INSO
12047
1st.Revision
2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
۱۲۰۴۷
تجدید نظر اول
۱۳۹۵

# فناوری اطلاعات –

# حاکمیت فناوری اطلاعات (IT) برای سازمان

# Information technology — Governance of IT for the organization

ICS: 35.080

**سازمان ملی استاندارد ایران**

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

**Iranian National Standardization Organization (INSO)**

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

**به نام خدا**

## آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها واسط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و الزامات خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

## کمیسیون فنی تدوین استاندارد
## «فناوری اطلاعات – حاکمیت فناوری اطلاعات (IT) برای سازمان»
## «تجدیدنظر اول»

| **رئیس:** | **سمت و/ یا محل اشتغال:** |
|---|---|
| ایزدپناه، سحرالسادات<br>(فوق لیسانس مهندسی فناوری اطلاعات) | رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران |
| **دبیر:** | |
| میر اسکندری، سید محمدرضا<br>(لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی) | مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات |
| **اعضاء:** (اسامی به ترتیب حروف الفبا) | |
| ناظمی، اسلام<br>(دکترای مهندسی کامپیوتر) | استادیار دانشگاه شهید بهشتی |
| نصیری آسایش، حمید رضا<br>(کارشناسی ارشد فناوری اطلاعات معماری سازمانی) | پژوهش‌گر دانشگاه شهید بهشتی |
| یعقوبی رفیع، کمال الدین<br>(کارشناسی ارشد فناوری اطلاعات معماری سازمانی) | پژوهش‌گر دانشگاه شهید بهشتی |
| دوست‌محمدی، وحید<br>(کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات) | کارشناس مرکز مدیریت راهبردی افتا |
| محمدیان، بهزاد<br>(فوق لیسانس مهندسی برق) | کارشناس مرکز مدیریت راهبردی افتا |
| ابوالقاسمی، پیمان<br>(کارشناسی ارشد مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |
| ارجمند، مهدی<br>(کارشناسی ارشد مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |
| رادمهر، وحید<br>(کارشناسی مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |

جوادزاده، غزاله

(کارشناسی ارشد مهندسی کامپیوتر)

پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

مغانی،مهدی

(فوق لیسانس ریاضی کاربردی)

کارشناس تدوین استانداردهای حوزه فناوری اطلاعات
سازمان فناوری اطلاعات ایران

**ویراستار:**

قسمتی، سیمین

(کارشناسی ارشد مهندسی فناوری اطلاعات)

مشاور مرکز آپا دانشگاه تربیت مدرس

## فهرست مندرجات

**عنوان** **صفحه**


آشنایی با سازمان ملی استاندارد ایران ج
کمیسیون فنی تدوین استاندارد د
پیش‌گفتار ز
مقدمه ح
۱ هدف و دامنهٔ کاربرد ۱
۲ اصطلاحات و تعاریف ۲
۳ منافع حاکمیت خوب فناوری اطلاعات ۸
۴ اصول و مدل حاکمیت خوب فناوری اطلاعات ۹
۴-۱ اصول ۹
۴-۲ مدل ۱۰
۵ راهنمایی برای حاکمیت فناوری اطلاعات ۱۲
۵-۱ عمومی ۱۲
۵-۲ اصل ۱: مسئولیت ۱۲
۵-۳ اصل ۲: راهبرد ۱۳
۵-۴ اصل ۳: اکتساب ۱۴
۵-۵ اصل ۴: عملکرد ۱۵
۵-۶ اصل ۵: انطباق ۱۵
۵-۷ اصل ۶: رفتار انسانی ۱۶
کتاب‌نامه ۱۸

## پیش‌گفتار

استاندارد «فناوری اطلاعات – حاکمیت فناوری اطلاعات (IT) برای سازمان» اولین بار در سال ۱۳۸۸ تدوین شد. این استاندارد بر اساس پیشنهادهای رسیده و بررسی توسط سازمان فناوری اطلاعات ایران و تایید در کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در چهارصد و بیست و هشتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۰۳/۰۵ تصویب شد، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ۱۲۰۴۷: سال ۱۳۸۸ است.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به توصیف زیر است:

ISO/IEC 38500:2015, Information technology — Governance of IT for the organization

**مقدمه**

هدف از این استاندارد ملی ارائه اصول، تعاریف، و یک مدل به نهادهای حاکمیتی برای استفاده هنگام ارزشیابی، هدایت و پایشِ کاربرد فناوری اطلاعات (IT) در سازمان‌های خود است.

این استاندارد ملی، استاندارد مشاوره‌ایِ سطح بالا و اصول‌گرا است. علاوه بر ارائه راهنماییِ گسترده در نقش نهاد حاکمیتی، سازمان‌ها را به استفاده از استانداردهای مناسب برای پی‌ریزی کردن حاکمیت IT تشویق می‌کند.

بسیاری از سازمان ها از IT به عنوان ابزار اساسی کسب و کار استفاده می‌کنند و تعداد کمی از آن‌ها بدون آن می تواند کارکرد موثر داشته باشد. همچنین IT یک عامل مهم در طرح‌های کسب و کار آیندهٔ بسیاری از سازمان‌ها است.

هزینه IT می‌تواند بخش قابل توجهی از هزینه‌های مالی و منابع انسانی سازمان را نشان دهد. با این حال، بازگشت این سرمایه گذاری اغلب به طور کامل محقق نمی‌شود و تاثیرات نامطلوب بر سازمان می تواند قابل توجه باشد.

از دلایل اصلی این نتایج منفی، تاکید بر جنبه‌های فنی، مالی و زمان‌بندیِ فعالیت‌های IT به جای تاکید بر زمینهٔ کسب و کار استفاده از IT است.

این استاندارد ملی اصول، تعاریف و مدل برای حاکمیت خوب IT ارائه می‌کند تا در بالاترین سطح سازمان‌ها به فهم و انجام تعهدات قانونی، مقرراتی و اخلاقی در رابطه با استفاده سازمان‌های خود از فناوری اطلاعات کمک کند.

