی حاضر توصیه می‌شود تا از پیوست الف به عنوان یک نقطه شروع برای انتخاب کنترل‌ها استفاده نمایند چرا که به این ترتیب مطمئن خواهند شد که هیچ یک از راهکارهای مهم کنترلی نادیده گرفته نشده است.

ح) دریافت تاییدیه مخاطره‌های باقیمانده پیشنهادی از مدیریت.

خ) دریافت مجوز مدیریت برای اجرا و بهره‌برداری از سیستم مدیریت امنیت اطلاعات.

د) تهیه بیانیه کاربردپذیری.

موارد ذیل باید در زمان تهیه بیانیه کاربردپذیری مدنظر قرار گرفته و در متن گزارش لحاظ گردد:

۱) اهداف کنترل و کنترل‌های انتخاب شده در بند ۴-۲-۱-ح و دلایل انتخاب آن‌ها.

۲) اهداف کنترل و کنترل‌هایی که در حال حاضر اجرا می‌شوند. ((به بند ۲) ۴-۲-۱-ث مراجعه نمایید) و

3) the exclusion of any control objectives and controls in Annex A and the justification for their exclusion.

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

4.2.2. Implement and operate the ISMS

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in 4.2.1g) to meet the control objectives.

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)).

NOTE: Measuring the effectiveness of controls allows managers and staff to determine how well controls achieve planned control objectives.

۳) حذف هر یک از اهداف کنترل و کنترل‌ها در پیوست الف، و ذکر دلایل توجیهی برای حذف.

یادآوری: بیانیه کاربردپذیری دربردارنده خلاصه‌ای از تصمیمات مربوط به اتخاذ تدابیر لازم جهت برخورد با مخاطره‌ها می‌باشد. ذکر دلایل توجیهی برای موارد حذف شده، نوعی روش کنترلی است که بر اساس آن اطمینان حاصل می‌شود که هیچ یک از اقدامات کنترلی اشتباهًا حذف نشده‌اند.

۴.۲.۲. اجرا و بهره‌برداری از سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را انجام دهد:

الف) قاعده‌مند کردن برنامه برخورد با مخاطره که در آن اقدامات مناسب مدیریت، منابع، مسئولیت‌ها و اولویت‌ها برای مدیریت مخاطره‌های امنیت اطلاعات شناسایی می‌شوند. (به بند ۵ مراجعه نمایید).

ب) اجرای برنامه برخورد با مخاطره‌ها به منظور دستیابی به اهداف کنترل تعیین شده که منابع مالی لازم و نقش‌ها و مسئولیت‌ها در آن لحاظ شده‌اند.

پ) اجرای کنترل‌های انتخاب شده در بند ۴-۲-۱- ح به منظور تامین اهداف کنترل.

ت) تعریف نحوه اندازه‌گیری اثربخشی کنترل‌ها یا مجموعه کنترل‌های انتخاب شده و معین کردن نحوه استفاده از این اندازه‌گیری‌ها در ارزشیابی اثربخشی کنترل به‌طوری‌که نتایج قابل مقایسه و تکرار پذیر بدست آید.(به بند ۴-۲-۳- پ مراجعه نمایید).

یادآوری : اندازه‌گیری اثربخشی کنترل‌ها به مدیران و کارکنان این امکان را خواهد داد تا تعیین نمایند که چگونه با کنترل‌های مناسب به اهداف کنترل برنامه‌ریزی شده دست خواهند یافت.

e) Implement training and awareness programmes (see 5.2.2).

f) Manage operation of the ISMS.

g) Manage resources for the ISMS (see 5.2).

h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3a)).

4.2.3. Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and reviewing procedures and other controls to:

1) promptly detect errors in the results of processing;

2) promptly identify attempted and successful security breaches and incidents;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) help detect security events and thereby prevent security incidents by the use of indicators; and

5) determine whether the actions taken to resolve a breach of security were effective.

ث) اجرای برنامه‌های آموزش و آگاه‌سازی. (به بند ۵-۲-۲ مراجعه نمایید).

ج) مدیریت بهره‌برداری از سیستم مدیریت امنیت اطلاعات.

ح) مدیریت منابع برای سیستم مدیریت امنیت اطلاعات. (به بند ۵-۲ مراجعه نمایید).

خ) اجرای روش‌های اجرایی و کنترل‌های دیگر تا به این ترتیب توانایی شناسایی فوری رویدادهای امنیتی و واکنش به حادثه‌های امنیتی برایش فراهم گردد. (به بند ۴-۲-۳-الف مراجعه نمایید).

۴.۲.۳. پایش و بازنگری سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را انجام دهد:

الف) اجرای روش‌های اجرایی پایش و بازنگری و سایر اقدامات کنترلی تا:

۱) اشتباهات بوجود آمده در نتایج پردازش به‌موقع شناسایی شوند،

۲) رخنه‌ها و حوادث امنیتی موفق و ناموفق به‌موقع شناسایی شوند،

۳) مدیریت را قادر سازد تا تشخیص دهد که آیا اقدامات امنیتی تفویض شده به افراد یا اجرا شده به‌وسیله فناوری اطلاعات طبق انتظار انجام می‌شود یا خیر،

۴) به شناسایی رویدادهای امنیتی کمک نماید و بوسیله آن و با استفاده از شاخص‌های موجود از بروز حوادث امنیتی جلوگیری نماید، و

۵) معین کند که آیا اقدامات اتخاذ شده جهت حل و فصل مشکل نقض امنیت کارآمد و موثر هستند یا خیر.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements have been met.

d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks, taking into account changes to:

1) the organization;

2) technology;

3) business objectives and processes;

4) identified threats;

5) effectiveness of the implemented controls; and

6) external events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate.

e) Conduct internal ISMS audits at planned intervals (see 6).

NOTE: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes.

f) Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified (see 7.1).

ب) تعهد به اینکه بازنگری‌های منظم در خصوص اثربخشی سیستم مدیریت امنیت اطلاعات (ازجمله برآورده‌شدن خط‌مشی و اهداف سیستم مدیریت امنیت اطلاعات و بازنگری کنترل‌های امنیتی) را انجام دهد و در این بین نتایج حاصل از ممیزی‌های امنیتی، حوادث، نتایج حاصل از اندازه‌گیری‌های اثربخشی، پیشنهادات و بازخورد از کلیه طرفین ذینفع را مدنظر قرار دهد.

پ) اندازه‌گیری اثربخشی کنترل‌ها تا از برآورده شدن الزامات امنیتی اطمینان حاصل نماید.

ت) بازنگری ارزشیابی مخاطرات در فواصل زمانی برنامه‌ریزی شده و بازنگری مخاطرات باقی‌مانده و سطوح قابل قبول شناسایی شده مخاطرات با در نظر گرفتن تغییرات در:

۱) سازمان،

۲) فناوری،

۳) اهداف کسب‌وکار و فرآیندها،

۴) تهدیدات شناسایی‌شده،

۵) اثربخشی کنترل‌های اجرا شده و

۶) رویدادهای بیرونی، مانند تغییرات در محیط‌های قانونی و آیین‌نامه‌ای، تغییر در تعهدات قراردادی و تغییرات در شرایط اجتماعی

ث) انجام ممیزی‌های داخلی سیستم مدیریت امنیت اطلاعات در فواصل زمانی برنامه‌ریزی شده . (به بند ۶ مراجعه نمایید).

یادآوری : ممیزی‌های داخلی که گاهی اوقات تحت عنوان ممیزی‌های شخص اول از آن نامبرده می‌شود، توسط خود سازمان، یا به نمایندگی از آن، به منظور اهداف و مقاصد داخلی انجام می‌شود.

ج) تعهد به اینکه بازنگری مدیریت سیستم مدیریت امنیت اطلاعات را به صورت منظم انجام دهد تا به این ترتیب از کفایت دامنه و اینکه بهبودها در فرآیند سیستم مدیریت امنیت اطلاعات شناسایی شده است. (به بند ۷-۱ مراجعه نمایید).

g) Update security plans to take into account the findings of monitoring and reviewing activities.

h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).

4.2.4 .Maintain and improve the ISMS

The organization shall regularly do the following.

a)Implement the identified improvements in the ISMS.

b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

d) Ensure that the improvements achieve their intended objectives.

4.3. Documentation requirements

4.3.1. General

Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

ح) بروزآوری طرح‌های امنیتی با توجه به نتایج حاصل از فعالیت‌های انجام شده در زمینه پایش و بازنگری.

خ) ثبت اقدامات و رویدادهایی که می‌تواند بر اثربخشی یا کارایی سیستم مدیریت امنیت اطلاعات تاثیرگذار باشد. (به بند ۴-۳-۳ مراجعه نمایید).

۴.۲.۴. نگهداری و ارتقای سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را به صورت منظم اجرا نماید:

الف)اجرای بهبودهای شناسایی شده در سیستم مدیریت امنیت اطلاعات.

ب) اجرای اقدامات اصلاحی و پیشگیرانه مناسب بر اساس موارد گفته شده در بندهای ۸-۲ و ۸-۳ . همچنین درس‌هایی را که از تجربیات امنیتی سایر سازمان‌ها و تجربیات خود سازمان فرا گرفته است به‌کار بندد.

پ)مبادله اطلاعات مربوط به اقدامات و بهبودها با تمام طرفین ذینفع، در سطح مناسبی از جزئیات، با شرایط و به شرحی که مورد توافق قرار گرفته است.

ت) اطمینان از اینکه بهبودهای موردنظر، اهداف مورد نظر را محقق خواهد نمود.

۴. ۳. الزامات مستندسازی

۴.۳.۱. کلیات

مستندات باید شامل سوابق تصمیم‌های مدیریت بوده و اطمینان خاطر دهد که اقدامات از طریق تصمیم‌ها و خطمشی‌های مدیریت قابل رهگیری بوده و همچنین اطمینان دهد که نتایج ثبت شده تکرارپذیر هستند.

این مهم است که بتوانیم ارتباط معکوس کنترل‌های انتخاب شده با نتایج ارزیابی مخاطرات و فرایند برخورد با مخاطره و سپس با خطمشی و اهداف ISMS را اثبات کنیم.

The ISMS documentation shall include:

a) documented statements of the ISMS policy (see 4.2.1b)) and objectives;

b) the scope of the ISMS (see 4.2.1a));

c) procedures and controls in support of the ISMS;

d) a description of the risk assessment methodology (see 4.2.1c));

e) the risk assessment report (see 4.2.1c) to 4.2.1g));

f) the risk treatment plan (see 4.2.2b));

g)documented procedures needed by the organization to ensure the effective planning, operation and

control of its information security processes and describe how to measure the effectiveness of controls

(see 4.2.3c));

h) records required by this International Standard (see 4.3.3); and

i) the Statement of Applicability.

NOTE 1: Where the term "documented procedure" appears within this International Standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2: The extent of the ISMS documentation can differ from one organization to another owing to:

- the size of the organization and the type of its activities; and
- the scope and complexity of the security requirements and the system being managed.

NOTE 3: Documents and records may be in any form or type of medium.

مستندات سیستم مدیریت امنیت اطلاعات باید دربردارنده موارد ذیل باشد:

الف) بیانیه‌های مستند خط‌مشی و اهداف سیستم مدیریت امنیت اطلاعات (به بند ۴-۲-۱-ب مراجعه نمایید).

ب) دامنه کاربرد سیستم مدیریت امنیت اطلاعات (به بند ۴-۲-۱-الف مراجعه نمایید)

پ) روش‌های اجرایی و کنترل‌ها در حمایت از سیستم مدیریت امنیت اطلاعات

ت) شرح متدولوژی ارزشیابی مخاطره (به بند ۴-۲-۱-پ مراجعه نمایید)

ث) گزارش ارزشیابی مخاطره (به بند ۴-۲-۱-ب تا ۴-۲-۱-ح مراجعه نمایید)

ح) روش‌های اجرایی مستندسازی شده مورد نیاز سازمان تا به این ترتیب از موثر بودن برنامه‌ریزی، بهره‌برداری و کنترل فرآیندهای امنیت اطلاعات آن اطمینان حاصل شود و امکان توصیف اندازه‌گیری اثربخشی کنترل‌ها فراهم گردد. (به بند ۴-۲-۳-پ مراجعه نمایید)

خ) سوابقی که به موجب استاندارد بین‌المللی حاضر لازم دانسته شده است (به بند ۴-۳-۳ مراجعه نمایید)

چ) بیانیه کاربردپذیری.

یادآوری ۱ : در این استاندارد بین‌المللی آنجا که عبارت " روش‌های اجرایی مستندسازی شده "بکار برده شود، منظور روش اجرایی ایجاد شده، مستندسازی شده، اجرا شده و حفظ شده می‌باشد.

یادآوری ۲ : محدوده مستندات سیستم مدیریت امنیت اطلاعات با توجه به موارد ذیل از یک سازمان به سازمان دیگر، متفاوت می‌باشد:

- اندازه سازمان و نوع فعالیت‌های آن؛ و
- دامنه و پیچیدگی الزامات امنیتی و سیستمی که تحت مدیریت قرار دارد.

یادآوری۳ : مستندات و سوابق می‌تواند در اشکال و فرمت‌های مختلف رسانه‌ای تهیه شود.

4.3.2. Control of documents

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

a) approve documents for adequacy prior to issue;

b) review and update documents as necessary and re-approve documents;

c) ensure that changes and the current revision status of documents are identified;

d) ensure that relevant versions of applicable documents are available at points of use;

e) ensure that documents remain legible and readily identifiable;

f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;

g) ensure that documents of external origin are identified;

h) ensure that the distribution of documents is controlled;

i) prevent the unintended use of obsolete documents; and

j) apply suitable identification to them if they are retained for any purpose.

4.3.3. Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled.

