INSO
20125
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
۲۰۱۲۵
چاپ اول
۱۳۹۴

فناوری اطلاعات

حاکمیت فناوری اطلاعات – چارچوب و مدل

Information Technology – Governance of IT – Frameowrk and Model

ICS: 35.020

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 تجاری 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 رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه به شرایط کلی و نیازمندی‌های 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، اجرای 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، اجرای 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– چارچوب و مدل »

رئیس :	**سمت و/ یا نمایندگی**
جلالت، بهنام (کارشناسی ارشد مهندسی صنایع)	کارشناس برنامه‌ریزی صنایع دفاع
دبیر:	
مرادی، فریبا (کارشناسی فناوری اطلاعات)	کارشناس فناوری اطلاعات و آماراداره کل استاندارد استان ایلام
اعضاء : (اسامی به ترتیب حروف الفبا)	
بای، مهیا (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش استان البرز
بشارتی، رضا (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات جهاددانشگاهی استان ایلام
بهادری، فاطمه (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش استان تهران
پدرام، سعیده (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش استان تهران
خلیلی فر، نوید (کارشناسی ارشد هوش مصنوعی)	معاون نرم‌افزار شرکت مهندسی پزشکی بهین پرداز پژوهش خاوران تهران
فرخی، ستاره (کارشناسی ادبیات زبان انگلیسی)	کارشناس آموزش جهاد دانشگاهی استان ایلام
مرادی، افسانه (کارشناسی مهندسی کامپیوتر)	کارشناس فناوری اطلاعات آموزش و پرورش استان تهران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

ستاندارد « فناوری اطلاعات – حاکمیت فناوری اطلاعات – چارچوب و مدل » که پیش نویس آن در کمیسیون فنی مربوط، توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و درسیصد و نود و نهمین اجلاسیه کمیته ملی فناوری اطلاعات مورخ ۱۳۹۴/۱۲/۸ مورد تصویب قرار گرفته است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱ به عنوان استاندارد ملی منتشر می شود.

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 خواهند شد و هر گونه 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 تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که در تهیه این استاندارد مورد استفاده قرار گرفته است به شرح زیر است

ISO/IEC TR38502:2014, Information technology - Governance of IT - Framework and model

فناوری اطلاعات - حاکمیت فناوری اطلاعات(IT) [1]– چارچوب و مدل

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین راهنمایی در مورد ماهیت و سازوکارهای مربوط به حاکمیت[2] و مدیریت، به همراه روابط میان آنها، در خصوص فناوری اطلاعات در یک سازمان است

این استاندارد، اطلاعاتی درباره چارچوب و مدلی ارائه می‌کند که می‌تواند برای برقراری مرزها و ارتباط میان حاکمیت و مدیریت به‌کارگیری حال و آتی فناوری اطلاعات در یک سازمان، استفاده شود.

این استاندارد، در موارد زیر کاربرد دارد:

- نهاد حاکمیتی؛
- مدیرانی که باید در محدوده مرجعیت و متولی‌گری ایجاد شده توسط حاکمیت، کار کنند؛
- مشاور یا افرادی که با حاکمیت سازمان‌هایی با هر اندازه و از هر نوع همکاری دارند؛ و
- توسعه‌دهندگان استانداردها درحوزه‌های حاکمیت فناوری اطلاعات و مدیریت فناوری اطلاعات.

۲

اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

۲-۱

قابل قبول[3]

انتظاراتی که ظرفیت نمایش منطقی یا شایسته دارد را از ذینفعان[4] برآورده می‌سازد.

۲-۲

پاسخگو[5]

مسئول اقدامات، تصمیم‌ها و کارآیی است.

۲-۳

پاسخ‌گویی[6]

حالت پاسخ‌گو بودن است.

یادآوری ۱- پاسخ‌گویی، به یک مسئولیت اختصاص داده شده مربوط می‌شود. مسئولیت ممکن است مبتنی بر مقررات یا توافق یا از طریق واگذاری به‌صورت بخشی از تفویض باشد.

1- Information Technology
2 -Governance
3- Acceptable
4 -Stakeholder
5-Accountable
6 -Accountability

۴-۲

حاکمیت شرکتی[1]

سامانه‌ای که توسط آن شرکت‌ها هدایت و واپایش[2] می‌شود.

یادآوری ۱- حاکمیت شرکتی، حاکمیت سازمانی است که به شرکت‌ها اعمال می‌شود.