این استاندارد ملی با تعریف حاکمیت شرکتی که به عنوان یک گزارش کمیته‌ی جنبه‌های مالی حاکمیت شرکتی (گزارش Cadbury) در سال۱۹۹۲ منتشر شده است، همسو است. گزارش Cadbury همچنین تعریف پایه‌ای از حاکمیت شرکتی در اصول OECD از حاکمیت شرکتی در سال ۱۹۹۲ ارائه کرده است (تجدیدنظر در سال ۲۰۰۴). حاکمیت متمایز از مدیریت است، و برای اجتناب از سردرگمی، دو مفهوم در این استاندارد تعریف شده و در استاندارد ISO/IEC TR 38502 به آن پرداخته شده است.

این استاندارد ملی در درجه اول به نهاد حاکمیتی می‌پردازد. در برخی از سازمان‌ها (نوعا کوچکتر)، اعضای نهاد حاکمیتی همچنین می‌توانند مدیران اجرایی باشند. این استاندارد ملی برای تمامی سازمان‌ها، از کوچکترین تا بزرگترین آن‌ها و بدون در نظر گرفتن هدف، طراحی و ساختار مالکیتشان، کاربست‌پذیر است.

پیاده‌سازی حاکمیت IT توسط مشخصات فنی ISO/IEC TS 38501 پوشش داده شده است.

# فناوری اطلاعات – حاکمیت فناوری اطلاعات (IT) برای سازمان

## ۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین اصول راهنما برای اعضای نهادهای حاکمیتی (می‌تواند شامل صاحبان، مدیران ارشد[1]، شرکا، مدیران اجرایی[2] یا موارد مشابه باشد) به‌منظور استفاده مؤثر، کارا و قابل‌قبول از فناوری اطلاعات در سازمان‌های خود است.

همچنین این استاندارد، راهنمایی‌هایی را برای افرادی که به نهادهای حاکمیتی مشاوره، آگاهی یا کمک ارائه می‌دهند، فراهم می‌کند. این افراد شامل موارد زیر می‌شوند:

- مدیران اجرایی؛
- اعضای گروه‌هایی که منابع را درون سازمان پایش[3] می‌کنند؛
- متخصصان بیرونی فنی و کسب‌وکار، مثل متخصصان حقوقی یا حسابداری، انجمن‌های صنفی یا صنعتی یا نهادهای حرفه‌ای؛
- تامین‌کنندگان درونی و بیرونی خدمت (شامل مشاوران)؛
- ممیزان[4].

این استاندارد ملی برای حاکمیت استفاده جاری و آتی فناوری اطلاعات سازمان‌ها، شامل: فرایندهای مدیریتی و تصمیمات مربوط به استفاده جاری و آتی از فناوری اطلاعات، کاربرد دارد. این فرایندها می‌توانند توسط متخصصان فناوری اطلاعات درون سازمان، تامین‌کنندگان بیرونی خدمات یا واحدهای کسب‌وکار درون سازمان واپایش[5] (کنترل) شود.

این استاندارد ملی، حاکمیت فناوری اطلاعات را به‌عنوان زیرمجموعه یا دامنه‌ای از حاکمیت سازمانی تعریف می‌کند، یا در مورد یک شرکت، به‌عنوان زیرمجموعه یا دامنه‌ای از حاکمیت شرکتی تعریف می‌کند.

این استاندارد ملی در تمام سازمان‌ها شامل شرکت‌های عمومی و خصوصی، نهادهای دولتی یا سازمان‌های غیرانتفاعی کاربردپذیر است. این استاندارد ملی در سازمان‌هایی با هراندازه از کوچک‌ترین تا بزرگ‌ترین، صرف‌نظر از وسعت استفاده آن‌ها از فناوری اطلاعات کاربردپذیر است.

هدف این استاندارد ملی، ارتقای استفاده مؤثر، کارا و قابل‌قبول[6] فناوری اطلاعات در تمام سازمان‌ها از طریق موارد زیر است:

- اطمینان‌بخشی به ذی‌نفعان از این جهت که اگر از اصول و شیوه‌های پیشنهاد شده در این استاندارد

1- Directors
2- Executive manager
3- Monitor
4- Auditors
5- Control
6- Acceptable

پیروی شود، می‌توانند از حاکمیت فناوری اطلاعات سازمان اطمینان داشته باشند.

- آگاهی دادن و راهنمایی کردن نهادهای حاکمیتی در حاکمیت استفاده از فناوری اطلاعات در سازمان‌های خود و
- برقراری درک واژگانی[1] برای حاکمیت فناوری اطلاعات.

**مراجع الزامی**

این استاندارد مراجع الزامی ندارد.

## ۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

**۲-۱**

**قابل‌قبول[2]**

انتظارات ذی‌نفع را برآورده می‌سازد یعنی قابلیت نمایش به‌عنوان یک موضوع معقول یا شایسته[3] را دارد.

**۲-۲**

**پاسخگو[4]**

جواب‌گو بودن برای کنش‌ها، تصمیمات و عملکرد است.

**۲-۳**

**پاسخگویی[5]**

حالت پاسخگو بودن است.

**یادآوری ۱**- پاسخگویی مربوط به یک مسئولیت تخصیص داده شده است. مسئولیت ممکن است بر مبنای مقررات یا توافق‌نامه یا از طریق انتسابی به‌عنوان بخشی از واگذاری اختیارات باشد.

1- Vocabulary
2- Acceptable
3- Merited
4- Accountable
5- Accountability

**۴-۲**

**حاکمیت شرکتی**[1]

سامانه‌ای که به‌وسیله آن، شرکت‌ها هدایت و واپایش می‌شوند.

**یادآوری ۱**- حاکمیت شرکتی، حاکمیت سازمانی است که در شرکت‌ها کاربرد دارد.

**یادآوری ۲**- از ۱۹۹۲ Cadbury و ۱۹۹۹ OECD برگرفته شده است.

**یادآوری ۳**- این تعریف به این منظور آورده شده است تا تکاملِ اصطلاح‌شناسی را نسبت به ویرایش پیشین شفاف سازد.

**۵-۲**

**هدایت**[2]

تبیین اهداف و دستاوردهای مطلوب است.

**یادآوری ۱**- هدایت درزمینه حاکمیت فناوری اطلاعات، شامل تنظیم اهداف، راهبردها و خط‌مشی‌های پذیرفته‌شده توسط اعضای سازمان است تا از استفاده فناوری اطلاعات برای نیل به اهداف کسب‌وکار اطمینان حاصل شود.