۴.۳.۲. کنترل مستندات

مستنداتی که به موجب استاندارد بین‌المللی حاضر لازم و ضروری دانسته شده‌اند باید محافظت و کنترل شوند. یک روش اجرایی مستند باید به‌گونه‌ای ایجاد شود که اقدامات مدیریتی لازم برای موارد زیر را تعریف کند:

الف) تایید مستندات از جهت کفایت قبل از انتشار؛

ب) بازنگری و روزآمدکردن مستندات برحسب لزوم و تصویب مجدد مستندات؛

پ) حصول اطمینان از این که تغییرات و وضعیت کنونی تجدید نظر مستندات مشخص شده است؛

ت) حصول اطمینان از این که نسخه‌های مربوط به مستندات قابل‌استفاده در مکان‌های استفاده در دسترس هستند؛

ث) حصول اطمینان از خوانا بودن و قابل‌شناسایی بودن مستندات؛

ج) حصول اطمینان از این که مستندات در دسترس افرادی که به آن‌ها نیاز دارند قرار خواهد گرفت و براساس رویه‌های لازم‌الاجرا در طبقه‌بندی آن‌ها منتقل، ذخیره‌سازی و در نهایت از درجه اعتبار ساقط می‌شوند؛

ح) حصول اطمینان از این که مستندات برون سازمانی شناسایی شده‌اند؛

خ) حصول اطمینان از این که توزیع مستندات تحت کنترل قرار دارد؛

چ) جلوگیری از استفاده ناخواسته از مستندات منسوخ و

د) استفاده از شناسنامه مناسب برای آن‌ها در صورتی که بنا به هر دلیل نگاهداری شده‌اند.

۴.۳.۳. کنترل سوابق

سوابق باید به‌گونه‌ای ایجاد و نگهداری شوند که امکان ارائه شواهد در خصوص انطباق با الزامات و بهره‌برداری موثر از سیستم مدیریت امنیت اطلاعات وجود داشته باشد، لذا این سوابق باید محافظت و کنترل شوند.

The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS.

EXAMPLE:

Examples of records are a visitors' book, audit reports and completed access authorization forms.

5. Management responsibility

5.1. Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an ISMS policy;

b) ensuring that ISMS objectives and plans are established;

c) establishing roles and responsibilities for information security;

d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);

سیستم مدیریت امنیت اطلاعات باید به هر الزام قانونی و آیین‌نامه‌ای مرتبط و تعهد قراردادی توجه داشته باشد. سوابق باید خوانا و به آسانی قابل شناسایی و بازیابی باقی بمانند. کنترل‌های مورد نیاز جهت شناسایی، ذخیره‌سازی، محافظت، بازیابی، زمان نگهداری و امحای سوابق باید مستندسازی شده و به مورد اجرا گذاشته شوند.

سوابق عملکرد فرآیند به شرحی که در بند ۴-۲ آمده است و تمام حوادث امنیتی بارز مرتبط با سیستم مدیریت امنیت اطلاعات باید نگهداری شوند.

مثال:

دفتر بازدیدکنندگان، گزارش‌های ممیزی و فرم‌های تکمیل شده مجوز ورود، همگی نمونه‌هایی از سوابق می‌باشند.

۵. مسئولیت مدیریت

۵. ۱. تعهد مدیریت

مدیریت باید تا با انجام موارد ذیل، تعهد خود نسبت به استقرار، اجرا، بهره‌برداری، پایش، بازنگری، حفظ و بهبود سیستم مدیریت امنیت اطلاعات را ثابت نماید:

الف) ایجاد یک خط‌مشی سیستم مدیریت امنیت اطلاعات؛

ب) حصول اطمینان از اینکه اهداف و برنامه‌های سیستم مدیریت امنیت اطلاعات تعیین شده‌اند؛

پ) تعیین نقش‌ها و مسئولیت‌های امنیت اطلاعات؛

ت) ابلاغ کردن به سازمان در زمینه اهمیت برآورده‌شدن اهداف امنیت اطلاعات و رعایت خط‌مشی امنیت اطلاعات، مسئولیت‌هایی که به موجب قانون تعیین شده است و لزوم بهبود مستمر؛

ث) تامین منابع کافی جهت استقرار، اجرا، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات (به بند ۱-۲-۵ مراجعه نماید).

f) deciding the criteria for accepting risks and the acceptable levels of risk;

g) ensuring that internal ISMS audits are conducted (see 6); and

h) conducting management reviews of the ISMS (see

5.2. Resource management

5.2.1. Provision of resources

The organization shall determine and provide the resources needed to:

a) establish, implement, operate, monitor, review, maintain and improve an ISMS;

b) ensure that information security procedures support the business requirements;

c) identify and address legal and regulatory requirements and contractual security obligations;

d) maintain adequate security by correct application of all implemented controls;

e) carry out reviews when necessary, and to react appropriately to the results of these reviews; and

f) where required, improve the effectiveness of the ISMS.

5.2.2. Training, awareness and competence

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

a) determining the necessary competencies for personnel performing work effecting the ISMS;

ج) تصمیم‌گیری در خصوص معیارهای پذیرش مخاطره و سطوح قابل‌پذیرش مخاطره؛

ح) حصول اطمینان از اجرا شدن ممیزی داخلی سیستم مدیریت امنیت اطلاعات (به بند ۶ مراجعه نمایید)؛ و

خ) اجرای بازنگری‌های مدیریت در سیستم مدیریت امنیت اطلاعات (به بند ۷ مراجعه نمایید).

۵. ۲. مدیریت منابع

۵. ۲. ۱. *تامین منابع*

سازمان باید منابع لازم جهت موارد ذیل را تعیین و تامین نماید:

الف) استقرار، اجرا، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات؛

ب) حصول اطمینان از این که رویه‌های امنیت اطلاعات، الزامات کسب‌وکار را پشتیبانی خواهد نمود؛

پ) شناسایی و توجه به الزامات قانونی وآیین نامه‌ای و تعهدات امنیتی قراردادها؛

ت) حفظ امنیت کافی از طریق استفاده صحیح از کلیه کنترل‌های پیاده سازی شده؛

ث) اجرای بازنگری‌ها برحسب لزوم و اتخاذ واکنش مناسب به نتایج این بازنگری‌ها و

ج) بهبود اثربخشی سیستم مدیریت امنیت اطلاعات در صورت لزوم.

۵. ۲. ۲. *آموزش، آگاه‌سازی و صلاحیت*

سازمان باید تا با اجرای موارد ذیل از صلاحیت کلیه کارکنان در اجرای مسئولیت‌ها و وظایف محوله به ایشان که در سیستم مدیریت امنیت اطلاعات تعریف شده است، اطمینان حاصل نماید:

الف) تعیین صلاحیت‌های لازم برای کارکنانی که اجرای کارهای موثر بر سیستم مدیریت امنیت اطلاعات را بر عهده دارند؛

b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;

c) evaluating the effectiveness of the actions taken; and

d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6. Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

a) conform to the requirements of this International Standard and relevant legislation or regulations;

b) conform to the identified information security requirements;

c) are effectively implemented and maintained; and

d) perform as expected.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

ب) برگزاری دوره‌های آموزشی یا اتخاذ سایر اقدامات (به عنوان مثال استخدام کارکنان ذی‌صلاح) به منظور برآورده شدن اینگونه نیازها؛

پ) ارزیابی اثربخشی اقدامات اتخاذ شده؛ و

ت) نگهداری سوابق تحصیلی، آموزشی، مهارت‌ها، تجربیات و توانایی‌ها (به بند ۳-۳-۴ مراجعه نمایید).

سازمان همچنین باید اطمینان حاصل نماید تا تمام کارکنان مرتبط، در خصوص اهمیت فعالیت‌های امنیت اطلاعات که بر عهده ایشان گذاشته شده است و همچنین میزان نقش و تاثیرگذاریشان در تحقق اهداف سیستم مدیریت امنیت اطلاعات آگاه هستند.

۶. ممیزی‌های داخلی سیستم مدیریت امنیت اطلاعات

سازمان باید ممیزی‌های داخلی سیستم مدیریت امنیت اطلاعات را در فواصل زمانی برنامه‌ریزی شده، اجرا نماید تا تعیین کند که اهداف کنترل، کنترل‌ها، فرآیندها و روش‌های اجرایی سیستم مدیریت امنیت اطلاعات:

الف) با الزامات استاندارد بین‌المللی حاضر و قوانین و مقررات مرتبط مطابقت دارد؛

ب) با الزامات شناسایی شده در حوزه امنیت اطلاعات مطابقت دارد؛

پ) به صورت اثر بخش عملیاتی و نگهداری شده است؛ و

ت) همانگونه که انتظار می‌رود اجرا شده است.

یک برنامه ممیزی با در نظر گرفتن جایگاه و اهمیت فرآیندها و حوزه‌هایی که باید مورد ممیزی قرار گیرند و همچنین نتایج ممیزی‌های قبلی باید طرح‌ریزی شود.

معیارها، دامنه کاربرد، تناوب و روش‌های ممیزی باید تعیین شود. انتخاب ممیزها و اجرای ممیزی‌ها باید به‌گونه‌ای انجام شود که واقع‌بینی و بی‌طرف بودن فرآیند ممیزی را تضمین نماید. ممیزها مجاز به ممیزی کارهای خود نخواهند بود.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8).

NOTE: ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing, may provide helpful guidance for carrying out the internal ISMS audits

7. Management review of the ISMS

7.1. General

Management shall review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained (see 4.3.3).

7.2. Review input

The input to a management review shall include:

a) results of ISMS audits and reviews;

مسئولیت‌ها و الزامات برای برنامه‌ریزی و اجرای ممیزی‌ها و برای گزارش‌دهی نتایج و نگهداری سوابق (به بند ۳-۳-۴ مراجعه نمایید) باید در یک روش اجرایی مستند تعریف شود.

مدیریت مسئول در قبال حوزه‌ای که قرار است مورد ممیزی قرار گیرد، باید اطمینان حاصل نماید که اقدامات جهت رفع عدم انطباق‌های تشخیص داده شده وعلل آن‌ها به موقع و بدون تاخیر اتخاذ شده‌اند.

اقدامات پیگیری باید شامل تصدیق اقدامات اتخاذ شده و گزارش نتایج تصدیق باشد. (به بند ۸ مراجعه نمایید).

یادآوری : رهنمودهای ISO 19011:2002 در خصوص ممیزی سیستم-های مدیریت کیفیت و یا زیست‌محیطی می‌تواند راهنمایی ارزشمندی در زمینه اجرای ممیزی‌های داخلی سیستم مدیریت امنیت اطلاعات فراهم نماید.

۷. بازنگری سیستم مدیریت امنیت اطلاعات توسط مدیریت

۷. ۱. کلیات

مدیریت باید تا سیستم مدیریت امنیت اطلاعات سازمان را در فواصل زمانی برنامه‌ریزی شده (حداقل یکبار در سال) مورد بازنگری قرار دهد تا به این ترتیب از تداوم تناسب، کفایت و اثربخشی آن اطمینان حاصل نماید. این بازنگری باید مواردی مانند ارزشیابی فرصت‌های بهبود و لزوم تغییر در سیستم مدیریت امنیت اطلاعات و از جمله خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات را شامل گردد.

نتایج این بازنگری‌ها باید به وضوح مستندسازی شده و سوابق مربوط به آن نگهداری شود. (به بند ۳-۳-۴ مراجعه نمایید).

۷. ۲. ورودی بازنگری

ورودی بازنگری مدیریت باید شامل موارد زیر باشد :

الف) نتایج ممیزی‌ها و بازنگری‌های سیستم مدیریت امنیت اطلاعات؛

b) feedback from interested parties;

c) techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;

d) status of preventive and corrective actions;

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) results from effectiveness measurements;

g) follow-up actions from previous management reviews;

h) any changes that could affect the ISMS; and

i) recommendations for improvement.

7.3. Review output

The output from the management review shall include any decisions and actions related to the following.

a) Improvement of the effectiveness of the ISMS.

b) Update of the risk assessment and risk treatment plan.

c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:

1) business requirements;

2) security requirements;

3) business processes effecting the existing business requirements;

4) regulatory or legal requirements;

5) contractual obligations; and

6) levels of risk and/or criteria for accepting risks.

d) Resource needs.

e) Improvement to how the effectiveness of controls is being measured.

ب) بازخورد از طرف‌های ذینفع؛

پ) فنون، محصولات یا رویه‌هایی که می‌توان به منظور بهبود کارایی و اثربخشی سیستم مدیریت امنیت اطلاعات در سازمان مورد استفاده قرار داد؛

ت) وضعیت اقدامات پیشگیرانه و اصلاحی؛

ث) آسیب‌پذیری‌ها یا تهدیدهایی که در ارزشیابی مخاطره قبلی مورد توجه کافی قرار نگرفته‌اند؛

ج) نتایج حاصل از اندازه‌گیری‌های اثربخشی؛

ح) اقدامات پیگیرانه از بازنگری‌های قبلی مدیریت؛

خ) هرگونه تغییراتی که می‌تواند بر سیستم مدیریت امنیت اطلاعات تاثیرگذار باشد و

چ) توصیه‌ها و پیشنهادات در جهت بهبود.

۷. ۳ خروجی بازنگری

خروجی بازنگری مدیریت باید متضمن و دربردارنده تصمیمات و اقدامات مرتبط با موارد ذیل باشد:

الف) بهبود اثربخشی سیستم مدیریت امنیت اطلاعات؛

ب) بروزکردن ارزشیابی مخاطره و برنامه برخورد با مخاطره.

پ) اصلاح روش‌های اجرایی و کنترل‌های تاثیرگذار بر امنیت اطلاعات، بر حسب لزوم، در پاسخ به رویدادهای داخلی و بیرونی که ممکن است بر سیستم مدیریت امنیت اطلاعات تاثیر بگذارند و از جمله تغییرات در:

۱) الزامات کسب‌وکار؛

۲) الزامات امنیتی؛

۳) فرآیندهای کسب‌وکار تاثیرگذار بر الزامات کسب‌وکار موجود؛

۴) الزامات آیین‌نامه‌ای و قانونی؛

۵) تعهدات قراردادی؛ و.

۶) سطوح مخاطره و یا معیارهای پذیرش مخاطره.

ت) نیازمندی‌های منابع

ث) بهبود نحوه اندازه‌گیری اثربخشی کنترل‌ها.

8. ISMS improvement

8.1. Continual improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).

8.2. Corrective action

The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action shall define requirements for:

a) identifying nonconformities;

b) determining the causes of nonconformities;

c) evaluating the need for actions to ensure that nonconformities do not recur;

d) determining and implementing the corrective action needed;

e) recording results of action taken (see 4.3.3); and

f) reviewing of corrective action taken.