یادآوری ۲- از Cadbury 1992 و OECD 1999

یادآوری ۳- تعریف برای روشن کردن تغییرات در واژگان ویرایش قبلی، گنجانده شده است.

۵-۲

هدایت[3]

مرتبط ساختن اهداف مطلوب و دستاوردها با یکدیگر است.

یادآوری ۱ - در زمینه حاکمیت فناوری اطلاعات، هدایت شامل تنظیم اهداف، راهبردها و خط‌مشی‌هایی است که توسط اعضاء سازمان اتخاذ می‌شوند، تا اطمینان حاصل شود که استفاده از فناوری اطلاعات می‌تواند اهداف کسب‌وکاری را برآورده سازد.

یادآوری ۲ - اهداف، راهبردها و خط‌مشی‌ها ممکن است در صورت دارا بودن اختیار از نهاد حاکمیت، توسط مدیران تعیین شود.

۶-۲

ارزیابی کردن[4]

لحاظ کردن و اخذ قضاوت‌های آگاهانه است.

یادآوری ۱- در زمینه‌ی حاکمیت فناوری اطلاعات، ارزشیابی شامل قضاوت‌های مربوط به شرایط داخلی و خارجی، حال و آتی و نیز فرصت‌های مرتبط با کاربرد جاری و آتی فناوری اطلاعات سازمان است.

1-Corporate Governance
2-Controlled
3-Direct
4-Evaluate

۷-۲

مدیر اجرایی[1]

فردی که دارای اختیار تفویض شده توسط نهاد حاکمیت برای پیاده‌سازی راهبردها و خط مشی ها، به منظور تحقق هدف سازمان است.

یادآوری ۱- مدیران اجرایی می‌توانند شامل نقش‌هایی باشند که به نهاد حکمرانی یا راس سازمان گزارش داده، یا اینکه پاسخ‌گویی کلی، برای عملکرد اصلی گزارش‌دهی باشند، برای مثال، مدیران ارشد اجرایی (CEOs)[2] رؤسای سازمان‌های حاکمیتی، مدیران ارشد مالی (CFOs)[3] ، مدیران ارشد عملیاتی (COOs)[4] ، مدیران ارشد اطلاعاتی (CIOs)[5] و نقش‌های مشابه.

یادآوری ۲ – در استانداردهای مدیریتی، از مدیران اجرایی ممکن است تحت عنوان مدیریت ارشد یاد شود.

۸-۲

حاکمیت

نظام هدایت کردن و واپایش است.

۹-۲

بدنه حاکمرانی[6]

فرد یا گروهی از افراد که پاسخگوی کارکرد و انطباق سازمان است.

۱۰-۲

چارچوب حاکمیت[7]

راهبردها، خط‌مشی‌ها و ساختارهای تصمیم‌گیری و پاسخ‌گویی‌ها، که از طریق آنها ترتیب های‌حاکمیت سازمان عمل می کند.

1- Executive Manager
2- Chief Executive Officers
3-Chief Financial Officers
4- Chief Operating Officers
5- Chief Information Officers
6- Governing Body
7- Governance Framework

۱۱-۲

حاکمیت فناوری اطلاعات[1]

سامانه‌ای که به واسطه آن، کاربردهای حال و آتی فناوری اطلاعات هدایت و واپایش می‌شود.

یادآوری ۱- حاکمیت فناوری اطلاعات، مولفه یا زیرمجموعه‌ای از حاکمیت سازمانی است.

یادآوری ۲ - این عبارت معادل عبارات زیر است: « حاکمیت شرکتی فناوری اطلاعات»، « حاکمیت بنگاهی فناوری اطلاعات» و « حاکمیت سازمانی فناوری اطلاعات ».

۱۲-۲

واپایش داخلی[2]

خط‌مشی‌ها، رویه‌ها، تجارب و ساختارهای سازمانی که برای ارائه اطمینان منطقی از این امر که اهداف کسب‌وکار محقق شده و این‌که وقایع نامطلوب پیشگیری شده، شناسایی شده و تصحیح خواهد شد، طراحی شده است.

۱۳-۲

فناوری اطلاعات

منابع به کار گرفته شده برای اکتساب، پردازش، ذخیره‌سازی و انتشار اطلاعات است.

یادآوری ۱- این عبارت شامل « فناوری ارتباطات (CT)[3]» و عبارت ترکیبی« فناوری اطلاعات و ارتباطات (ICT)[4]» نیز است.

۱۴-۲

سرمایه‌گذاری[5]

تخصیص منابع برای دستیابی به اهداف تعریف شده و دیگر منافع است.