**یادآوری ۲**- اهداف، راهبردها و خط‌مشی‌ها می‌توانند توسط مدیران تنظیم شوند به شرطی که از طرف نهاد حاکمیتی دارای اختیار باشند.

**۶-۲**

**ارزشیابی کردن**[3]

ملاحظه و قضاوت‌های آگاهانه است.

**یادآوری ۱**- در زمینه حاکمیت فناوری اطلاعات، ارزشیابی شامل قضاوت‌هایی راجع به شرایط و فرصت‌های درونی یا بیرونی و جاری و آتی است که مربوط به استفاده جاری و آتی سازمان از فناوری اطلاعات است.

**۷-۲**

**مدیر اجرایی**

کسی که از طرف نهاد حاکمیتی سازمان صاحب اختیارات برای پیاده‌سازی راهبردها و خط‌مشی‌ها در جهت نیل به هدف سازمان است.

**یادآوری۱**- مدیریت اجرایی می‌تواند شامل نقش‌هایی باشد که به نهاد حاکمیتی سازمان یا بالاترین مقام سازمان گزارش دهد و یا به‌طور کلی دارای مسئولیت پاسخگویی برای کارکرد گزارش دهی عمده باشد، به‌عنوان مثال، مدیران ارشد اجرایی (CEOs)[4]، سران سازمان‌های دولتی، مقامات ارشد مالی (CFOs)[1]، مدیران ارشد عملیاتی (COOs)[2]، مدیران ارشد اطلاعات

1- Corporate governance
2- Direct
3- Evaluate
4- Chief Executive Officers

(CIOs)[3] و وظایف مشابه.

**یادآوری ۲**- در استانداردهای مدیریت، مدیران اجرایی می‌توانند بالاترین رتبه مدیریت باشند.

**۸-۲**

**حاکمیت [4]**

سامانه هدایت و واپایش است.

**۹-۲**

**نهاد حاکمیتی[5]**

شخص یا گروهی که پاسخگوی عملکرد و انطباق سازمان هستند.

**۱۰-۲**

**حاکمیت فناوری اطلاعات [6]**

سامانه‌ای که استفاده جاری و آتی از فناوری اطلاعات را هدایت و واپایش می‌کند.

**یادآوری ۱**- حاکمیت فناوری اطلاعات یک جز یا زیرمجموعه‌ای از حاکمیت سازمان است.

**یادآوری ۲**- اصطلاح حاکمیت فناوری اطلاعات معادل با اصطلاح حاکمیت شرکتی فناوری اطلاعات، حاکمیت بنگاهی فناوری اطلاعات و حاکمیت سازمانی فناوری اطلاعات است.

**۱۱-۲**

**رفتار انسانی [7]**

تعامل بین انسان‌ها و سایر عناصر سامانه است.

**یادآوری ۱**- رفتار انسانی شامل فرهنگ، نیازها و تمایلات افراد به‌صورت فردی یا گروهی است.

**یادآوری ۲**- از دیدگاه فناوری اطلاعات، تعداد زیادی گروه یا جوامع انسانی با نیازها، آرزوها و رفتارهای خاص خودشان وجود دارد. به‌عنوان مثال افرادی که از سامانه‌های اطلاعاتی استفاده می‌کنند شاید نیازهای مربوط به دسترسی‌پذیری و ارگونومی و همچنین دردسترس‌بودن و عملکرد را نشان دهند. افرادی که نقش‌های شغلی آن‌ها به دلیل استفاده از فناوری اطلاعات تغییر می‌کند ممکن است نیازهای مربوط به ارتباطات، آموزش و تضمین مجدد[8] را داشته باشند. افرادی که درگیر پیاده‌سازی و

---

1- Chief Financial Officers
2- Chief Operating Officers
3- Chief Information Officers
4- Governance
5- Governing body
6- Governance of IT
7- Human behaviour
1- Reassurance

اجرای قابلیت فناوری اطلاعات هستند، ممکن است نیازهای مربوط به شرایط کاری و توسعه مهارت‌ها را داشته باشند.

**۱۲-۲**

**فناوری اطلاعات (IT)** [۱]

منابعی که برای اکتساب، پردازش، ذخیره‌سازی و انتشار اطلاعات استفاده می‌شوند.

**یادآوری ۱-** همچنین این اصطلاح شامل «فناوری ارتباطات (CT)[۲]» و اصطلاح مرکب «فناوری ارتباطات و اطلاعات (ICT)[۳]» است.

**۱۳-۲**

**سرمایه‌گذاری** [۴]

تخصیص منابع برای دستیابی به اهداف و سایر منافع تعریف‌شده است.

**۱۴-۲**

**مدیریت**[۵]

اعمال واپایش و نظارت با داشتن اختیار و پاسخگویی که توسط حاکمیت برقرار می‌شود.

**یادآوری ۱-** واژه مدیریت اغلب به‌عنوان اصطلاح جمعی برای کسانی به کار می‌رود که مسئولیت واپایش سازمان یا بخشی از سازمان را دارند. واژه مدیر برای پرهیز از اشتباه گرفتن با سامانه‌های مدیریت استفاده می‌شود.

**۱۵-۲**

**مدیران** [۶]

گروهی از افراد که مسئولیت واپایش و نظارت سازمان یا بخشی از آن را دارد.

**یادآوری ۱-** مدیران اجرایی رده‌ای از مدیران هستند.

**۱۶-۲**

**پایش**

بازنگری به‌عنوان مبنایی برای تصمیمات و تنظیمات مناسب است.

---

2- Information Technology
3- Communications Technology
4- Information and communications technology
5- Investment
6- Management
7- Managers

**یادآوری ۱**- پایش شامل دستیابی روزمره به اطلاعاتی در مورد پیشرفت حاصل شده در مقایسه با طرح‌ها همچنین بررسی‌های ادواری دستاوردهای کلی در مقایسه با نتایج و راهبردهای توافق شده است تا مبنایی برای تصمیم‌گیری و تنظیمات فراهم آورد.