8.3. Preventive action

The organization shall determine action to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

a) identifying potential nonconformities and their causes;

b) evaluating the need for action to prevent occurrence of nonconformities;

c) determining and implementing preventive action needed;

d) recording results of action taken (see 4.3.3); and

۸. بهبود سیستم مدیریت امنیت اطلاعات

۸. ۱. بهبود مستمر

سازمان باید با استفاده از خط‌مشی امنیت اطلاعات، اهداف امنیت اطلاعات، نتایج ممیزی، تجزیه و تحلیل رویدادهای پایش‌شده، اقدامات اصلاحی و پیشگیرانه و بازنگری مدیریت، سبب بهبود مستمر در اثربخشی سیستم مدیریت امنیت اطلاعات شود.(به بند ۷ مراجعه نمایید).

۸. ۲. اقدامات اصلاحی

سازمان باید برای رفع علل عدم‌انطباق‌ها با الزامات سیستم مدیریت امنیت اطلاعات، اقدامات لازم را به عمل آورده و به این ترتیب از بروز مجدد آن‌ها جلوگیری نماید. الزامات مربوط به موارد ذیل باید در یک روش اجرایی مستند برای اقدامات اصلاحی تعیین گردد:

الف) شناسایی عدم‌انطباق‌ها؛

ب) تعیین علل عدم‌انطباق‌ها؛

پ) ارزیابی نیاز به اقدامات به منظور حصول اطمینان از عدم بروز مجدد عدم انطباق‌ها؛

ت) تعیین و انجام اقدامات اصلاحی مورد نیاز؛

ث) ثبت نتایج اقدامات بعمل‌آمده (به بند ۳-۳-۴ مراجعه نمایید)؛ و

ج) بازنگری اقدامات اصلاحی بعمل آمده.

۸. ۳. اقدامات پیشگیرانه

سازمان باید اقدامی برای رفع علل عدم انطباق‌های بالقوه با الزامات سیستم مدیریت امنیت اطلاعات، به منظور پیشگیری از رخداد آن‌ها، تعیین کند. اقدامات پیشگیرانه باید متناسب با تاثیر مشکلات بالقوه باشند.

روش اجرائی مستند برای اقدام پیشگیرانه باید شامل الزامات ذیل باشد:

الف) شناسایی موارد عدم‌انطباق بالقوه و علل آن‌ها؛

ب) ارزیابی نیاز به اقدامی که از رخداد عدم انطباق‌ها پیشگیری کند؛

پ) تعیین و اجرای اقدام پیشگیرانه مورد نیاز؛

ت)ثبت سوابق نتایج اقدام انجام شده (بند ۴-۳-۳) و

e) reviewing of preventive action taken.

The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

NOTE: Action to prevent nonconformities is often more cost-effective than corrective action.

ث) بازنگری اقدام پیشگیرانه انجام شده.

سازمان باید مخاطره‌های تغییر یافته را شناسایی نماید و با تمرکز بر مخاطره‌هایی که به‌طور قابل توجه تغییر یافته‌اند، الزامات مربوط به اقدامات پیشگیرانه را تعیین نماید.

نتایج حاصل از ارزشیابی مخاطره، نقش قابل توجهی در تعیین اولویت اقدامات پیشگیرانه ایفا می‌نمایند.

یادآوری : در اغلب اوقات اقدام در جهت پیشگیری از بروز عدم‌انطباق‌ها در مقایسه با اقدامات اصلاحی مقرون به صرفه‌تر خواهد بود.

Annex A(normative); Control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 17799:2005 Clauses 5 to 15. The lists in Table A.1 are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in 4.2.1.

ISO/IEC 17799:2005 Clauses 5 to 15 provide implementation advice and guidance on best practice in support of the controls specified in A.5 to A.15.

Table A.1 – Control objectives and controls

Table A.1 – Control objectives and controls

A.5 Security policy		
A.5.1 Information security policy **Objective:** *To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*		
A.5.1.1	**Information security policy document**	**Control** An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	**Review of the information security policy**	**Control** The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness

پیوست الف(الزامی)؛ اهداف کنترلی و کنترل ها

اهداف کنترل و کنترل‌های مندرج در جدول الف-۱، دقیقًا از موارد مندرج در بندهای ۵ تا ۱۵ از ISO/IEC 17799:2005 اقتباس شده است و کاملاً همراستا با آن می‌باشد. فهرست‌های مندرج در این جدول، کامل و جامع نیستند و یک سازمان می‌تواند بنا به تشخیص و صلاحدید خود سایر اهداف کنترل و کنترل‌ها را اضافه نماید. اهداف کنترل و کنترل‌های مندرج در این جداول به عنوان بخشی از فرآیند سیستم مدیریت امنیت اطلاعات، به شرحی که در بند ۱-۲-۴ بیان شده است، انتخاب گردیده است.

بندهای ۵ تا ۱۵ از ISO/IEC 17799:2005، در جهت پشتیبانی از کنترل‌های مندرج در بندهای الف-۵ تا الف-۱۵ (جدول الف-۱ اهداف کنترل و کنترل ها) بر اساس بهترین تجارب عملی، توصیه‌ها و رهنمودهایی برای پیاده سازی ارئه می‌نماید.

جدول A-1- اهداف کنترل و کنترل ها

الف-۵ خط‌مشی امنیت		
الف-۵-۱ خط‌مشی امنیت اطلاعات **هدف:** *فراهم سازی جهت‌گیری و حمایت مدیریت برای امنیت اطلاعات بر اساس الزامات کسب و کار و قوانین و مقررات مربوطه.*		
الف ۵-۱-۱	سند خط‌مشی امنیت اطلاعات	کنترل یک سند خط‌مشی امنیت اطلاعات باید توسط مدیریت به تایید برسد و پس از انتشار به کلیه کارمندان و طرف‌های ذینفع بیرونی ابلاغ گردد.
الف ۵-۱-۲	بازنگری خط-مشی امنیت اطلاعات	کنترل بیانیه خط‌مشی امنیت اطلاعات باید در فواصل زمانی برنامه‌ریزی شده و یا در صورت بروز تغییرات قابل توجه مورد بازنگری قرار گیرد تا به این ترتیب از تداوم تناسب، کفایت و اثربخشی آن اطمینان حاصل شود.

A.6 Organization of information security		
A.6.1 Internal organization **Objective**: *To manage information security within the organization.*		
A.6.1.1	Management commitment to information security	**Control** Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities
A.6.1.2	Information security coordination	**Control** Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
A.6.1.3	Allocation of information security responsibilities	**Control** All information security responsibilities shall be clearly defined
A.6.1.4	Authorization process for information processing facilities	**Control** A management authorization process for new information processing facilities shall be defined and implemented
A.6.1.5	Confidentiality agreements	**Control** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
A.6.1.6	Contact with authorities	**Control** Appropriate contacts with relevant authorities shall be maintained
A.6.1.7	Contact with special interest groups	**Control** Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained

الف-۶ - ساختار امنیت اطلاعات		
الف-۶-۱ ساختار داخلی **هدف**: *مدیریت امنیت اطلاعات در داخل سازمان*		
الف ۶-۱-۱	تعهد مدیریت نسبت به امنیت اطلاعات	**کنترل** مدیریت ملزم خواهد بود تا به صورت فعال امنیت داخلی سازمان را با جهت دهی شفاف، تعهدات مشخص، به‌کارگماری صریح و قبول مسئولیت‌های امنیت‌اطلاعات پشتیبانی نماید.
الف ۶-۱-۲	هماهنگی امنیت اطلاعات	**کنترل** فعالیت‌های امنیت اطلاعات باید توسط نمایندگان بخش‌های مختلف سازمان که دارای نقش‌ها و وظایف شغلی مرتبط هستند، هماهنگ شود.
الف ۶-۱-۳	تخصیص مسئولیت‌های امنیت اطلاعات	**کنترل** کلیه مسئولیت‌های امنیت اطلاعات باید به وضوح تعیین و تعریف شود.
الف ۶-۱-۴	فرآیند صدور مجوز برای امکانات لازم جهت پردازش اطلاعات	**کنترل** یک فرآیند مدیریت صدور مجوز برای امکانات جدید پردازش اطلاعات باید تعریف و به مورد اجرا گذاشته شود.
الف ۶-۱-۵	توافقات محرمانگی	**کنترل** الزامات مربوط به توافقات محرمانگی یا عدم-افشاء که منعکس‌کننده نیازهای سازمان به محافظت از اطلاعات می‌باشد باید تعیین و به‌طور منظم مورد بازنگری قرار داده شود.
الف ۶-۱-۶	ارتباط با مقامات مسئول	**کنترل** ارتباطات مناسب با مقامات مسئول ذی‌ربط باید حفظ شود.
الف ۶-۱-۷	ارتباط با گروه های ذینفع خاص	**کنترل** ارتباطات مناسب با گروه‌های با علاقه ویژه (SIG) یا سایر گروه‌های تخصصی امنیت و انجمن‌های حرفه‌ای باید حفظ شود.

A.6.1.8	**Independent review of information security**	**Control** The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur
A.6.2 External parties **Objective:** *To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties*		
A.6.2.1	**Identification of risks related to external parties**	**Control** The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.6.2.2	**Addressing security when dealing with customers**	**Control** All identified security requirements shall be addressed before giving customers access to the organization's information or assets
A.6.2.3	**Addressing security in third party agreements**	**Control** Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements

الف ۶-۱-۸	**بازنگری مستقل امنیت اطلاعات**	**کنترل** رویکرد سازمان در مدیریت امنیت اطلاعات و اجرای آن (به عنوان مثال اهداف کنترل، کنترل‌ها، خط‌مشی‌ها ، فرایندها، رویه‌های مربوط به امنیت اطلاعات) باید به صورت مستقل و در فواصل زمانی برنامه‌ریزی شده و یا در صورت بروز هرگونه تغییرات قابل ملاحظه در نحوه اجرای امنیت مورد بازنگری قرار داده شود.
الف-۶-۲ طرفهای بیرونی **هدف:** *حفظ امنیت اطلاعات سازمان و امکانات پردازش اطلاعاتی که توسط گروه‌های بیرونی قابل دسترس بوده، پردازش می‌شوند، به ایشان ارسال می‌شوند یا توسط ایشان مدیریت می‌شوند.*		
الف ۶-۲-۱	**شناسایی مخاطره‌های مرتبط باطرف های بیرونی**	**کنترل** مخاطره‌های وارد بر اطلاعات و امکانات پردازش اطلاعات سازمان که ناشی از فرآیند-های کسب‌وکار بوده و مرتبط با طرف‌های بیرونی می‌باشد، قبل از مجوز دسترسی باید شناسایی شده و کنترل‌های مناسب پیاده سازی شود.
الف ۶-۲-۲	**توجه به موضوع امنیت هنگام ارتباط با مشتریان**	**کنترل** تمامی الزامات امنیتی شناسایی شده، پیش از اعطای دسترسی اطلاعات یا دارایی سازمان به مشتری باید مورد توجه قرارگیرد.
الف ۶-۲-۳	**توجه به موضوع امنیت در توافقات اشخاص ثالث**	**کنترل** توافقات با اشخاص ثالث از جمله توافق در خصوص دسترسی، پردازش، تبادل یا مدیریت اطلاعات سازمان یا امکانات پردازش اطلاعات، یا اضافه کردن محصولات یا خدمات به مراکز پردازش اطلاعات باید تمام الزامات امنیتی مربوطه را در بر داشته باشد.

A.7 Asset management		
A.7.1 Responsibility for assets **Objective:** *To achieve and maintain appropriate protection of organizational assets.*		
A.7.1.1	**Inventory of assets**	**Control** All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A.7.1.2	**Ownership[1] of assets**	**Control** All information and assets associated with information processing facilities shall be 'owned'[3] by a designated part of the organization.
A.7.1.3	**Acceptable use of assets**	**Control** Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
A.7.2 Information classification **Objective**: *To ensure that information receives an appropriate level of protection.*		
A.7.2.1	**Classification guidelines**	**Control** Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
A.7.2.2	**Information labelling and handling**	**Control** An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization

1 Explanation: The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset.

الف-۷ مدیریت دارایی‌ها		
الف-۷-۱ مسئولیت در قبال دارایی‌ها **هدف:** *محقق‌شدن هدف محافظت از دارایی‌های سازمان و تامین محافظت لازم از آن‌ها*		
الف ۷-۱-۱	**لیست دارایی‌ها**	**کنترل** کلیه دارایی‌ها باید به‌طور دقیق شناسایی-شده و یک لیست از کلیه دارایی‌های مهم باید تنظیم و نگهداری شود.
الف ۷-۱-۲	**مالکیت[1] دارایی-ها**	**کنترل** مسئولیت مالکیت کلیه اطلاعات و دارایی-های مربوط به مراکز پردازش اطلاعات باید به یک بخش معین از سازمان واگذار شود.
الف ۷-۱-۳	**استفاده قابل پذیرش و صحیح از دارایی‌ها**	**کنترل** قوانین مربوط به استفاده قابل پذیرش و صحیح از اطلاعات و دارایی‌های مربوط به مراکز پردازش اطلاعات باید تعیین، مستندسازی و به مورد اجرا گذاشته شود.
الف-۷-۲ طبقه‌بندی اطلاعات **هدف**: *به منظور اطمینان از این که از اطلاعات در یک سطح مناسب محافظت می‌شود.*		
الف ۷-۲-۱	**راهنمای طبقه-بندی**	**کنترل** اطلاعات باید بر حسب میزان ارزش، الزامات قانونی، حساسیت و میزان اهمیتی که برای سازمان دارند طبقه‌بندی شوند.
الف ۷-۲-۲	**برچسب زنی و مراقبت از اطاعات**	**کنترل** در خصوص برچسب‌زنی و مراقبت از اطلاعات، لازم خواهد بود تا یک مجموعه مناسب از رویه‌ها بر اساس طرح طبقه‌بندی که توسط سازمان انتخاب می‌شود، ایجاد و به مورد اجرا گذاشته شود.