۱۵-۲

مدیریت

عمل واپایش و نظارت در محدوده اختیار و پاسخ‌گویی ایجاد شده توسط حاکمیت است.

یادآوری ۱- این عبارت اغلب به عنوان یک اصطلاح جمعی برای آنهایی به کار می‌رود که دارای مسئولیت‌پذیری برای واپایش یک سازمان و یا بخش‌هایی از یک سازمان هستند. عبارات « مدیران » برای اجتناب از اشتباه گرفتن با سامانه‌های مدیریتی استفاده شده است.

1- Governance Of IT
2-Internal Control
3-Communications Technology
4 -Information and Communications Technology
5 -Investment

۱۶-۲

سامانه مدیریتی[1]

مجموعه‌ای از عناصر همبسته و متعامل یک سازمان، برای ایجاد خط‌مشی‌ها و اهداف و فرآیندها برای دستیابی آن اهداف است.

یادآوری ۱- یک سامانه مدیریتی می‌تواند یک اصل واحد یا چندین اصل را بیان کند.

یادآوری ۲- سامانه‌های مدیریتی باید در محدوده راهبردها، ساختارها، مسئولیت‌پذیری‌ها و پاسخگویی‌های مشخص شده در چارچوب حاکمیت سازمان عمل کنند.

[منبع: رهنمودهای ISO/IEC، قسمت ۱، ضمیمه متمم ISO- رویه‌های برای2013،ISO ، پیوست SL، پیوست 2،3.04 ،اصطلاح شده – یادآوری ۲ اضافه شده است.]

۱۷-۲

مدیران[2]

گروهی از افراد که مسئول نظارت بر یک سازمان و یا بخش‌هایی از یک سازمان هستند.

یادآوری ۱- مدیران اجرایی، رده ای از مدیران هستند.

۱۸-۲

پایش[3]

بازنگری به عنوان مبنایی برای تصمیم هاو تعدیلات مناسب است.

یادآوری ۱- پایش به شکل روزمره درگیر کسب اطلاعات در مورد پیشرفت طرح‌ها و نیز بررسی دوره‌ای دستاوردهای کلی در مقایسه با راهبردها دستاوردهای توافق شده، به منظور ارائه مبنایی برای تصمیم‌گیری و تعدیل طرح‌ها است.

یادآوری ۲- پایش شامل بازنگری انطباق با قوانین، مقررات و خط‌مشی‌های سازمانی است.

1- Managers System
2- Managers
3-Monitor

۲-۱۹

سازمان[1]

فرد یا گروهی از افرادی که کارکردهای خود را با مسئولیت‌ها، اختیارها و ارتباط‌های خود به منظور تحقق اهداف آن دارند.

یادآوری ۱- مفهوم سازمان شامل، ولی نه فقط به، تجار، شرکت، مؤسسه، کارخانه، کسب‌وکار، مشارکت، خیریه یا مؤسسه، بخش و یا ترکیبی از آنها، ثبت شده عمومی یا خصوصی، محدود می شود.

[منبع: رهنمودهای ISO/IEC، قسمت ۱، ضمیمه متمم ISO- رویه‌های برای 2013، ISO، پیوست SL، پیوست2،3.01]

۲-۲۰

حاکمیت سازمانی[2]

سامانه‌ای که به واسطه آن سازمان‌ها هدایت و واپایش می‌شوند.

۲-۲۱

خط‌مشی[3]

نیت‌ها و مسیر یک سازمان، آن‌گونه که به طور رسمی توسط نهاد حکمرانی یا مدیران اجرایی آن، که با اختیار ما است عمل می‌کنند، تصریح شده است.

۲-۲۲

پیشنهاد[4]

مجموعه‌ای از منافع، هزینه‌ها، مخاطرات، فرصت‌ها و دیگر عوامل که قابل کاربرد برای تصمیم‌هایی است که باید اتخاذ شود.

۲-۲۳

منابع[5]

افراد، رویه‌ها، نرم‌افزار، اطلاعات، تجهیزات، موارد مصرفی ، زیرساخت، و سرمایه و وجوه عملیاتی وزمان است.

[منبع رهنمود: ISO/IEC 38500:2008, 1.6.13].

1- Organization
2-Organizational Governance
3-Policy
4-Proposal
5-Resources

۲۴-۲

مسئولیت‌پذیری[1]

تعهد به عمل و اتخاذ تصمیم‌ها برای دستیابی به دستاوردها الزامی است.

۲۵-۲

مخاطره[2]

تأثیر عدم قطعیت بر اهداف است.