**یادآوری ۲**- پایش شامل بررسی انطباق با قانون[1]، مقررات و خط‌مشی‌های سازمانی مرتبط است.

**۲-۱۷**

**سازمان[2]**

شخص یا گروهی از اشخاص که دارای کارکردهایی با مسئولیت، اختیارات و رابطه‌ها برای دستیابی به اهداف خود هستند.

**یادآوری ۱**- مفهوم سازمان شامل این موارد است: تک‌فروش[3]، شرکت، سهامی، دفتر شراکتی[4]، بنگاه، مراجع دارای اختیار، شراکت، بنگاه نیکوکاری، موسسه، قسمت یا ترکیبی از همهٔ آن‌ها چه ثبت شده باشد و چه عمومی یا خصوصی باشد، اما محدود به آن‌ها نمی‌شود.

[منبع:
Consolidated ISO Supplement 2013-Procedures specific to ISO, Annex XL, Appendix 2.
یادآوری به این استاندارد اضافه شده است.]

**۲-۱۸**

**حاکمیت سازمانی[5]**

سامانه‌ای که توسط آن، سازمان‌ها هدایت و واپایش می‌شوند.

**۲-۱۹**

**خط‌مشی[6]**

تمایلات و جهت‌گیری یک سازمان که توسط نهاد حاکمیتی سازمان یا مدیران اجرایی آن که دارای اختیارات مناسب هستند، به‌طور رسمی بیان می‌شود.

1- Legislation
2- Organization
3- Sole-trader
4- Firm
5- Organizational governance
6- Policy

**۲-۲۰**

**پیشنهاد**[1]

مجموعه منافع، هزینه‌ها، مخاطره‌ها، فرصت‌ها و سایر عوامل که برای تصمیم‌گیری کاربردپذیر است.

**مثال:** موارد کسب‌وکار

**۲-۲۱**

**منابع** [2]

مردم، روش‌های اجرایی، نرم‌افزار، اطلاعات، تجهیزات، مواد مصرفی، زیرساخت، وجوه سرمایه‌ای و عملیاتی و زمان است.

**۲-۲۲**

**مسئولیت** [3]

التزام به عمل و تصمیم‌گیری برای دستیابی به دستاوردهای مورد نیاز است.

**۲-۲۳**

**مخاطره** [4]

تأثیر عدم قطعیت بر اهداف است.

**یادآوری ۱**- یک تأثیر، انحرافی از انتظارات است – مثبت یا منفی

**یادآوری ۲**- تأثیرات منفی تهدیدها را بازتاب می‌دهند درحالی‌که مخاطره‌های مثبت فرصت‌ها را بازتاب می‌کنند.

[منبع: راهنمای ISO Guide 73:2009]

**۲-۲۴**

**ذی‌نفع** [5]

هر شخص، گروه یا سازمان که بتواند تأثیر گذارد، تأثیر بپذیرد یا دارای این درک باشد که از یک عمل یا تصمیم تاثیر می‌پذیرد.

[منبع: اقتباس از راهنمای ISO Guide 73:2009]

1- Proposal
2- Resources
3- Responsibility
4- Risk
5- Stakeholder

**۲۵-۲**

**استفاده از فناوری اطلاعات**[1]

طرح‌ریزی، طراحی، توسعه، استقرار، بهره‌برداری، مدیریت و کاربست فناوری اطلاعات برای نیل به اهداف کسب‌وکار و ارزش‌آوری برای سازمان است.

**یادآوری ۱**- استفاده از فناوری اطلاعات هم شامل تقاضا و هم عرضه فناوری اطلاعات است.

**یادآوری ۲**- استفاده از فناوری اطلاعات شامل استفاده جاری و آتی از آن است.

## ۳ منافع حاکمیت خوب فناوری اطلاعات

حاکمیت خوب فناوری اطلاعات به نهاد حاکمیتی سازمان کمک می‌کند تا اطمینان حاصل کند که استفاده از فناوری اطلاعات مشارکت مثبتی در عملکرد سازمان دارد. این مشارکت از طرق زیر است:

- نوآوری در خدمات، بازارها و کسب‌وکار
- هم‌سویی فناوری اطلاعات با نیازهای کسب‌وکار
- پیاده‌سازی و بهره‌برداری مناسب دارایی‌های فناوری اطلاعات
- شفافیت مسئولیت و پاسخگویی هم برای تأمین و هم برای تقاضای فناوری اطلاعات در دستیابی به اهداف سازمان
- تداوم و پایداری کسب‌وکار
- تخصیص کارای منابع
- اقدامات خوب در برقراری ارتباط با ذی‌نفعان و
- تحقق واقعی منافع مورد انتظار از هر سرمایه‌گذاری فناوری اطلاعات

این استاندارد ملی اصولی را برای استفاده مؤثر، کارا و قابل‌قبول از فناوری اطلاعات فراهم می‌کند.

نهادهای حاکمیتی از طریق حصول اطمینان از تبعیت سازمانشان از این اصول، در مدیریت مخاطره‌ها و تقویت بهره‌برداری از فرصت‌های به وجود آمده ناشی از استفاده از فناوری اطلاعات، کمک می‌شوند.

همچنین حاکمیت خوب فناوری اطلاعات به نهاد حاکمیتی سازمان در حصول اطمینان از تبعیت با التزامات (مقرراتی، قانونی[2] و قراردادی) درباره استفاده قابل‌قبول از فناوری اطلاعات کمک می‌کند. این استاندارد ملی مدلی برای حاکمیت فناوری اطلاعات را بنا نهاده است. مخاطره نهادهای حاکمیتی در مورد عدم رعایت الزامات از طریق توجه به این مدل در کاربست مناسب این اصول کاهش پیدا می‌کند.