۱ عبارت مالک اشاره به فرد یا موجودیتی دارد که مسئولیتش برای کنترل، تولید، توسعه، نگهداری، استفاده، و امنیت دارائی توسط مدیریت تائید شده است. عبارت مالک اشاره به فردی نیست که مستقیماً به دارایی دسترسی دارد

A.8 Human resources security		
A.8.1 Prior to employment [1] **Objective**: *To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.*		
A.8.1.1	**Roles and responsibilities**	**Control** Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.
A.8.1.2	**Screening**	**Control** Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
A.8.1.3	**Terms and conditions of employment**	**Control** As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

1 Explanation: The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

الف-۸ امنیت منابع انسانی		
الف-۸-۱ قبل از استخدام [1] **هدف**: *حصول اطمینان از این که کارکنان، پیمانکاران و کاربران ثالث مسئولیت-های خود را می‌شناسند و برای وظایفی که برای ایشان در نظرگرفته شده است مناسب هستند و مخاطرات سرقت، کلاهبرداری یا سوء استفاده از امکانات کاهش خواهد یافت.*		
الف ۸-۱-۱	**وظایف و مسئولیت‌ها**	**کنترل** وظایف و مسئولیت‌های امنیتی کارکنان، پیمانکاران و کاربران ثالث باید بر اساس خط-مشی امنیت اطلاعات سازمان تعریف و مستند-سازی شود.
الف ۸-۱-۲	**گزینش**	**کنترل** به‌منظور تایید پیشینه تمامی نامزدهای استخدامی، پیمانکاران و کاربران ثالث باید بر اساس قوانین، مقررات و معیارهای اخلاقی مربوطه و متناسب با الزامات کسب‌وکار، طبقه-بندی اطلاعاتی که قرار است در دسترس قرار گیرند و مخاطره‌های مشاهده شده بررسی انجام شود.
الف ۸-۱-۳	**ضوابط و شرایط استخدام**	**کنترل** کارکنان، پیمانکاران و کاربران ثالث ملزم خواهند بود تا به عنوان بخشی از تعهدات قراردادیشان، ضوابط و شرایط قرارداد استخدامی خود را که مسئولیت‌های ایشان و سازمان را در قبال امنیت اطلاعات تعیین میکند پذیرش نموده و امضاء نمایند.

۱ توضیح: واژه" استخدام "در اینجا کلیه موارد ذیل را شامل می‌شود: استخدام فرد (به صورت موقت یا دائمی) تعیین جایگاه شغلی، تغییر جایگاه شغلی، واگذاری قراردادها و فسخ هر یک از این قراردادها.

A.8.2 During employment **Objective**: *To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.*		
A.8.2.1	**Management responsibilities**	**Control** Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
A.8.2.2	**Information security awareness, education and training**	**Control** All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
A.8.2.3	**Disciplinary process**	**Control** There shall be a formal disciplinary process for employees who have committed a security breach.
A.8.3 Termination or change of employment **Objective**: *To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.*		
A.8.3.1	**Termination responsibilities**	**Control** Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
A.8.3.2	**Return of assets**	**Control** All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

الف-۸-۲ ضمن خدمت **هدف:** *حصول اطمینان از این که کلیه کارکنان، پیمانکاران و کاربران ثالث نسبت به تهدیدها و نگرانی‌های مرتبط با امنیت اطلاعات، مسئولیت‌ها و تعهدات خویش آگاهی داشته و آمادگی لازم برای حمایت از خط‌مشی امنیت اطلاعات در جریان کار عادی خویش را داشته و مخاطره ناشی از خطای انسانی را کاهش خواهند داد.*		
الف ۸-۲-۱	**مسئولیت‌های مدیریت**	**کنترل** مدیریت ملزم خواهد بود تا از کارکنان، پیمانکاران و کاربران ثالث بخواهد تا امنیت را بر اساس خط‌مشی‌ها و رویه‌های تعیین شده سازمان به مورد اجرا بگذارند.
الف ۸-۲-۲	**آگاهی ،تحصیل و آموزش امنیت اطلاعات**	**کنترل** کلیه کارکنان سازمان و بر حسب مورد پیمانکاران و کاربران ثالث ملزم خواهند بود تا برحسب نوع شغل‌شان، دوره‌های آموزشی و آگاه‌سازی و بروزآوری‌های مرتب در خصوص خط‌مشی‌ها و رویه‌های سازمان را طی نمایند.
الف ۸-۲-۳	**فرآیند انظباطی**	**کنترل** در مورد آن‌دسته از کارکنانی که مرتکب نقض امنیت می‌شوند، وجود یک فرآیند انضباطی رسمی الزامی خواهد بود.
الف-۸-۳ فسخ یا تغییر شغل **هدف:** *حصول اطمینان از این که کارکنان، پیمانکاران و کاربران ثالث بر اساس یک ضابطه مشخص، سازمان را ترک کرده یا تغییر شغل داده‌اند.*		
الف ۸-۳-۱	**مسئولیت‌های خاتمه خدمت**	**کنترل** مسئولیت‌ها در قبال فسخ استخدام یا تغییر آن باید به صراحت تعیین شده و تخصیص داده شوند.
الف ۸-۳-۲	**عودت دارایی‌ها**	**کنترل** کلیه کارکنان، پیمانکاران و اشخاص ثالث ملزم خواهند بود تا به محض فسخ استخدام، قرارداد یا موافقت‌نامه خود، نسبت به عودت دارایی‌های سازمان که در اختیارشان قرار داشته است اقدام نمایند.

A.8.3.3	Removal of access rights	**Control** The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
A.9 Physical and environmental security		
A.9.1 Secure areas **Objective**: *To prevent unauthorized physical access, damage and interference to the organization's premises and information.*		
A.9.1.1	Physical security perimeter	**Control** Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	**Control** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	**Control** Physical security for offices, rooms, and facilities shall be designed and applied.
A.9.1.4	Protecting against external and environmental threats	**Control** Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-mad disaster shall be designed and applied.

الف ۸-۳-۳	حذف حقوق دسترسی	**کنترل** حق دسترسی کلیه کارکنان، پیمانکاران و کاربران ثالث به اطلاعات و مراکز پردازش اطلاعات باید به محض فسخ استخدام، قرارداد یا موافقت‌نامه حذف شده و یا به محض هرگونه تغییر، تنظیم شود.
الف-۹ امنیت فیزیکی و پیرامونی		
الف-۹-۱ مکان‌های امن **هدف:** *جلوگیری از دسترسی غیرمجاز، خسارت و تعرض به دارایی و اطلاعات سازمان*		
الف ۹-۱-۱	حصار امنیت فیزیکی	**کنترل** به منظور محافظت از مناطقی که اطلاعات و امکانات پردازش اطلاعات در آن قرار دارند، استفاده از موانع امنیتی (حصارهایی مانند دیوارها، گیت‌های ورودی که با استفاده از کارت‌های ورود کنترل می‌شوند یا پیشخوان‌های پذیرش که توسط پرسنل بازرسی اداره می‌شوند) لازم و ضروری خواهد بود.
الف ۹-۱-۲	کنترل‌های مبادی ورودی فیزیکی	**کنترل** مکان‌های امن باید با استفاده از کنترل‌های ورودی مناسب محافظت شوند تا به این ترتیب اطمینان حاصل شود که افراد مجاز اجازه دسترسی دارند.
الف ۹-۱-۳	تامین امنیت ادارات، اتاق‌ها و تجهیزات	**کنترل** طراحی و به اجرا گذاشتن امنیت فیزیکی ادارات، اتاق‌ها و تجهیزات الزامی است.
الف ۹-۱-۴	محافظت در برابر تهدیدات خارجی و محیطی	**کنترل** محافظت فیزیکی در برابر خسارات ناشی از آتش‌سوزی، سیل، زمین لرزه، انفجار، ناآرامی‌های اجتماعی و سایر اَشکال بلایای طبیعی یا ساخته دست بشر باید طراحی و به مورد اجرا گذاشته شود.

A.9.1.5	**Working in secure areas**	**Control** Physical protection and guidelines for working in secure areas shall be designed and applied.
A.9.1.6	**Public access, delivery and loading areas**	**Control** Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access
A.9.2 Equipment security **Objective**: *To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.*		
A.9.2.1	**Equipment siting and protection**	**Control** Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.9.2.2	**Supporting utilities**	**Control** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities
A.9.2.3	**Cabling security**	**Control** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
A.9.2.4	**Equipment maintenance**	**Control** Equipment shall be correctly maintained to ensure its continued availability and integrity

الف ۹-۱-۵	**کار کردن در مکان‌های امن**	**کنترل** محافظت فیزیکی و دستورالعمل‌های مربوط به کارکردن در مکان‌های امن باید طراحی و به مورد اجرا گذاشته شود.
الف ۹-۱-۶	**نواحی دسترسی عمومی، تحویل و بارگیری**	**کنترل** نقاط دسترسی از جمله نقاط تحویل و بار-گیری و سایر نقاطی که احتمال ورود افراد غیرمجاز به آن‌ها می‌رود باید کنترل شده و حتی‌الامکان از مراکز پردازش اطلاعات مجزا گردد تا به این ترتیب از دسترسی غیرمجاز به آن‌ها جلوگیری شود.
الف ۹-۲ امنیت تجهیزات **هدف:** *جلوگیری از فقدان، خسارت، سرقت یا به مخاطره افتادن دارایی‌ها و ایجاد وقفه در فعالیت‌های سازمان*		
الف ۹-۲-۱	**تعیین محل تجهیزات و محافظت از آن**	**کنترل** تعیین محل مناسب یا محافظت از تجهیزات باید به‌گونه‌ای انجام شود که مخاطره‌های ناشی از تهدیدها و خطرهای زیست‌محیطی و فرصت برای دسترسی غیرمجاز کاهش یابد.
الف ۹-۲-۲	**تاسیسات پشتیبانی**	**کنترل** تجهیزات باید در برابر قطع برق و سایر وقفه‌های ناشی از بروز خرابی در تاسیسات پشتیبانی محافظت شوند.
الف ۹-۲-۳	**امنیت کابل کشی‌ها**	**کنترل** کابل‌های برق و مخابرات که وظیفه انتقال داده‌ها یا پشتیبانی از خدمات اطلاع‌رسانی را دارند باید د برابر قطع‌شدگی یا آسیب‌دیدگی محافظت شوند.
الف ۹-۲-۴	**نگهداری تجهیزات**	**کنترل** تجهیزات باید به‌درستی نگهداری شوند تا در دسترس بودن و بی‌عیب بودن آن‌ها مورد اطمینان واقع گردد.

A.9.2.5	Security of equipment off-premises	**Control** Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
A.9.2.6	Secure disposal or re-use of equipment	**Control** All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
A.9.2.7	Removal of property	**Control** Equipment, information or software shall not be taken off-site without prior authorization
A.10 Communications and operations management		
A.10.1 Operational procedures and responsibilities **Objective**: *To ensure the correct and secure operation of information processing facilities*		
A.10.1.1	Documented operating procedure	**Control** Operating procedures shall be documented, maintained, and made available to all users who need them.
A.10.1.2	Change management	**Control** Changes to information processing facilities and systems shall be controlled.

الف ۹-۲-۵	امنیت تجهیزاتی که در خارج از محوطه سازمان هستند	**کنترل** امنیت تجهیزاتی که در خارج از محوطه سازمان قرار دارند، باید با در نظر گرفتن مخاطره‌های مختلف ناشی از کار کردن در خارج از محوطه سازمان تامین گردد.
الف ۹-۲-۶	امحاء یا استفاده دوباره از تجهیزات به طور ایمن	**کنترل** تمام اجزای تجهیزاتی که دارای وسایل ذخیره‌سازی هستند باید چک شوند تا به این ترتیب اطمینان حاصل شود که قبل از امحا، همه داده‌های حساس و نرم‌افزارهای دارای حق امتیاز پاک شده و یا به طور ایمن رونویسی شده باشند.
الف ۹-۲-۷	خارج ساختن اموال	**کنترل** تجهیزات، اطلاعات یا نرم‌افزار نباید بدون مجوز قبلی از محل خارج گردند.
الف-۱۰ مدیریت ارتباطات و عملیات		
الف-۱۰-۱ روشهای اجرایی عملیاتی و مسئولیت‌ها **هدف:** *حصول اطمینان از عملیات صحیح و امن تجهیزات پردازش اطلاعات.*		
الف ۱۰-۱-۱	رویه‌های عملیاتی مستند-سازی شده	**کنترل** رویه‌های عملیاتی (اجرایی) باید مستندسازی شده، نگاهداری شده و در اختیار کاربرانی که به آن‌ها نیاز دارند قرار داده شود.
الف ۱۰-۱-۲	مدیریت تغییر	**کنترل** هرگونه تغییر در سیستم‌ها و امکانات پردازش اطلاعات باید تحت کنترل باشد.

A.10.1.3	**Segregation of duties**	**Control** Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.10.1.4	**Separation of development, test and operational facilities**	**Control** Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.
A.10.2 Third party service delivery management **Objective**: *To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.*		
A.10.2.1	**Service delivery**	**Control** It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
A.10.2.2	**Monitoring and review of third party services**	**Control** The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

الف ۱۰-۱-۳	تفکیک وظایف	**کنترل** وظایف و حوزه‌های مسئولیت باید تفکیک شوند تا به این ترتیب فرصت‌های موجود برای انجام هرگونه تغییر غیرمجاز یا غیرعمدی یا سوءاستفاده از دارایی سازمان کاهش یابد.
الف ۱۰-۱-۴	جداسازی امکانات توسعه، آزمایش و عملیاتی	**کنترل** امکانات توسعه، آزمایش و عملیات باید از یکدیگر مجزا شوند تا به این ترتیب مخاطره-های دسترسی یا تغییر غیرمجاز در سیستم عملیاتی کاهش یابد.
الف ۱۰-۲ مدیریت ارائه خدمات به اشخاص ثالث **هدف:** *اجرا و حفظ سطح مناسبی از امنیت اطلاعات و ارائه خدمات در راستای موافقت‌نامه‌های ارائه خدمات به اشخاص ثالث*		
الف ۱۰-۲-۱	تحویل خدمات	**کنترل** باید اطمینان حاصل کرد که مطابق با توافق نحوه تحویل خدمت که با اشخاص ثالث به عمل آمده، کنترل‌های امنیتی، مشخصات خدمت و سطوح تحویل، توسط اشخاص ثالث پیاده‌سازی، اجرا و نگاهداری شده است.
الف ۱۰-۲-۲	پایش و بازنگری خدمات اشخاص ثالث	**کنترل** خدمات، گزارش‌ها و سوابقی که توسط اشخاص ثالث ارائه می‌گردد باید به‌طور منظم پایش و مورد بازنگری قرار گیرد و ممیزی‌ها نیز باید به‌طور منظم انجام پذیرد.