یادآوری ۱- یک اثر، انحرافی از انتظار است- مثبت و/یا منفی.

[منبع رهنمود: ISO Guide 73:2009, 1.1 اصلاح شده- یادآوری‌های ۲ تا ۵ حذف شده است].

۲۶-۲

اشتیاق مخاطره[3]

میزان و نوع مخاطره‌ای است که یک سازمان تمایل دارد آنرا دنبال کرده یا حفظ کند.

[منبع رهنمود: ISO Guide 73:2009, 3.7.1.2].

۲۷-۲

سودبران

هر فرد، گروه یا سازمانی که می‌تواند اثرگذار یا تاثیرپذیر باشد، یا اینکه خودآنها را به شکل تأثرپذیرنده بواسطه تصمیم یا فعالیتی محسوب کند.

[منبع رهنمود:ISO Guide 73:2009, 3.2.1.1 اصلاح شده – این نکته حذف شده است.]

۲۸-۲

استفاده از فناوری اطلاعات[4]

طرح‌ریزی، طراحی، توسعه، استقرار، عملیات، مدیریت و کاربرد فناوری اطلاعات برای برآورده کردن اهداف کسب‌وکار، خلق ارزش برای کسب‌وکار است.

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

یادآوری ۲- استفاده از فناوری اطلاعات شامل کاربردهای حال و آتی است.

1-Responsibility
2-Risk
3-Risk Appetite
4-Use Of IT

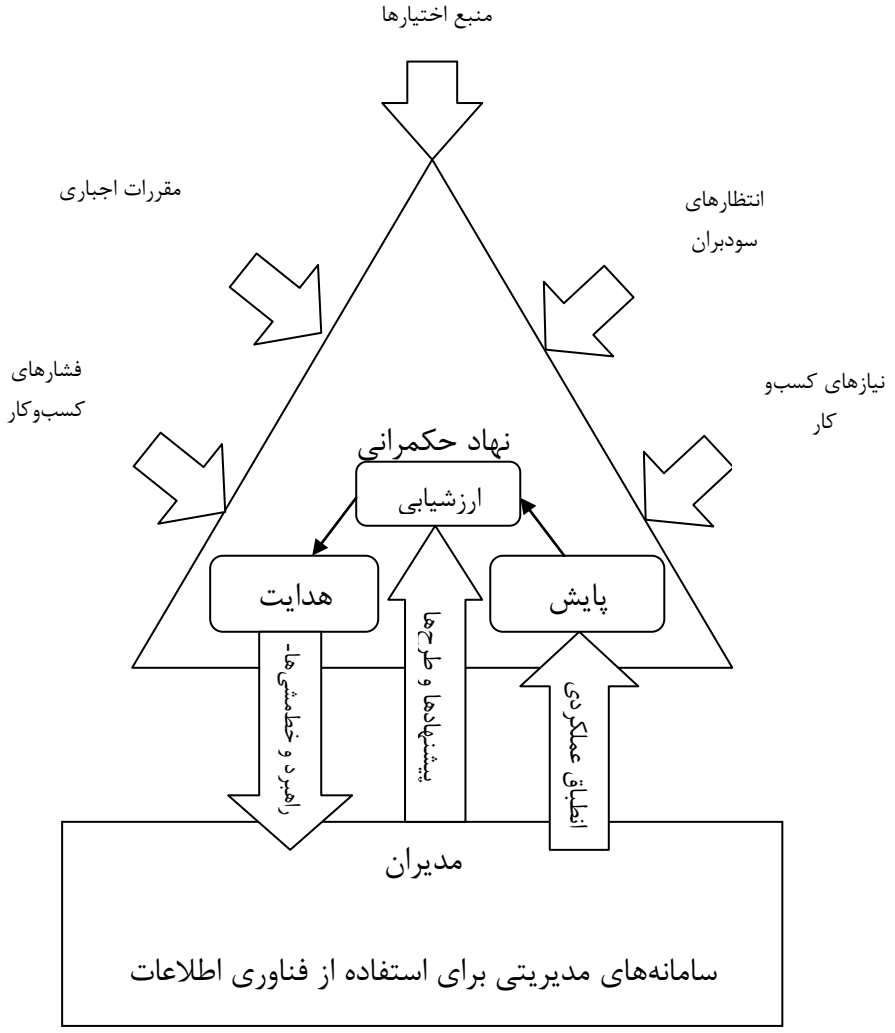
۳ مدل و چارچوب

۳-۱ مدلی برای حاکمیت فناوری اطلاعات

۳-۱-۱ مسئولیت‌ها و پاسخ‌گویی‌های نهاد حکمرانی

نهاد حکمرانی، مسئول و پاسخگوی استفاده‌های حال و آتی فناوری اطلاعات در یک سازمان، به عنوان بخشی از مسئولیت کلی آنها برای حاکمیت سازمانی است.