سامانه‌های فناوری اطلاعات ناکافی و استفاده نامناسب از فناوری اطلاعات می‌تواند سازمان را با مخاطره برآورده نشدن التزامات قانونی مواجه کند. به‌عنوان مثال، در برخی حوزه‌های قضایی[3]، اگر سامانه حسابداری

1- Use of IT
2- Legislation
3- Jurisdictions

ناکافی باعث پرداخت نشدن مالیات شود، اعضای نهاد حاکمیتی سازمان می‌توانند شخصاً پاسخگو باشند.
فرایندهای مرتبط با فناوری اطلاعات با مخاطره‌های معینی همراه است که توصیه می‌شود به‌درستی به آن‌ها پرداخته شود. به‌عنوان مثال: نهاد حاکمیتی سازمان و اعضای آن می‌توانند در موارد زیر پاسخگو باشند:

- قوانین و مقررات نقض حریم خصوصی، هرزنامه، بهداشت و ایمنی، ثبت سوابق
- عدم انطباق با استانداردهای مربوط به امنیت و مسئولیت اجتماعی
- موضوعات مربوط به حقوق مالکیت معنوی شامل توافق حق استفاده

نهاد حاکمیتی که از راهنمای این استاندارد استفاده می‌کند، با احتمال بیشتری التزامات خود را برآورده خواهد ساخت.

## ۴ اصول و مدل حاکمیت خوب فناوری اطلاعات

### ۴-۱ اصول

این بند شش اصل حاکمیت خوب فناوری اطلاعات را توصیف می‌کند. این اصول رفتارهای ارجح برای راهنماییِ تصمیم‌گیری را بیان می‌دارند. توضیح هر اصل، به آنچه اتفاق می‌افتد اشاره می‌کند اما چگونگی و زمان شخصی که توصیه می‌شود آن را پیاده‌سازی کند را تعیین نمی‌کند. این جنبه‌ها بستگی به ماهیت سازمانی دارد که اصل را پیاده‌سازی می‌کند. توصیه می‌شود نهادهای حاکمیتی کاربست این اصول را الزام آور نمایند.

**اصل ۱: مسئولیت**

افراد یا گروه‌های درون سازمان مسئولیت خود را با توجه به تأمین و تقاضای فناوری اطلاعات، درک و قبول کنند. کسانی که مسئولیت کنش‌ها را دارند، اختیار انجام آن‌ها را نیز دارا می‌باشند.

**اصل ۲: راهبرد**

راهبرد کسب‌وکار سازمان، قابلیت‌های جاری و آتی فناوری اطلاعات را در نظر بگیرد. طرح‌های استفاده از فناوری اطلاعات نیازهای جاری و پیش روی راهبرد کسب‌وکار سازمان را تامین کنند.

**اصل ۳: اکتساب**

اکتساب فناوری اطلاعات برای دلایلی معتبر و بر اساس تحلیل مناسب و مداوم، به همراه تصمیم‌گیری روشن و شفاف انجام می‌شود. تعادل مناسبی بین منافع، فرصت‌ها، هزینه‌ها و مخاطره‌های کوتاه‌مدت و بلندمدت وجود دارد.

**اصل ۴: عملکرد**

فناوری اطلاعات برای پشتیبانی از سازمان، ارائه خدمات، سطوح خدمت، کیفیت خدمت به‌منظور برآوردن

نیازهای جاری و آتی کسب‌وکار ضروری است و مناسب است.

**اصل ۵: انطباق**

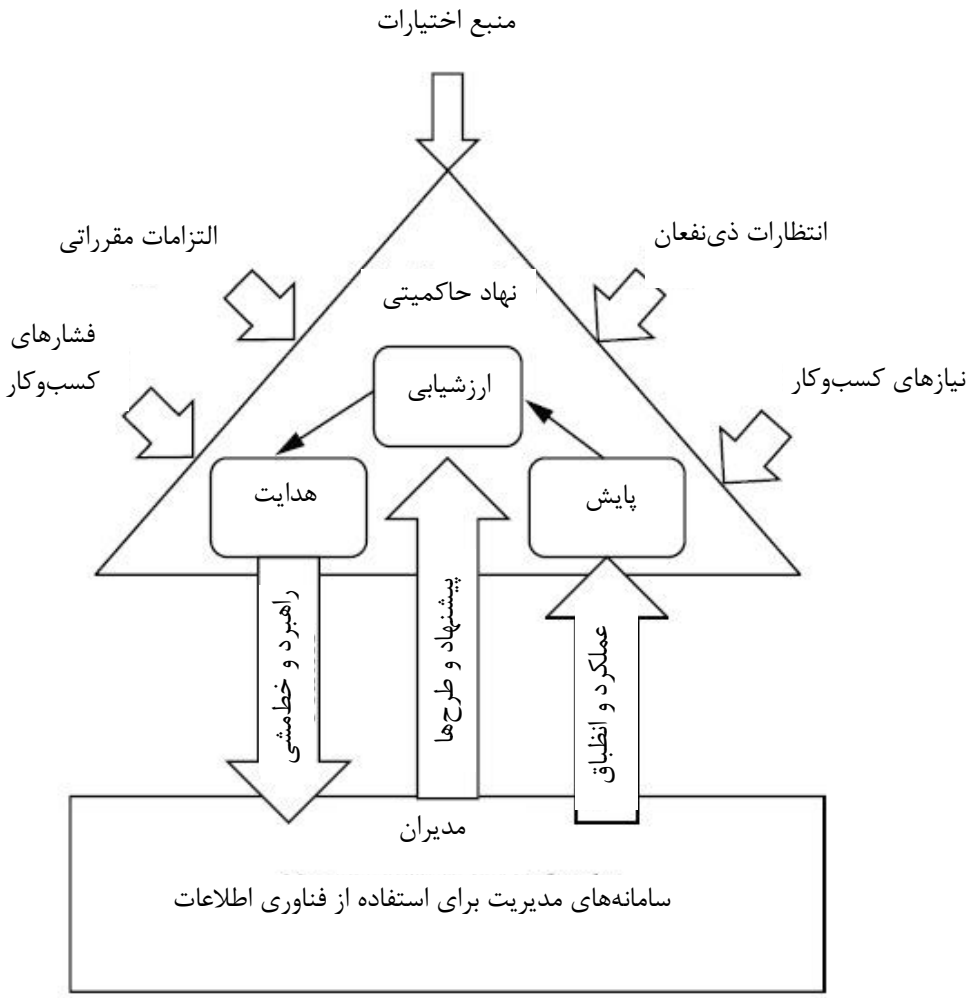
استفاده از فناوری اطلاعات با تمامی قوانین و مقررات الزامی مطابقت دارد. خط‌مشی‌ها و روش‌ها به‌روشنی تعریف، پیاده‌سازی و الزام شده‌اند.