A.10.2.3	**Managing changes to third party services**	**Control** Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 System planning and acceptance **Objective**: *To minimize the risk of systems failures.*		
A.10.3.1	**Capacity management**	**Control** The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
A.10.3.2	**System acceptance**	**Control** Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 Protection against malicious and mobile code **Objective**: *To protect the integrity of software and information.*		
A.10.4.1	**Controls against malicious code**	**Control** Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

الف ۱۰-۲-۳	**مدیریت تغییرات در خدمات اشخاص ثالث**	**کنترل** تغییرات در شیوه ارائه خدمات، شامل حفظ و بهبود خط‌مشی‌های فعلی امنیت اطلاعات، رویه‌ها و کنترل‌ها با توجه به اهمیت سیستم‌های کسب و کار و فرآیندهای مرتبط به آن و ارزیابی مجدد مخاطرات، باید مدیریت شود.
الف ۱۰-۳ طرح‌ریزی و پذیرش سیستم **هدف:** *به حداقل‌رساندن مخاطره ناشی از خرابی‌های سیستم*		
الف ۱۰-۳-۱	**مدیریت ظرفیت**	**کنترل** استفاده از منابع باید مورد پایش قرار گرفته، اصلاح‌شده و برآورد ظرفیت مورد نیاز آینده انجام شود تا به این ترتیب از کارایی سیستم موردنظر اطمینان حاصل شود.
الف ۱۰-۳-۲	**پذیرش سیستم**	**کنترل** معیارهای پذیرش سیستم‌های جدید اطلاعات، نسخه‌های ارتقاء یافته و نسخه‌های جدید باید تعیین شود و تست‌های مناسب سیستم(ها) در جریان توسعه و قبل از پذیرش انجام شود.
الف ۱۰-۴ محافظت در برابر کدهای مخرب و سیار **هدف:** *محافظت از یکپارچگی نرم‌افزار و اطلاعات*		
الف ۱۰-۴-۱	**اقدامات کنترلی در برابر کدهای مخرب**	**کنترل** اقدامات نظارتی در خصوص آشکارسازی، پیشگیری و بازیابی به منظور محافظت در برابر کدهای مخرب و رویه‌های مناسب آگاه‌سازی کاربر باید به مورد اجرا گذاشته شود.

A.10.4.2	**Controls against mobile code**	**Control** Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A.10.5 Back-up **Objective**: *To maintain the integrity and availability of information and information processing facilities*		
A.10.5.1	**Information back-up**	**Control** Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.
A.10.6 Network security management **Objective:** *To ensure the protection of information in networks and the protection of the supporting infrastructure.*		
A.10.6.1	**Network controls**	**Control** Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

الف ۱۰-۴-۲	**اقدامات کنترلی در برابر کدهای سیار**	**کنترل** در جایی که استفاده از کدهای سیار مجاز دانسته شده است، باید اطمینان حاصل شود که کد سیار مجاز بر اساس یک سیاست و خط‌مشی امنیتی کاملا" مشخص کار می‌کند و از اجرایی‌شدن کدهای سیار غیرمجاز باید جلوگیری شود.
الف-۱۰-۵ پشتیبان گیری **هدف:** *حفظ یکپارچگی و در دسترس بودن اطلاعات و امکانات پردازش اطلاعات*		
الف ۱۰-۵-۱	**پشتیبان گیری از اطلاعات**	**کنترل** نسخه‌های پشتیبان اطلاعات و نرم‌افزار باید به‌طور منظم بر اساس خط‌مشی مورد توافق تهیه و تست شوند.
الف-۱۰-۶ مدیریت امنیت شبکه **هدف:** *حصول اطمینان از محافظت اطلاعات در شبکه‌ها و محافظت از زیر-ساختارهای پشتیبان*		
الف ۱۰-۶-۱	**کنترل‌های شبکه**	**کنترل** شبکه‌ها باید به‌طور مناسب مدیریت و کنترل شوند تا به این ترتیب در برابر تهدیدات محافظت شوند و امنیت سیستم‌ها و نرم‌افزار-های تحت شبکه از جمله اطلاعات در حال گذر حفظ شوند.

A.10.6.2	**Security of network services**	**Control** Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 Media handling **Objective**: *To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.*		
A.10.7.1	**Management of removable media**	**Control** There shall be procedures in place for the management of removable media.
A.10.7.2	**Disposal of media**	**Control** Media shall be disposed of securely and safely when no longer required, using formal procedures.
A.10.7.3	**Information handling procedures**	**Control** Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
A.10.7.4	**A.10.7.4 Security of system documentation**	**Control** System documentation shall be protected against unauthorized access.

الف ۱۰-۶-۲	امنیت خدمات شبکه	**کنترل** مشخصه‌های امنیتی، سطوح خدمات و الزامات مدیریتی تمامی خدمات شبکه باید تعیین و در هریک از موافقت‌نامه‌های خدمات شبکه لحاظ گردد، اعم از این‌که خدمات در - داخل انجام شود یا برون‌سپاری شود.
الف-۱۰-۷ اداره‌کردن رسانه **هدف:** *جلوگیری از افشای غیرمجاز،تغییر، از بین‌بردن یا نابودسازی دارایی‌ها و ایجاد وقفه در تداوم کسب‌وکار*		
الف ۱۰-۷-۱	مدیریت رسانه-های قابل جابجایی	**کنترل** وجود رویه‌های اجرایی برای مدیریت رسانه-های قابل‌جابجایی لازم و ضروری خواهد بود.
الف ۱۰-۷-۲	امحای رسانه‌ها	**کنترل** رسانه‌هایی‌که دیگر نیازی بدان‌ها نیست باید بر اساس رویه‌های رسمی و به صورت امن و ایمن امحا شوند.
الف ۱۰-۷-۳	رویه‌های جابجایی اطلاعات	**کنترل** رویه‌های مربوط به جابه‌جایی و ذخیره‌سازی اطلاعات باید به‌گونه‌ای تعیین شوند که از این اطلاعات در برابر افشای غیـرمجاز یا سوءاستفاده محافظت شود.
الف ۱۰-۷-۴	امنیت مستندات سیستم	**کنترل** مستندات سیستم در برابر دسترسی غیر-مجاز باید محافظت شود.

A.10.8 Exchange of information **Objective**: *To maintain the security of information and software exchanged within an organization and with any external entity.*		
A.10.8.1	**Information exchange policies and procedures**	**Control** Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
A.10.8.2	**Exchange agreements**	**Control** Agreements shall be established for the exchange of information and software between the organization and external parties.
A.10.8.3	**Physical media in transit**	**Control** Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
A.10.8.4	**Electronic messaging**	**Control** Information involved in electronic messaging shall be appropriately protected.
A.10.8.5	**Business information systems**	**Control** Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

الف-۱۰-۸ تبادل اطلاعات **هدف :** *حفظ امنیت اطلاعات و نرم‌افزار مبادله‌شده در یک سازمان و با هرنهاد بیرونی.*		
الف ۱۰-۸-۱	**خط‌مشی‌ها و رویه‌های تبادل اطلاعات**	**کنترل** خط‌مشی‌ها، رویه‌ها و اقدامات کنترلی رسمی تبادل اطلاعات، باید به نحوی به مورد اجرا گذاشته شوند که با استفاده از تمامی امکانات تبادل اطلاعات از فرآیند تبادل اطلاعات محافظت شود.
الف ۱۰-۸-۲	**موافقت‌نامه‌های تبادل**	**کنترل** توافق‌نامه‌های تبادل اطلاعات و نرم‌افزار بین سازمان و مخاطبان برون‌سازمانی لازم و ضروری می‌باشد.
الف ۱۰-۸-۳	**رسانه‌های فیزیکی در حال انتقال**	**کنترل** رسانه‌های حاوی اطلاعات باید در برابر دسترسی غیرمجاز، سوءاستفاده یا صدمه در جریان نقل و انتقال بیرون از مرزهای فیزیکی سازمان محافظت شوند.
الف ۱۰-۸-۴	**ارسال پیغام به صورت الکترونیکی**	**کنترل** اطلاعاتی که در قالب پیغام الکترونیکی مبادله می‌شوند، باید به صورت مناسب محافظت شوند.
الف ۱۰-۸-۵	**سیستم‌های اطلاعات کسب‌وکار**	**کنترل** خط‌مشی‌ها و رویه‌ها باید به‌گونه‌ای ایجاد و به مورد اجرا گذاشته شوند که امکان محافظت از اطلاعات مرتبط با ارتباطات بین سیستم‌های کسب‌وکار سازمان وجود داشته باشد.

A.10.9 Electronic commerce services **Objective:** *To ensure the security of electronic commerce services, and their secure use.*		
A.10.9.1	**Electronic commerce**	**Control** Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
A.10.9.2	**On-line transactions**	**Control** Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.10.9.3	**Publicly available information**	**Control** The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 Monitoring **Objective**: *To detect unauthorized information processing activities.*		
A.10.10.1	**Audit logging**	**Control** Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

الف-۱۰-۹ خدمات تجارت الکترونیک **هدف:** *حصول اطمینان از امنیت خدمات تجارت الکترونیک و استفاده ایمن از آن‌ها.*		
الف ۱۰-۹-۱	**تجارت الکترونیک**	**کنترل** اطلاعات مربوط به تجارت الکترونیک که از طریق شبکه‌های عمومی منتقل می‌شوند باید در برابر فعالیت‌های غیرقانونی، اختلافات موجود بر سر قرارداد، افشا و تعدیل غیرمجاز محافظت شوند.
الف ۱۰-۹-۲	**معاملات برخط**	**کنترل** اطلاعات مربوط به معاملات برخط باید به‌گونه‌ای محافظت شوند که از انتقال ناقص، مسیریابی غلط، تغییر غیرمجاز پیام، افشای غیرمجاز، تکثیر یا تجدید پیام غیرمجاز جلوگیری شود.
الف ۱۰-۹-۳	**اطلاعاتی که در دسترس عموم قرار دارد**	**کنترل** یکپارچگی اطلاعاتی که از طریق یک سیستم با کاربری عمومی در معرض دسترسی قرار می‌گیرند باید به‌گونه‌ای محافظت گردد که از هر گونه تغییر غیرمجاز جلوگیری شود.
الف-۱۰-۱۰ پایش **هدف:** *آشکارسازی فعالیت‌های غیرمجاز پردازش اطلاعات*		
الف ۱۰-۱۰-۱	**ثبت وقایع ممیزی**	**کنترل** سابقه وقایع ممیزی که شامل فعالیت‌های کاربر، اعتراضات و رویدادهای امنیت اطلاعات می‌باشد باید ایجاد و به مدت زمان توافق‌شده نگاهداری شود تا به ما در بررسی‌های آتی و پایش کنترل دسترسی کمک کند.

A.10.10.2	**Monitoring system use**	**Control** Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A.10.10.3	**Protection of log information**	**Control** Logging facilities and log information shall be protected against tampering and unauthorized access.
A.10.10.4	**Administrator and operator logs**	**Control** System administrator and system operator activities shall be logged.
A.10.10.5	**Fault logging**	**Control** Faults shall be logged, analyzed, and appropriate action taken.
A.10.10.6	**Clock synchronization**	**Control** The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11 Access control		
A.11.1 Business requirement for access control Objective: *To control access to information.*		
A.11.1.1	**Access control policy**	**Control** An access control policy shall be established, documented, and reviewed based on business and security requirements for access.

الف ۱۰-۱۰-۲	استفاده از سیستم پایش	**کنترل** رویه‌های مربوط به پایش استفاده از امکانات پردازش اطلاعات باید ایجاد شود و نتایج اقدامات پایش باید بصورت منظم بازبینی شوند.
الف ۱۰-۱۰-۳	محافظت از اطلاعات ثبت وقایع	**کنترل** امکانات ثبت وقایع و اطلاعات ثبت شده باید در برابر دسترسی‌های پنهانی و غیر- مجاز محافظت شوند.
الف ۱۰-۱۰-۴	ثبت وقایع راهبر و متصدی سیستم	**کنترل** وقایع فعالیت‌های راهبر سیستم و متصدی سیستم باید ثبت گردد.
الف ۱۰-۱۰-۵	ثبت وقایع خرابی	**کنترل** وقایع خرابی باید ثبت شده و مورد تجزیه و تحلیل قرار گیرند و برخوردهای مناسب در این خصوص بعمل آید.
الف ۱۰-۱۰-۶	همزمان کردن ساعت	**کنترل** ساعت‌های کلیه سیستم‌های پردازش اطلاعات در یک سازمان یا دامنه امنیت باید با استفاده از یک مبداء زمانی دقیق مورد توافق، همزمان شوند.
الف-۱۱ کنترل دسترسی		
الف-۱۱-۱ الزامات کاری برای کنترل دسترسی **هدف:** *کنترل دسترسی به اطلاعات*		
الف ۱۱-۱-۱	خط‌مشی کنترل دسترسی	**کنترل** باید یک خط‌مشی کنترل دسترسی براساس الزامات کاری و امنیتی مربوط به دسترسی ایجاد، مستندسازی و بازنگری شود.

A.11.2 User access management **Objective**: *To ensure authorized user access and to prevent unauthorized access to information systems*		
A.11.2.1	**User registration**	**Control** There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A.11.2.2	**Privilege management**	**Control** The allocation and use of privileges shall be restricted and controlled.
A.11.2.3	**User password management**	**Control** The allocation of passwords shall be controlled through a formal management process.
A.11.2.4	**Review of user access rights**	**Control** Management shall review users' access rights at regular intervals using a formal process.
A.11.3 User responsibilities **Objective**: *To prevent unauthorized user access, and compromise or theft of information and information processing facilities.*		
A.11.3.1	**Password use**	**Control** Users shall be required to follow good security practices in the selection and use of passwords.
A.11.3.2	**Unattended user equipment**	**Control** Users shall ensure that unattended equipment has appropriate protection.