**اصل ۶: رفتار انسانی**

خط‌مشی‌ها، روش‌ها و تصمیمات فناوری اطلاعات احترام به رفتار انسانی را نشان می‌دهد که شامل نیازهای جاری و تکاملی تمامی «افراد دخیل فرایند» است.

## ۲-۴ مدل

توصیه می‌شود نهاد حاکمیتی، فناوری اطلاعات را از طریق سه کار زیر حاکمیت کند:
الف- ارزشیابی استفاده جاری و آتی از فناوری اطلاعات
ب- هدایت آماده‌سازی و پیاده‌سازی مستقیم راهبردها و خط‌مشی‌ها برای حصول اطمینان از این که استفاده از فناوری اطلاعات اهداف کسب‌وکار را برآورده می‌سازد.
پ- پایش انطباق با خط‌مشی‌ها و عملکرد در مقایسه با راهبردها
اختیارات برای جنبه‌های معین فناوری اطلاعات ممکن است به مدیران درون سازمان واگذار شود. اگرچه پاسخگویی برای استفاده مؤثر، کارا و قابل‌قبول فناوری اطلاعات توسط یک سازمان با نهاد حاکمیتی سازمان باقی می‌ماند و نمی‌تواند محول شود.
شکل ۱ مدل حاکمیت فناوری اطلاعات با استفاده از ارزشیابی–هدایت-پایش را نشان می‌دهد. شرح آن در ادامه شکل آمده است.
شکل ۱ عناصر و رابطه‌های به تصویر کشیده شده را توصیف می‌کند.




**شکل ۱- مدل حاکمیت فناوری اطلاعات**

## ارزشیابی

توصیه می‌شود نهادهای حاکمیتی درخصوص استفاده جاری و آتی فناوری اطلاعات شامل طرح‌ها، پیشنهادها و چیدمان‌های تأمین(درونی، بیرونی یا هر دو) بررسی و قضاوت نمایند.

در ارزشیابیِ استفاده از فناوری اطلاعات، توصیه می‌شود نهادهای حاکمیتی فشارهای درونی و بیرونی که بر سازمان وارد می‌شود، نظیر تغییر فنی، گرایشات اقتصادی و اجتماعی، التزامات مقرراتی[1]، انتظارات قانونی[2] ذی‌نفعان و تأثیرات سیاسی را در نظر گیرند. توصیه می‌شود نهادهای حاکمیتی با تغییر شرایط، ارزشیابی را به صورت مستمر به عهده گیرند. همچنین توصیه می‌شود نیازهای جاری و آتی کسب‌وکار را در نظر بگیرند – اهداف سازمانی جاری و آتی که باید محقق شوند نظیر حفظ مزیت رقابتی و همچنین اهداف مشخص طرح‌ها و پیشنهادهایی که ارزشیابی می‌شوند.

1- Regulatory obligations
2- Legitimate

**هدایت**

توصیه می‌شود نهادهای حاکمیتی مسئولیت آماده‌سازی و پیاده‌سازی مستقیم راهبردها و خط‌مشی‌ها را تعیین کنند. توصیه می‌شود راهبردها در جهت سرمایه‌گذاری در فناوری اطلاعات و این که توصیه می‌شود فناوری اطلاعات به چه چیزی دست یابد، تنظیم شوند. توصیه می‌شود خط‌مشی‌ها رفتار دقیق و بی‌عیبی در استفاده از فناوری اطلاعات ایجاد کنند.

توصیه می‌شود نهادهای حاکمیتی در سازمان‌های خود فرهنگ حاکمیت خوب فناوری اطلاعات را از طریق درخواست از مدیران برای تأمین اطلاعات زمان‌بندی شده، تشویق کنند تا با جهت‌گیری سازگاری داشته باشد و با شش اصل حاکمیت خوب انطباق داشته باشد.

در صورت لزوم، توصیه می‌شود نهادهای حاکمیتی ارسالِ پیشنهادها برای تصویب را هدایت کنند تا به نیازهای شناسایی شده بپردازند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی از طریق سامانه‌های اندازه‌گیری مناسب، عملکرد فناوری اطلاعات را پایش کنند. توصیه می‌شود آن‌ها از تطابق عملکرد با راهبردها، به‌ویژه در مورد اهداف کسب‌وکار اطمینان مجدد حاصل کنند. همچنین توصیه می‌شود نهادهای حاکمیتی از مطابقت فناوری اطلاعات با التزامات بیرونی (مقرراتی، قانونی، قراردادی) و شیوه‌های کاری داخلی مطمئن شوند.

## ۵ راهنمایی برای حاکمیت فناوری اطلاعات

### ۵-۱ عمومی

بندهای بعدی، راهنمایی را برای اصول عمومی حاکمیت خوب فناوری اطلاعات و روش‌های لازم برای پیاده-سازی این اصول در بر می‌گیرد.

روش‌های توصیف شده جامع نیستند، ولی نقطه شروعی برای بحث در مورد مسئولیت‌های نهاد حاکمیتی سازمان برای حاکمیت فناوری اطلاعات را فراهم می‌کنند. به همین دلیل این روش‌ها به‌عنوان راهنمایی برای حاکمیت فناوری اطلاعات پیشنهاد می‌شوند.

مسئولیت هر سازمان است که به صورت فردی، کنش‌های مشخص مورد نیاز برای پیاده‌سازی اصول را با در نظر گرفتن ماهیت سازمان و تحلیل مناسب مخاطره‌ها و فرصت‌های استفاده از فناوری اطلاعات تعیین کند.

### ۵-۲ اصل ۱: مسئولیت

**ارزشیابی**

توصیه می‌شود نهادهای حاکمیتی گزینه‌های انتخابی برای به عهده گرفتن مسئولیت با توجه به استفاده جاری و آتی سازمان از فناوری اطلاعات را ارزشیابی کنند. توصیه می‌شود نهادهای حاکمیتی در ارزشیابی

گزینه‌های انتخابی به دنبال حصول اطمینان از استفاده مؤثر، کارا و قابل‌قبول از فناوری اطلاعات در پشتیبانی از اهداف کسب‌وکار جاری و آتی باشند.
توصیه می‌شود نهادهای حاکمیتی صلاحیت آن‌هایی که مسئولیت تصمیم‌گیری در مورد فناوری اطلاعات دارند را ارزشیابی کنند. توصیه می‌شود این افراد عموماً مدیران کسب‌وکار باشند که مسئولیت اهداف و عملکرد کسب‌وکار سازمان را بر عهده دارند و متخصصانی که فرایندها و ارزش‌های کسب‌وکار را می‌دانند، با ایشان همکاری کنند.

**هدایت**

توصیه می‌شود نهادهای حاکمیتی با توجه به مسئولیت‌های نسبت داده شده‌ی فناوری اطلاعات، راهبردها را هدایت کنند. توصیه می‌شود نهادهای حاکمیتی اطلاعاتی که دریافت می‌کنند تا مسئولیت و پاسخگویی خود را انجام دهند، را هدایت کنند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی سازوکارهای مناسب برای حاکمیت فناوری اطلاعات را پایش کنند.
توصیه می‌شود نهادهای حاکمیتی عملکرد افرادی که مسئولیت حاکمیت فناوری اطلاعات را دارند را پایش کنند. (مثل افرادی که در کمیته‌های راهنما خدمت می‌کنند یا پیشنهادهایی به نهاد حاکمیتی سازمان می‌دهند.)
توصیه می‌شود نهاد حاکمیتی سازمان افرادی که مسئولیت دانش و درک مسئولیت خود را دارند را پایش کند.

### ۳-۵ اصل ۲: راهبرد

**ارزشیابی**

توصیه می‌شود نهادهای حاکمیتی به‌منظور حصول اطمینان از این که فناوری اطلاعات، پشتیبانی از نیازهای جاری و آتی کسب‌وکار را تأمین می‌کند، توسعه‌های فناوری اطلاعات و فرایندهای کسب‌وکار را ارزشیابی کنند.
توصیه می‌شود نهادهای حاکمیتی در زمان بررسی طرح‌ها و خط‌مشی‌ها، استفاده از فناوری اطلاعات و فعالیت‌های فناوری اطلاعات را ارزشیابی کنند تا اطمینان حاصل شود که با اهداف سازمان هم سو باشند و نیازهای قانونی کلیدی ذی‌نفعان را برآورده سازند.
همچنین توصیه می‌شود نهاد حاکمیتی سازمان تجارب خوب را در نظر داشته باشد.
توصیه می‌شود نهادهای حاکمیتی اطمینان حاصل نمایند که استفاده از فناوری اطلاعات در حیطه مدیریت مخاطره مناسب قرار دارد.

**هدایت**

توصیه می‌شود نهادهای حاکمیتی آماده‌سازی و استفاده از راهبردها و خط‌مشی‌ها را هدایت کنند تا اطمینان حاصل نمایند که سازمان از توسعه فناوری اطلاعات نفع می‌برد.
همچنین توصیه می‌شود نهادهای حاکمیتی، ارسال پیشنهادها برای استفاده نوآورانه از فناوری اطلاعات را که سازمان را قادر می‌سازد تا به چالش‌ها یا فرصت‌های جدید پاسخ دهد، کسب‌وکارهای جدید را به عهده بگیرد یا فرایندها را بهبود بخشد، تشویق کند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی پیشرفت پیشنهادهای مصوب فناوری اطلاعات را پایش کنند تا مطمئن شوند آن‌ها در چارچوب زمانی مطلوب و با استفاده از منابع معین به اهداف دست پیدا می‌کنند. توصیه می‌شود نهادهای حاکمیتی استفاده از فناوری اطلاعات را پایش کنند تا اطمینان حاصل نمایند که منافع مورد نظر را به دست می‌آورد.

### ۴-۵ اصل ۳: اکتساب

**ارزشیابی**

توصیه می‌شود نهادهای حاکمیتی گزینه‌های تأمین فناوری اطلاعات را برای تحقق پیشنهادهای تاییدشده، متعادل کردن مخاطرات و ارزش‌گذاری پول سرمایه‌گذاری‌های پیشنهاد شده، ارزشیابی کنند.

**هدایت**

توصیه می‌شود نهادهای حاکمیتی دارایی‌های فناوری اطلاعات (سامانه‌ها و زیرساخت) را طوری هدایت کنند تا به روش مناسبی تعیین شده و شامل آماده‌سازی مستندات مناسب باشند و در حالی‌که از تأمین توانایی‌های مطلوب، اطمینان حاصل کند.
توصیه می‌شود نهادهای حاکمیتی تأمین مقدمات پشتیبانی نیازهای کسب‌وکار سازمان (شامل مقدمات تأمین درونی و بیرونی) را هدایت کنند.
توصیه می‌شود نهادهای حاکمیتی طوری هدایت کنند تا سازمان و تأمین کنندگانشان، فهم مشترک از تمایلات سازمان در هرگونه اکتساب فناوری اطلاعات توسعه دهند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی سرمایه‌گذاری‌های فناوری اطلاعات را پایش کنند تا اطمینان حاصل نمایند که ظرفیت‌های مورد نیاز را تامین می‌کنند.
توصیه می‌شود نهادهای حاکمیتی میزان فهم مشترک سازمان و تأمین کنندگان خود از تمایلات سازمان در ایجاد هرگونه اکتساب فناوری اطلاعات را پایش کنند.

### ۵-۵ اصل ۴: عملکرد

**ارزشیابی**

توصیه می‌شود نهادهای حاکمیتی طرح‌های پیشنهاد شده توسط مدیران را ارزشیابی کنند تا اطمینان حاصل نمایند که فناوری اطلاعات از فرایندهای کسب‌وکار با توانایی‌ها و ظرفیت‌های مطلوب پشتیبانی می‌کند.
توصیه می‌شود این پیشنهادها عملیات عادی مداوم سازمان و رفتار با مخاطره مرتبط با استفاده از فناوری اطلاعات را نشان دهند.
توصیه می‌شود نهادهای حاکمیتی مخاطره‌های عملیات مداوم کسب‌وکار که از فعالیت‌های فناوری اطلاعات ناشی می‌شود را ارزشیابی کنند.
توصیه می‌شود نهاد حاکمیتی مخاطره‌های یکپارچگی اطلاعات و حفاظت دارایی‌های فناوری اطلاعات شامل مالکیت‌های فکری پیوسته و حافظه‌ی سازمانی را ارزشیابی کنند.
توصیه می‌شود نهادهای حاکمیتی گزینه‌های انتخابی برای اطمینان از تصمیمات به هنگام و مؤثر درباره استفاده از فناوری اطلاعات در پشتیبانی از اهداف کسب‌وکار را ارزشیابی کنند.
توصیه می‌شود نهادهای حاکمیتی موثر بودن و عملکرد حاکمیت فناوری اطلاعات سازمان را به‌طور منظم ارزشیابی کنند.