الف-۱۱-۲ مدیریت دسترسی کاربر **هدف:** *حصول اطمینان از دسترسی مجاز کاربران و جلوگیری از دسترسی غیرمجاز به سیستم‌های اطلاعات*		
الف ۱-۲-۱۱	**ثبت‌نام کاربر**	**کنترل** وجود یک رویه رسمی ثبت‌نام و لغو ثبت‌نام کاربر در محل برای اعطا و لغو حق دسترسی به کلیه سیستم‌های اطلاعاتی و خدمات لازم و ضروری خواهد بود.
الف ۲-۲-۱۱	**مدیریت اختیارات ویژه**	**کنترل** تخصیص و استفاده از اختیارات ویژه باید محدود و کنترل شده باشد.
الف ۳-۲-۱۱	**مدیریت کلمه عبور کاربر**	**کنترل** تخصیص کلمه‌های عبور، باید براساس یک فرآیند رسمی مدیریتی کنترل شود.
الف ۴-۲-۱۱	**بازنگری حقوق دسترسی کاربر**	**کنترل** مدیریت ملزم خواهد بود تا با استفاده از یک فرآیند رسمی، حقوق دسترسی کاربران را در فواصل زمانی منظم مورد بازنگری قرار دهد.
الف-۱۱-۳ مسئولیت‌های کاربر **هدف:** *جلوگیری از دسترسی کاربر غیرمجاز و به مخاطره افتادن یا سرقت اطلاعات و امکانات پردازش اطلاعات*		
الف ۱-۳-۱۱	**استفاده از کلمه عبور**	**کنترل** کاربران ملزم خواهند بود تا در انتخاب و استفاده از کلمات عبور از روش‌های امنیتی مناسب تبعیت کنند.
الف ۲-۳-۱۱	**تجهیزات بدون مراقبت کاربر**	**کنترل** کاربران باید از این بابت که تجهیزات بدون مراقبت به طور مناسب محافظت می‌شوند، اطمینان حاصل نمایند.

A.11.3.3	**Clear desk and clear screen policy**	**Control** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.11.4 Network access control **Objective**: *To prevent unauthorized access to networked services*		
A.11.4.1	**Policy on use of network services**	**Control** Users shall only be provided with access to the services that they have been specifically authorized to use.
A.11.4.2	**User authentication for external connections**	**Control** Appropriate authentication methods shall be used to control access by remote users.
A.11.4.3	**Equipment identification in networks**	**Control** Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
A.11.4.4	**Remote diagnostic and configuration port protection**	**Control** Physical and logical access to diagnostic and configuration ports shall be controlled.
A.11.4.5	**Segregation in networks**	**Control** Groups of information services, users, and information systems shall be segregated on networks.

الف ۱۱-۳-۳	**خط‌مشی میزکار تمیز و صفحه نمایش پاک**	**کنترل** یک خط‌مشی میزکار تمیز در مورد کاغذها و رسانه‌های ذخیره‌سازی قابل جابجایی و یک خط‌مشی صفحه نمایش پاک در مورد امکانات پردازش اطلاعات باید مورد پذیرش قرار گیرد.
الف ۱۱-۴ کنترل دسترسی به شبکه **هدف:** *جلوگیری از دسترسی غیرمجاز به خدمات شبکه.*		
الف ۱۱-۴-۱	**خط‌مشی استفاده از خدمات شبکه**	**کنترل** کاربران باید تنها به خدماتی دسترسی داشته باشند که مجوز استفاده از آن‌ها به صورت مشخص صادر شده باشد.
الف ۱۱-۴-۲	**احراز هویت کاربر برای ارتباطات بیرونی**	**کنترل** به‌منظور کنترل دسترسی، روش‌های احراز هویت مناسب، برای کاربران راه دور باید مورد استفاده قرار گیرد.
الف ۱۱-۴-۳	**شناسایی تجهیزات در شبکه**	**کنترل** شناسایی خودکار تجهیزات باید به عنوان یک روش برای احراز هویت ارتباط از مکان‌ها و تجهیزات خاص مورد توجه قرار گیرد.
الف ۱۱-۴-۴	**محافظت از درگاه عیب یابی و پیکر-بندی از راه دور**	**کنترل** دسترسی فیزیکی و منطقی به پورت‌های عیب یابی و پیکربندی باید کنترل شود.
الف ۱۱-۴-۵	**تفکیک در شبکه ها**	**کنترل** گروه‌های مختلف سرویس‌های اطلاعات، کاربران و سیستم‌های اطلاعاتی باید بر روی شبکه‌ها تفکیک و مجزا شوند.

A.11.4.6	**Network connection control**	**Control** For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).
A.11.4.7	**Network routing control**	**Control** Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 Operating system access control **Objective**: *To prevent unauthorized access to operating systems.*		
A.11.5.1	**Secure log-on procedures**	**Control** Access to operating systems shall be controlled by a secure log-on procedure.
A.11.5.2	**User identification and authentication**	**Control** All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A.11.5.3	**Password management system**	**Control** Systems for managing passwords shall be interactive and shall ensure quality passwords.

الف ۱۱-۴-۶	**کنترل اتصال به شبکه**	**کنترل** در مورد شبکه‌های مشترک و به‌خصوص شبکه‌هایی که در مرزهای سازمان توسعه یافته‌اند لازم است تا توانایی کاربران در اتصال به شبکه بر اساس خط‌مشی کنترل دسترسی و الزامات برنامه‌های کاربردی کسب و کار محدود شود. (به بند ۱۱-۱ مراجعه نمایید)
الف ۱۱-۴-۷	**کنترل مسیریابی شبکه**	**کنترل** کنترل‌های مسیریابی در شبکه‌ها باید به مورد اجرا گذاشته شود تا به این ترتیب اطمینان حاصل گردد که اتصالات کامپیوتری و گردش اطلاعاتی، خط‌مشی کنترل دسترسی برنامه-های کاربردی کسب‌وکار را نقض نکرده‌اند.
الف-۱۱-۵ کنترل دسترسی به سیستم عامل **هدف:** *جلوگیری از دسترسی غیرمجاز به سیستم‌های عامل*		
الف ۱۱-۵-۱	**رویه‌های ورود امن به سیستم**	**کنترل** دسترسی به سیستم‌های عامل باید به‌وسیله رویه ورود امن کنترل شود.
الف ۱۱-۵-۲	**شناسایی کاربر و احراز هویت**	**کنترل** کلیه کاربران باید یک شناسه منحصر به فرد (ID) فقط برای کاربری خود داشته باشند و یک تکنیک مناسب احراز هویت برای اثبات هویت ادعاشده توسط یک کاربر انتخاب گردد.
الف ۱۱-۵-۳	**سیستم مدیریت کلمه عبور**	**کنترل** سیستم‌های مربوط به مدیریت کلمات عبور باید تعاملی بوده و کیفیت کلمات‌عبور را تضمین نماید.

A.11.5.4	**Use of system utilities**	**Control** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.11.5.5	**Session time-out**	**Control** Inactive sessions shall shut down after a defined period of inactivity.
A.11.5.6	**Limitation of connection time**	**Control** Restrictions on connection times shall be used to provide additional security for high-risk applications.
A.11.6 Application and information access control **Objective:** *To prevent unauthorized access to information held in application systems.*		
A.11.6.1	**Information access restriction**	**Control** Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
A.11.6.2	**Sensitive system isolation**	**Control** Sensitive systems shall have a dedicated (isolated) computing environment.
A.11.7 Mobile computing and teleworking **Objective:** *To ensure information security when using mobile computing and teleworking facilities.*		

الف ۱۱-۵-۴	استفاده از برنامه-های کمکی سیستم	**کنترل** استفاده از برنامه‌های کمکی که ممکن است باعث جلوگیری از کنترل‌های سیستم و برنامه‌های کاربردی شود باید محدود و به شدت کنترل شوند.
الف ۱۱-۵-۵	انقضای مهلت نشست	**کنترل** نشست‌های غیرفعال باید پس از گذشت یک مدت زمان معین عدم فعالیت خاتمه یابد.
الف ۱۱-۵-۶	محدود ساختن زمان ارتباط	**کنترل** به‌منظور تامین‌امنیت بیشتر برای نرم‌افزارهای با مخاطره بالا، محدود ساختن زمان ارتباط ضروری خواهد بود.
الف ۱۱-۶ کنترل دسترسی به اطلاعات و برنامه‌های کاربردی **هدف:** *جلوگیری از دسترسی غیرمجاز به اطلاعاتی که در سیستم‌های کاربردی نگاهداری می‌شوند.*		
الف ۱۱-۶-۱	محدودیت دسترسی به اطلاعات	**کنترل** دسترسی کاربران و کارمندان پشتیبانی به اطلاعات و توابع سیستم کاربردی باید بر اساس خط‌مشی مشخص کنترل دسترسی محدود شود.
الف ۱۱-۶-۲	جداسازی سیستم-های حساس	**کنترل** سیستم‌های حساس باید از یک محیط محاسباتی اختصاصی (مجزا) برخوردار باشند.
الف ۱۱-۷ کار از راه دور و پردازش سیار **هدف:** *حصول اطمینان از امنیت اطلاعات در زمان استفاده از امکانات کار از راه دور و پردازش سیار*		

A.11.7.1	Mobile computing and communications	**Control** A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
A.11.7.2	Teleworking	**Control** A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12 Information systems acquisition, development and maintenance		
A.12.1 Security requirements of information systems **Objective:** *To ensure that security is an integral part of information systems.*		
A.12.1.1	Security requirements analysis and specification	**Control** Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
A.12.2 Correct processing in applications **Objective:** *To prevent errors, loss, unauthorized modification or misuse of information in applications.*		
A.12.2.1	Input data validation	**Control** Data input to applications shall be validated to ensure that this data is correct and appropriate.
A.12.2.2	Control of internal processing	**Control** Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

الف ۱۱-۷-۱	پردازش و ارتباطات سیار	**کنترل** جاری بودن یک خط‌مشی رسمی به‌جا و شایسته و اتخاذ اقدامات امنیتی مناسب برای محافظت در برابر مخاطره‌های وارد بر استفاده از امکانات ارتباطی و محاسباتی سیار لازم و ضروری است.
الف ۱۱-۷-۲	کار از راه دور	**کنترل** ایجاد و اجرای خط‌مشی، برنامه‌ها و رویه‌های عملیاتی در مورد فعالیت‌های کار از راه دور لازم و ضروری است.
الف-۱۲ اکتساب، توسعه و نگهداری سیستم‌های اطلاعاتی		
الف-۱۲-۱ الزامات امنیتی سیستم‌های اطلاعاتی **هدف:** *حصول اطمینان از این که امنیت، جزء لاینفکی از سیستم‌های اطلاعاتی می‌باشد.*		
الف ۱۲-۱-۱	مشخصات و تجزیه و تحلیل الزامات امنیتی	**کنترل** درگزارش الزامات کسب و کار سیستم‌های اطلاعاتی جدید یا موارد ارتقاء در سیستم‌های اطلاعاتی موجود باید الزامات مربوط به کنترل‌های امنیتی معین شده باشد.
الف-۱۲-۲ پردازش صحیح در برنامه‌های کاربردی **هدف:** *جلوگیری از بروز خطاها، ضرر و زیان، تغییر و تبدیل غیرمجاز یا سوء استفاده از اطلاعات موجود در برنامه‌های کاربردی*		
الف ۱۲-۲-۱	صحه گذاری داده‌های ورودی	**کنترل** داده‌های ورودی به برنامه‌های کاربردی باید صحه گذاری شوند تا از درستی و مناسب بودن داده‌ها اطمینان حاصل شود.
الف ۱۲-۲-۲	کنترل پردازش‌های داخلی	**کنترل** به‌منظور آشکارسازی هرگونه خرابی اطلاعات درحین پردازش خطاها یا اقدامات عمدی کنترل‌های صحه‌گذاری باید در نرم‌افزارهای کاربردی گنجانده شود.

A.12.2.3	**Message integrity**	**Control** Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
A.12.2.4	**Output data validation**	**Control** Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 Cryptographic controls **Objective**: *To protect the confidentiality, authenticity or integrity of information by cryptographic means.*		
A.12.3.1	**Policy on the use of cryptographic controls**	**Control** A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.12.3.2	**Key management**	**Control** Key management shall be in place to support the organization's use of cryptographic techniques.
A.12.4 Security of system files **Objective**: *To ensure the security of system files.*		
A.12.4.1	**Control of operational software**	**Control** There shall be procedures in place to control the installation of software on operational systems
A.12.4.2	**Protection of system test data**	**Control** Test data shall be selected carefully, and protected and controlled.

الف ۱۲-۲-۳	یکپارچگی پیام	**کنترل** الزامات مربوط به حصول اطمینان از صحت و محافظت از یکپارچگی پیام در برنامه‌های کاربردی باید تعیین شود و کنترل‌های مناسب تعیین و به مورد اجرا گذاشته شود.
الف ۱۲-۲-۴	صحه گذاری داده‌های خروجی	**کنترل** داده‌های خروجی از یک برنامه کاربردی باید صحه‌گذاری شود تا از درستی و مناسب بودن پردازش اطلاعات ذخیره شده با شرایط موجود اطمینان حاصل شود.
الف-۱۲-۳ کنترل‌های رمزنگاری **هدف:** *محافظت از محرمانگی، اعتبار و یکپارچگی اطلاعات بوسیله رمزنگاری*		
الف ۱۲-۳-۱	خط‌مشی استفاده از کنترل‌های رمزنگاری	**کنترل** خط‌مشی استفاده از کنترل‌های رمزنگاری به منظور محافظت از اطلاعات باید ایجاد و به مورد اجرا گذاشته شود.
الف ۱۲-۳-۲	مدیریت کلید	**کنترل** مدیریت کلید باید به مورد اجرا گذاشته شود تا به این ترتیب از بکارگیری فنون رمزنگاری سازمان حمایت و پشتیبانی شود.
الف-۱۲-۴ امنیت فایل‌های سیستم **هدف:** *حصول اطمینان از امنیت فایل‌های سیستم*		
الف ۱۲-۴-۱	کنترل نرم‌افزار عملیاتی	**کنترل** وجود رویه‌های مناسب برای کنتـرل نصب نرم‌افزار بر روی سیستم‌های عامل لازم و ضروری خواهد بود.
الف ۱۲-۴-۲	محافظت از داده‌های تست سیستم	**کنترل** داده‌های تست باید به‌دقت انتخاب شده، و محافظت و کنترل شوند.