**هدایت**

توصیه می‌شود نهادهای حاکمیتی از تخصیص منابع کافی اطمینان حاصل نمایند، تا فناوری اطلاعات نیازهای سازمان را، مطابق با اولویت‌های مورد توافق و محدودیت‌های بودجه برآورده کند.
توصیه می‌شود نهادهای حاکمیتی آن دسته از مسئولین را برای حصول اطمینان از این که فناوری اطلاعات در هنگام نیازهای کسب‌وکار، با اطلاعات صحیح و روزآمد که در برابر از بین رفتن و سوء استفاده محافظت می‌شوند، از سازمان پشتیبانی می‌کند، هدایت کنند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی وسعت پشتیبانی‌های فناوری اطلاعات از کسب‌وکار را پایش کنند. توصیه می‌شود نهادهای حاکمیتی وسعت منابع تخصیص داده شده و محدودیت‌های بودجه مطابق با اهداف کسب‌وکار را پایش کنند.
توصیه می‌شود نهادهای حاکمیتی وسعت خط‌مشی‌های پیروی شده به‌طور صحیح مانند دقت و صحت داده‌ها و استفاده کارا از فناوری اطلاعات را پایش کنند.

### ۵-۶ اصل ۵: انطباق

**ارزشیابی**

توصیه می‌شود نهادهای حاکمیتی به‌طور منظم وسعت مطابقت با التزامات (مقرراتی، قانونی، قراردادی)،

خط‌مشی‌های درونی، استانداردها و راهنماهای حرفه‌ای توسط فناوری اطلاعات را ارزشیابی کنند.
توصیه می‌شود نهادهای حاکمیتی به‌طور منظم انطباق درونی سازمان با چارچوب کار آنی برای حاکمیت فناوری اطلاعات را ارزشیابی کنند.

**هدایت**

توصیه می‌شود نهادهای حاکمیتی آن دسته از مسئولین را که سازوکار های منظم عادی را برقرار می‌کنند، برای اطمینان از این که استفاده از فناوری اطلاعات با التزامات مربوطه، خط‌مشی‌های درونی، استانداردها و راهنما تطابق دارد، هدایت کنند.
توصیه می‌شود نهادهای حاکمیتی خط‌مشی‌های ایجاد شده و تایید شده را برای توانمندسازی سازمان در برآوردن الزامات درونی در استفاده از فناوری اطلاعات، هدایت کنند.
توصیه می‌شود نهادهای حاکمیتی کارمندان فناوری اطلاعات را با پیروی از راهنمای مربوطه برای رفتار حرفه‌ای و توسعه هدایت کنند.
توصیه می‌شود نهادهای حاکمیتی تمام کنش‌های مربوط به اخلاقی بودن فناوری اطلاعات را هدایت کنند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی از طریق گزارش دهی مناسب و روش‌های ممیزی، مقبولیت و انطباق فناوری اطلاعات را پایش کنند تا اطمینان حاصل کنند که بازنگری‌ها برای ارزیابی وسعت رضایت سازمان به هنگام، جامع و مناسب باشند.
توصیه می‌شود نهادهای حاکمیتی فعالیت‌های فناوری اطلاعات شامل امحای[1] دارایی‌ها و داده‌ها را پایش کنند تا از برآورده شدن التزامات محیطی، حریم خصوصی، مدیریت دانش راهبردی، حراست از حافظه‌ی سازمانی و سایر التزامات مربوطه اطمینان حاصل کند.

### ۷-۵ اصل ۶: رفتار انسانی

**ارزشیابی**

توصیه می‌شود نهادهای حاکمیتی جهت حصول اطمینان از این که رفتارهای انسانی شناسایی شده و به درستی درنظر گرفته شده‌اند؛ فعالیت‌های فناوری اطلاعات را ارزشیابی کنند.

**هدایت**

توصیه می‌شود نهادهای حاکمیتی سازگاریِ فعالیت‌های فناوری اطلاعات با رفتار انسانی شناسایی شده را هدایت کنند. توصیه می‌شود نهادهای حاکمیتی مخاطره‌ها، فرصت‌ها، موضوعات و نگرانی‌هایی که توسط هر

1- Disposal

شخص در هر زمان شناسایی و گزارش می‌شود را هدایت کنند. توصیه می‌شود این مخاطره‌ها در تطابق با خط‌مشی‌های منتشر شده و روش‌های اجرایی مربوط به تصمیم‌گیرندگان، مدیریت شوند.

**پایش**

توصیه می‌شود نهادهای حاکمیتی فعالیتهای فناوری اطلاعات را جهت اطمینان از این که رفتارهای انسانی شناسایی شده مرتبط باقی بمانند و توجه مناسبی به آن‌ها شود، پایش کنند.
توصیه می‌شود نهادهای حاکمیتی روش‌های کاری را پایش کنند تا از سازگاری آنها با استفاده مناسب از فناوری اطلاعات، اطمینان حاصل کنند.

## کتاب‌نامه


**[1]** ISO/IEC TR 38502, Information technology — Governance of IT — Framework and model

**[2]** ISO/IEC TS 38501, Information technology — Corporate governance of IT implementation guide

**[3]** ISO/IEC Directives Part 1, Consolidated ISO Supplement, 2013, Annex SL, Appendix 2

**[4]** Report of the Committee on the Financial Aspects of Corporate Governance. Sir Adrian Cadbury, London, 1992 ISBN 0 85258 913 1

**[5]** OECD Principles of Corporate Governance. OECD, 1999 and 2004