A.12.4.3	Access control to program source code	**Control** Access to program source code shall be restricted.
A.12.5 Security in development and support processes **Objective:** *To maintain the security of application system software and information.*		
A.12.5.1	Change control procedures	**Control** The implementation of changes shall be controlled by the use of formal change control procedures.
A.12.5.2	Technical review of applications after operating system changes	**Control** When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.12.5.3	Restrictions on changes to software packages	**Control** Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
A.12.5.4	Information leakage	**Control** Opportunities for information leakage shall be prevented.
A.12.5.5	Outsourced software development	**Control** Outsourced software development shall be supervised and monitored by the organization
A.12.6 Technical Vulnerability Management **Objective:** *To reduce risks resulting from exploitation of published technical vulnerabilities.*		
A.12.6.1	Control of technical vulnerabilities	**Control** Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

الف ۱۲-۴-۳	کنترل دسترسی به کد منبع برنامه	**کنترل** دسترسی به کد منبع برنامه باید محدود شود.
الف-۱۲-۵ امنیت در فرآیندهای توسعه و پشتیبانی **هدف:** *حفظ امنیت نرم‌افزار سیستم و اطلاعات کاربردی*		
الف ۱۲-۵-۱	رویه‌های کنترل تغییر	**کنترل** اعمال تغییرات باید با استفاده از رویه‌های رسمی کنترل تغییر، کنترل شود.
الف ۱۲-۵-۲	بازنگری فنی برنامه‌های کاربردی پس از اعمال تغییرات در سیستم عامل	**کنترل** هنگامی که سیستم‌های عامل تغییر می‌کنند، برنامه‌های کاربردی حیاتی کسب و کار باید مورد بازنگری قرار گرفته و تست شود تا از عدم تأثیر سوء بر عملیات سازمانی یا امنیت، اطمینان حاصل شود.
الف ۱۲-۵-۳	اعمال محدودیتها در خصوص تغییرات در بسته‌های نرم‌افزاری	**کنترل** از تغییر و تبدیل در بسته‌های نرم‌افزاری در حد امکان باید ممانعت بعمل آید و به تغییرات لازم و ضروری محدود شود و کلیه تغییرات باید دقیقًا کنترل شوند.
الف ۱۲-۵-۴	نشت اطلاعات	**کنترل** از فرصت‌های نشت اطلاعات باید جلوگیری شود.
الف ۱۲-۵-۵	توسعه نرم‌افزار-های برون سپاری شده	**کنترل** توسعه نرم‌افزارهای برون‌سپاری شده باید توسط سازمان نظارت و پایش شود.
الف-۱۲-۶ مدیریت آسیب‌پذیری فنی **هدف:** *کاهش مخاطره‌های ناشی از بهره‌برداری از آسیب‌پذیری‌های فنی منتشر شده*		
الف ۱۲-۶-۱	کنترل آسیب-پذیری‌های فنی	**کنترل** اطلاعات به‌موقع درباره آسیب‌پذیری‌های فنی سیستم‌های اطلاعاتی که در حال حاضر مورد استفاده قرار می‌گیرند باید جمع‌آوری شده و میزان مواجهه سازمان با این آسیب‌ها ارزشیابی شده و معیارهای مناسب برای توجه به مخاطره‌های وارد بر آن بعمل آید.

A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses **Objective:** *To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.*		
A.13.1.1	Reporting information security events	**Control** Information security events shall be reported through appropriate management channels as quickly as possible.
A.13.1.2	Reporting security weaknesses	**Control** All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services
A.13.2 Management of information security incidents and improvements **Objective**: *To ensure a consistent and effective approach is applied to the management of information security incidents.*		
A.13.2.1	Responsibilities and procedures	**Control** Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	**Control** There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	**Control** Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

الف-۱۳ مدیریت حادثه امنیت اطلاعات		
الف-۱۳-۱ گزارش‌دهی از رویدادها ونقاط ضعف امنیت اطلاعات **هدف :** *حصول اطمینان از این که رویدادها و نقاط ضعف امنیت اطلاعات مرتبط با سیستم‌های اطلاعاتی به‌گونه‌ای اطلاع رسانی می‌شوند که امکان اتخاذ اقدامات اصلاحی به‌موقع وجود دارد.*		
الف ۱-۱-۱۳	گزارش‌دهی رویدادهای امنیت اطلاعات	**کنترل** رویدادهای امنیت اطلاعات باید از طریق کانال‌های مدیریتی مناسب و در اسرع وقت گزارش شود.
الف ۲-۱-۱۳	گزارش‌دهی نقاط ضعف امنیت	**کنترل** تمامی کارکنان، پیمانکاران و کاربران ثالث سیستم‌ها و خدمات اطلاعاتی ملزم خواهند بود تا در صورت مشاهده یا ظنین شدن به هرگونه نقطه ضعف در سیستم‌ها یا خدمات اطلاعاتی مراتب را ثبت و گزارش نمایند.
الف-۱۳-۲ مدیریت حوادث و بهبودهای امنیت اطلاعات **هدف:** *حصول اطمینان از این که یک رویکرد مؤثر و استوار برای مدیریت حوادث امنیت اطلاعات مورد استفاده قرار گرفته است.*		
الف ۱-۲-۱۳	مسئولیت‌ها و روش‌های اجرایی	**کنترل** مسئولیت‌های مدیریتی و روش‌های اجرایی باید به‌گونه‌ای تعیین شوند که واکنش سریع، مؤثر و منظم به حوادث امنیت اطلاعاتی تضمین شود.
الف ۲-۲-۱۳	یادگیری از حوادث امنیت اطلاعات	**کنترل** برای اینکه نوع، حجم و هزینه‌های حوادث امنیتی قابل اندازه‌گیری و پایش باشند باید ساز و کارهای مناسبی وجود داشته باشد.
الف ۳-۲-۱۳	جمع‌آوری شواهد	**کنترل** در مواردی که انجام اقدامات پیگیری علیه یک فرد یا سازمان پس از بروز حادثه امنیت اطلاعاتی نیازمند اقدامات قانونی است (مدنی یا جزایی)، شواهد مربوطه در خصوص انطباق با قوانین باید جمع‌آوری، نگهداری و ارائه گردد.

A.14 Business continuity management		
A.14.1 Information security aspects of business continuity management **Objective**: *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.*		
A.14.1.1	Including information security in the business continuity management process	**Control** A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
A.14.1.2	Business continuity and risk assessment	**Control** Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	**Control** Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
A.14.1.4	Business continuity planning framework	**Control** A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
A.14.1.5	Testing, maintaining and reassessing business continuity plans	**Control** Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

الف-۱۴ مدیریت تداوم کسب و کار		
الف-۱۴-۱ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب وکار **هدف:** *خنثی کردن وقفه‌های وارد شده به فعالیت‌های کسب وکار و محافظت از فرآیندهای بحرانی کسب و کار در برابر اثرات ناشی از خرابی‌های عمده سیستم های اطلاعاتی یا بلایا و حصول اطمینان از احیای به‌موقع آن‌ها*		
الف ۱-۱-۱۴	لحاظ نمودن امنیت اطلاعات در فرآیند مدیریت تداوم کسب و کار	**کنترل** یک فرآیند مدیریتی در خصوص تداوم کسب و کار در کل سازمان باید ایجاد و حمایت شود که در آن به الزامات امنیت اطلاعات مورد نیاز برای تداوم کسب و کار سازمان اشاره شده باشد.
الف ۲-۱-۱۴	تداوم کسب و کار و ارزشیابی مخاطره	**کنترل** حوادثی که موجب بروز وقفه در فرآیندهای کسب و کار می‌شوند به‌همراه احتمال بروز و اثرگذاری چنین وقفه‌هایی و پیامدهای آن در امنیت اطلاعات باید شناسایی و تعیین شوند.
الف ۳-۱-۱۴	توسعه و اجرای طرح‌های تداوم با لحاظ نمودن امنیت اطلاعات	**کنترل** بعد از ایجاد وقفه و یا بروز خرابی در فرآیندهای کسب و کار، به منظور حفظ یا از سرگیری عملیات و اطمینان از در دسترس بودن اطلاعات در سطوح و بازه‌های زمانی قابل قبول باید طرح هایی ایجاد و پیاده‌سازی شوند.
الف ۴-۱-۱۴	چارچوب طرح ریزی تداوم کسب و کار	**کنترل** به‌منظور اطمینان از سازگاری همه طرح‌های تداوم کسب و کار باید یک چارچوب برای طرح‌ها ایجاد و به مورد اجرا گذاشته شود تا به طور پیوسته الزامات امنیت اطلاعات مورد توجه قرار گرفته و اولویت‌های آزمایش و نگهداری طرح‌ها نیز در آن تعیین شود.
الف ۵-۱-۱۴	آزمایش، نگهداری و ارزشیابی مجدد طرح‌های تداوم کسب و کار	**کنترل** طرح‌های تداوم کسب و کار باید به‌طور منظم آزمایش و بروزآوری شوند تا به این ترتیب از روزآمد بودن و اثربخش بودنشان اطمینان حاصل شود.

A.15 Compliance		
A.15.1 Compliance with legal requirements **Objective**: *To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.*		
A.15.1.1	**Identification of applicable legislation**	**Control** All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
A.15.1.2	**Intellectual property rights (IPR)**	**Control** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
A.15.1.3	**Protection of organizational records**	**Control** Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
A.15.1.4	**Data protection and privacy of personal information**	**Control** Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
A.15.1.5	**Prevention of misuse of information processing facilities**	**Control** Users shall be deterred from using information processing facilities for unauthorized purposes.

الف-۱۵ انطباق		
الف-۱۵-۱ انطباق با الزامات قانونی **هدف:** *جلوگیری از نقض هر نوع قانون، مقررات، تعهدات آیین نامه ای یا قراردادی و هر یک از الزامات امنیتی*		
الف ۱-۱-۱۵	**شناسایی قوانین قابل اجرا**	**کنترل** تمامی مقررات، تعهدات آیین‌نامه‌ای و قراردادی مرتبط و رویکرد سازمان جهت برآورد ساختن این الزامات باید به صراحت تعیین و مستند-سازی شده و نزد هر یک از سیستم‌های اطلاعاتی و سازمان به صورت روزآمد نگاهداری گردد.
الف ۲-۱-۱۵	**حقوق دارایی-های معنوی**	**کنترل** رویه‌های مناسب باید به‌گونه‌ای به مورد اجرا گذاشته شوند که از انطباق با الزامات قانون‌گذار، تعهدات آیین‌نامه‌ای و قراردادی مربوط به استفاده از محصولاتی که در رابطه با آن حقوق مالکیت معنوی متصور می‌باشد و محصولات نرم-افزاری با مالکیت انحصاری اطمینان حاصل شود.
الف ۳-۱-۱۵	**محافظت از سوابق سازمانی**	**کنترل** سوابق مهم باید مطابق با مقررات ، تعهدات آیین نامه‌ای و قراردادی والزامات کسب و کار، در برابر گم شدن، نابودی و تحریف محافظت شوند.
الف ۴-۱-۱۵	**حافظت از داده‌ها وعدم افشای اطلاعات شخصی**	**کنترل** حفاظت از داده‌ها و موضوع محرمانگی باید به-گونه‌ای که در مقررات و آیین نامه‌های مرتبط و برحسب مورد در بندهای قرارداد مقرر شده‌است تضمین شوند.
الف ۵-۱-۱۵	**جلوگیری از سوءاستفاده از امکانات پردازش اطلاعات**	**کنترل** باید از به‌کارگیری امکانات پردازش اطلاعات برای مقاصد غیرمجاز توسط کاربران، ممانعت شود.

A.15.1.6	**Regulation of cryptographic controls**	**Control** Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 Compliance with security policies and standards, and technical compliance **Objective:** *To ensure compliance of systems with organizational security policies and standards.*		
A.15.2.1	**Compliance with security policies and standards**	**Control** Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
A.15.2.2	**Technical compliance checking**	**Control** Information systems shall be regularly checked for compliance with security implementation standards.
A.15.3 Information systems audit considerations **Objective**: *To maximize the effectiveness of and to minimize interference to/from the information systems audit process.*		
A.15.3.1	**Information systems audit controls**	**Control** Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2	**Protection of information systems audit tools**	**Control** Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

الف ۱۵-۱-۶	**مقررات کنترل‌های رمزنگاری**	**کنترل** کنترل‌های رمزنگاری باید مطابق با قراردادها، قوانین و مقررات مربوطه مورداستفاده قرار گیرند.
الف-۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیت و انطباق فنی **هدف:** *حصول اطمینان از انطباق سیستم‌ها با استانداردها و خط‌مشی‌های امنیتی سازمان*		
الف ۱۵-۲-۱	**انطباق با استانداردها و خط‌مشی‌های امنیتی**	**کنترل** مدیران باید اطمینان حاصل نمایند که کلیه رویه‌های امنیتی در چارچوب حوزه مسئولیت‌شان، برای دستیابی به انطباق با خط‌مشی‌ها و استانداردهای امنیتی به‌درستی انجام شده است.
الف ۱۵-۲-۲	**کنترل انطباق فنی**	**کنترل** سیستم‌های اطلاعاتی از حیث انطباق با استاندارد‌های اجرایی امنیت باید به‌طور منظم بررسی شوند.
الف-۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی **هدف:** *افزایش اثربخشی و به حداقل رسانیدن تداخل در و یا ناشی از فرآیند ممیزی سیستم‌های اطلاعاتی*		
الف ۱۵-۳-۱	**کنترل‌های ممیزی سیستم‌های اطلاعاتی**	**کنترل** الزامات و فعالیت‌های ممیزی مرتبط با بررسی سیستم‌های عامل باید به دقت طرح‌ریزی شده و مورد توافق قرار گیرد تا مخاطره‌های ناشی از توقف در فرآیندهای کسب و کار کاهش یابد.
الف ۱۵-۳-۲	**محافظت از ابزارهای ممیزی سیستم‌های اطلاعاتی**	**کنترل** دسترسی به ابزارهای ممیزی سیستم‌های اطلاعاتی باید کنترل و محافظت شود تا از هرگونه سوءاستفاده یا مخاطرات احتمالی جلوگیری شود.

9. Annex B(Informative)

OECD principles and this International Standard

The principles given in the OECD Guidelines for the Security of Information Systems and Networks apply to all policy and operational levels that govern the security of information systems and networks. This International Standard provides an information security management system framework for implementing some of the OECD principles using the PDCA model and the processes described in Clauses 4, 5, 6 and 8, as indicated in Table B.1.

Table B.1 — OECD principles and the PDCA model

OECD principle	Corresponding ISMS process and PDCA phase
Awareness Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.	This activity is part of the Do phase (see 4.2.2 and 5.2.2).
Responsibility All participants are responsible for the security of information systems and networks.	This activity is part of the Do phase (see 4.2.2 and 5.1).
Response Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.	This is in part a monitoring activity Check phase (see 4.2.3 and 6 to 7.3) and a responding activity Act phase (See 4.2.4 and 8.1 to 8.3). This can also be covered by some aspects of the Plan and Check phases.

۹. پیوست ب(اطلاعاتی)

اصول OECD و استاندارد بین‌المللی حاضر

اصول مندرج در رهنمودهای OECD (سازمان همکاری و توسعه اقتصادی) مربوط به امنیت سیستم‌های اطلاعات و شبکه‌ها در مورد تمام خط‌مشی‌ها و سطوح عملیاتی حاکم بر امنیت سیستم‌های اطلاعاتی و شبکه‌ها قابل کاربرد می‌باشد. استاندارد بین‌المللی حاضر، با استفاده از مدل PDCA و فرآیندهای اشاره شده در بندهای ۴، ۵، ۶ و ۸ و به شرحی که در جدول ب۱ آمده است، چارچوب سیستم مدیریت امنیت اطلاعات را برای پیاده‌سازی برخی از اصول OECD فراهم آورده است.

جدول ب۱ – اصول OECD و مدل PDCA

اصول OECD	فرآیند سیستم مدیریت امنیت اطلاعات و فاز PDCA مشابه
آگاه‌سازی کلیه کارکنان ملزم خواهند بود نسبت به ضرورت امنیت سیستم-های اطلاعات و شبکه‌ها و آنچه که می‌توانند در جهت ارتقای امنیت انجام دهند، آگاهی و شناخت پیدا کنند.	این فعالیت بخشی از فاز Do (اجرا) می‌باشد. (به بندهای ۲-۲-۴ و ۲-۲-۵ نگاه کنید.)
مسئولیت کلیه کارکنان در قبال امنیت سیستم‌های اطلاعات و شبکه‌ها مسئول هستند.	این فعالیت بخشی از فاز Do (اجرا) می‌باشد. (به بندهای ۲-۲-۴ و ۱-۵ نگاه کنید.)
واکنش (پاسخ) کلیه کارکنان ملزم خواهند بود با عکس‌العمل به‌موقع و نشان دادن یک رفتار تعاملی ضمن جلوگیری از حوادث امنیتی، آن‌ها را شناسایی نموده و به آن‌ها واکنش مناسب نشان دهند.	این فعالیت تا حدودی یک فعالیت پایشی از فاز Check (بررسی) (به بندهای ۳-۲-۴ و ۶ تا ۳-۷ نگاه کنید) و یک فعالیت واکنشی از فاز Act (اقدام) می‌باشد. (به بندهای ۴-۲-۴ و ۱-۸تا ۳-۸ نگاه کنید). این آیتم به وسیله برخی از جوانب فازهای طرح‌ریزی و بررسی پوشش داده می‌شود.

Risk assessment Participants should conduct risk assessments.	This activity is part of the Plan phase (see 4.2.1) and risk reassessment is part of the Check phase (see 4.2.3 and 6 to 7.3).
Security design and implementation Participants should incorporate security as an essential element of information systems and networks.	Once a risk assessment has been completed, controls are selected for the treatment of risks as part of the Plan phase (see 4.2.1). The Do phase (see 4.2.2 and 5.2) then covers the implementation and operational use of these controls.
Security management Participants should adopt a comprehensive approach to security management.	The management of risk is a process which includes the prevention, detection and response to incidents, ongoing maintenance, review and audit. All of these aspects are encompassed in the Plan, Do, Check and Act phases.
Reassessment Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.	Reassessment of information security is a part of the Check phase (see 4.2.3 and 6 to 7.3) where regular reviews should be undertaken to check the effectiveness of the information security management system, and improving the security is part of the Act phase (see 4.2.4 and 8.1 to 8.3).

ارزشیابی مخاطره کلیه کارکنان ملزم خواهند بود ارزشیابی مخاطره را هدایت کنند.	این فعالیت بخشی از فاز Plan (طرح‌ریزی) (به بند ۱-۲-۴ نگاه کنید) و ارزشیابی مجدد مخاطره بخشی از فاز Check (بررسی) (به بندهای ۳-۲-۴ و ۶ تا ۳-۷ نگاه کنید) است.
طراحی و اجرای امنیت کلیه کارکنان ملزم خواهند بود تا موضوع امنیت را به عنوان مؤلفه و جزء اساسی سیستم‌های اطلاعاتی و شبکه‌ها مورد توجه قرار دهند.	پس از آن که ارزشیابی مخاطره تکمیل می‌شود، اقدامات کنترلی برای مقابله با مخاطره‌ها به عنوان فاز طرح‌ریزی انتخاب می‌شوند (به بند ۲-۱-۴ نگاه کنید). سپس فاز Do (اجرا) شروع می‌شود که شامل اجرا و استفاده عملی از این اقدامات کنترلی می‌باشد (به بندهای ۲-۲-۴ و ۲-۵ نگاه کنید).
مدیریت امنیت کلیه کارکنان ملزم خواهند بود تا در رابطه با مدیریت امنیت، رویکرد جامعی را انتخاب و اتخاذ نمایند.	مدیریت مخاطره، فرآیندی است که پیشگیری، آشکارسازی و واکنش به حوادث، نگهداری مستمر، بازنگری و ممیزی را شامل می‌شود. تمامی این جوانب در فازهای Plan، Do، Check و Act لحاظ شده است.
ارزشیابی مجدد کلیه کارکنان ملزم خواهند بود تا امنیت سیستم‌های اطلاعاتی و شبکه‌ها را مورد بازنگری و ارزشیابی مجدد قرار دهند و اصلاحات لازم را در سیاست‌ها و خط مشی‌های امنیت، روش‌ها، معیارها و رویه‌ها اعمال نمایند	ارزشیابی دوباره امنیت اطلاعات بخشی از فاز Check می‌باشد (به بندهای ۳-۲-۴ و ۶ تا ۳-۷ نگاه کنید) که طی آن بازنگری‌های منظم باید به منظور کنترل اثربخشی سیستم مدیریت امنیت اطلاعات انجام شود و بهبود امنیت نیز بخشی از فاز Act به شمار می‌رود. (به بندهای ۴-۲-۴ و ۸ تا ۳-۸ نگاه کنید).

10. Annex C(Informative)

Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

Table C.1 shows the correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard.

Table C.1 — Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

This International Standard	ISO 9001:2000	ISO 14001:2004
0 Introduction 0.1 General 0.2 Process approach 0.3 Compatibility with other management systems	0 Introduction 0.1 General 0.2 Process approach 0.3 Relationship with ISO 9004 0.4 Compatibility with other management systems	Introduction
1 Scope 1.1 General 1.2 Application	1 Scope 1.1. General 1.2. Application	1 Scope
2 Normative references	2 Normative reference	2 Normative reference
3 Terms and definitions	3 Terms and definitions	3 Terms and definitions
4 Information security management system 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS	4 Quality management system 4.1 General requirements	4 EMS requirements 4.1 General requirements 4.4 Implementation and operation

۱۰. پیوست پ(اطلاعاتی)

شباهت بین ISO 9001:2000 ، ISO 14001:2004 و استاندارد بین المللی حاضر

جدول پ۱، شباهت بین ISO 9001:2000 ، ISO 14001:2004 و استاندارد بین المللی حاضر را نشان می‌دهد.

استاندارد بین المللی حاضر	ISO 9001:2000	ISO 14001:2004
۰ مقدمه ۰. ۱ کلیات ۰. ۲ رویکرد فرآیند ۰. ۳ سازگاری با سایر سیستم-های مدیریت	۰ مقدمه ۰. ۱ کلیات ۰. ۲ رویکرد فرآیند ۰. ۳ ارتباط با ISO 9004 ۰. ۴ سازگاری با سایر سیستم‌های مدیریت	مقدمه
۱ دامنه کاربرد ۱. ۱ کلیات ۱. ۲ کاربرد	۱ دامنه کاربرد ۱. ۱ کلیات ۱. ۲ کاربرد	۱ دامنه کاربرد
۲ مراجع عادی	۲ مراجع عادی	۲ مراجع عادی
۳ شرایط و ضوابط	۳ شرایط و ضوابط	۳ شرایط و ضوابط
۴ سیستم مدیریت امنیت اطلاعات ۴. ۱ الزامات کلی ۴. ۲ ایجاد و مدیریت سیستم مدیریت امنیت اطلاعات ۴. ۲. ۱ ایجاد سیستم مدیریت امنیت اطلاعات	۴ سیستم مدیریت امنیت اطلاعات ۴. ۱ الزامات کلی	۴ الزامات EMS ۴. ۱ الزامات کلی ۴. ۴ اجرا و بهره‌برداری

4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS 4.2.4 Maintain and improve the ISMS	8.2.3 Monitoring and measurement of 8.2.4 Monitoring and measurement of product	4.5.1 Monitoring and measurement
4.3 Documentation requirements 4.3.1 General 4.3.2 Control of documents 4.3.3 Control of records	4.2 Documentation requirements 4.2.1 General 4.2.2 Quality manual 4.2.3 Control of documents 4.2.4 Control of records	4.4.5 Documentation control 4.5.4 Control of records
5 Management responsibility 5.1 Management commitment	5 Management responsibility 5.1 Management commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	4.2 Environmental policy 4.3 Planning
5.2 Resource management 5.2.1 Provision of resources 5.2.2 Training, awareness and competence	6 Resource management 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, awareness and training 6.3 Infrastructure 6.4 Work environment	4.4.2 Competence, training, and awareness

۴.۲.۲ اجرا و بهره‌برداری از سیستم مدیریت امنیت اطلاعات ۴.۲.۳ پایش و بازنگری سیستم مدیریت امنیت اطلاعات ۴.۲.۴ نگهداری و بهبود سیستم مدیریت امنیت اطلاعات	۸.۲.۳ پایش و اندازه‌گیری فرآیندها ۸.۲.۴ پایش و اندازه‌گیری محصول	۴.۵.۱ پایش و اندازه‌گیری
۴.۳ الزامات مستندات ۴.۳.۱ کلیات ۴.۳.۲ کنترل مدارک ۴.۳.۳ کنترل سوابق	۴.۲ الزامات مستندات ۴.۲.۱ کلیات ۴.۲.۲ دستورالعمل کیفیت ۴.۲.۳ کنترل مدارک ۴.۲.۴ کنترل سوابق	۴.۴.۵ کنترل مستندات ۴.۵.۴ کنترل سوابق
۵ مسئولیت مدیریت ۵.۱ تعهد مدیریت	۵ مسئولیت مدیریت ۵.۱ تعهد مدیریت ۵.۲ کانون مشتری ۵.۳ خط‌مشی کیفیت ۵.۴ برنامه‌ریزی ۵.۵ مسئولیت، اختیارات و ارتباطات	۴.۲ خط‌مشی زیست محیطی ۴.۳ برنامه‌ریزی
۵.۲ مدیریت منابع ۵.۲.۱ تامین منابع ۵.۲.۲ آموزش، آگاه‌سازی و صلاحیت	۶ مدیریت منابع ۶.۱ تامین منابع ۶.۲ منابع انسانی ۶.۲.۲ صلاحیت، آگاه‌سازی و آموزش ۶.۳ زیرساختار ۶.۴ محیط کار	۴.۴.۲ صلاحیت، آگاه‌سازی و آموزش

6 Internal ISMS audits	8.2.2 Internal Audit	4.5.5 Internal audit
7 Management review of the ISMS 7.1 General 7.2 Review input 7.3 Review output	5.6 Management review 5.6.1 General 5.6.2 Review input 5.6.3 Review output	4.6 Management review
8 ISMS improvement 8.1 Continual improvement	8.5 Improvement 8.5.1 Continual improvement	
8.2 Corrective action	8.5.3 Corrective actions	4.5.3 Non-conformity, corrective action and preventive action
8.3 Preventive action	8.5.3 Preventive actions	
Annex A Control objectives and Controls **Annex B OECD principles and this International Standard** **Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard**	**Annex A Correspondence between ISO 9001:2000 and ISO 14001:1996**	**Annex A Guidance on the use of this International Standard** **Annex B Correspondence between ISO 14001:2004 and ISO 9001:2000**

۶ ممیزی های داخلی سیستم مدیریت امنیت اطلاعات	۸. ۲. ۲ ممیزی های داخلی	۴. ۵. ۵ ممیزی های داخلی
۷ بازنگری سیستم مدیریت امنیت اطلاعات توسط مدیریت ۷. ۱ کلیات ۷. ۲ بازنگری ورودی ۷. ۳ بازنگری خروجی	۵. ۶ بازنگری مدیریت ۵. ۶. ۱ کلیات ۵. ۶. ۲ بازنگری ورودی ۵. ۶. ۳ بازنگری خروجی	۴. ۶ بازنگری مدیریت
۸ ممیزی های داخلی سیستم مدیریت امنیت اطلاعات ۸،۱ بهبود سیستم مدیریت امنیت اطلاعات	۸،۵ بهبود ۸،۵،۱ بهبود سیستم مدیریت امنیت اطلاعات	
۸. ۲ اقدامات اصلاحی	۸. ۵. ۳ اقدامات اصلاحی	۴. ۵. ۳ عدم انطباق، اقدامات اصلاحی و اقدامات پیشگیرانه
۸. ۳ اقدامات پیشگیرانه	۸. ۵. ۳ اقدامات اصلاحی	
پیوست الف : اهداف کنترل و اقدامات کنترلی پیوست ب :اصول OECD و استاندارد بین‌المللی حاضر پیوست پ : شباهت بین ISO 9001:2000، ISO 14001:2004و استاندارد بین‌المللی حاضر	پیوست الف : شباهت بین ISO 9001:2000، ISO 14001:2004	پیوست الف :راهنمایی درباره استفاده از استاندارد بین‌المللی حاضر پیوست ب: شباهت بین ISO 9001:2000 – ISO 14001:2004

Bibliography

Standards publications

[1] ISO 9001:2000, Quality management systems — Requirements

[2] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[3] ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security

[4] ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards

[5] ISO 14001:2004, Environmental management systems — Requirements with guidance for use

[6] ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management

[7] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[8] ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems

[9] ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards

Other publications

[1] OECD, Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[2] NIST SP 800-30, Risk Management Guide for Information Technology Systems

[3] Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986