اختیارها، مسئولیت و پاسخگویی نهاد حکمرانی، بستگی به مرجع اختیار آن خواهد داشت، مانند ترتیب های قانون‌گذاری که تحت آن عمل می‌کند. سطح مورد توافق اختیارها در مرزهای محدوده سازمان، به طور عمومی مستندسازی خواهد شد و بسته به اندازه و نوع سازمان و چارچوب قانون‌گذاری قابل کاربرد در سازمان، به شکل یک منشور برای سازمان یا توافق ساده‌ای بین طرف‌ها خواهد بود.



شکل۱-مدل حاکمیت فناوری اطلاعات (برگرفته از ISO/IEC 38500:2008)

در بسیاری از شرکت‌های سهامی عام، نهادحکمرانی، یک هیئت است، مثل هیئت سرپرستان. حوزه‌های قضایی وجود دارد که در آنها، یک ساختار هیئتی دو لایه با یک هیئت مشاوره و هیئت اجرایی به کار گرفته شده است.

۳-۱-۲ وظایف حاکمیت فناوری اطلاعات

استاندارد ISO/IEC 38500 توصیه می‌کند که نهاد حکمرانی استفاده از فناوری اطلاعات را از طریق وظایف زیر مدیریت می‌کند:

- ارزشیابی
- هدایت
- پایش

وظایف ارزیابی، هدایت و پایش در همکاری نزدیک بین نهاد حکمرانی و مدیران اجرا شده، تا نهاد حکمرانی را قادر سازد که استفاده از فناوری اطلاعات را به منظور تحقق اهداف کسب وکار را هدایت و واپایش کند.
ضمن تقبل فعالیت‌های مدیریتی، نهاد حکمرانی باید الزامات مقرراتی و انتظارهای قانونی سودبران را در تصمیم ها و نیز تأثیر فضای کسب‌وکار، از جمله فشارهای کسب‌وکار و نیازهای تجاری را مد نظر داشته باشد.

۳-۱-۳ مسئولیت‌پذیری‌ها و پاسخ‌گویی‌های مدیران

مدیران، مسئول حصول اطمینان از دستیابی به اهداف سازمان در محدوده راهبردها و خط‌مشی‌های ایجاد شده توسط نهاد حکمرانی، هستند. مدیران نسبت به نهاد حکمرانی نسبت به مسئولیت‌های واگذار شده، پاسخگو هستند.
سازمان‌ها ممکن است از طریق یک سلسه مراتب مدیریتی عمل کنند، این‌گونه که CEO دارای مسئولیت کلی بوده و مدیران دیگر سازمان چه به صورت مستقیم و چه به صورت غیرمستقیم، به شکلی که مناسب است، گزارش‌دهی می‌کنند. در برخی از سازمان‌ها، مدیران اجرایی منتخب ممکن است بخشی از نهاد حکمرانی باشند.

۳-۱-۴ قابلیت کاربرد مدل

مدلی که برای حاکمیت فناوری اطلاعات در این بخش توصیف شده، همچنین می‌تواند برای لحاظ کردن الزامات در سازمان‌هایی که در آن یک نهاد حکمرانی رسمی مثل هیئت مدیران وجود ندارد، استفاده شود. این ممکن است شامل سازمان‌های دولتی باشد، جایی که در آن اختیار، مسئولیت و پاسخ‌گویی در بازوی سیاسی دولت باقی می‌ماند. در چنین شرایطی، اختیار و مسئولیت برای حاکمیت ممکن است به طور مستقیم به یک یا چند مدیر سازمان تفویض شود. این مورد به طور عموم CEO (یا معادل) سازمان خواهد بود، که مسئولیت‌های نهاد حکمرانی را اجرا خواهد کرد. در کسب‌وکارهای خرد، همان فرد ممکن است نقش نهاد حکمرانی و CEO را اخذ کند.

۳-۲ ارتباط میان حاکمیت و مدیریت فناوری اطلاعات

عناصر کلیدی ارتباط میان حاکمیت و مدیریت فناوری اطلاعات که در مدل منعکس شده، به شکل زیر است:

الف) **مسئولیت‌های نهاد حکمرانی:** اعضاء نهاد حکمرانی، مسئول حاکمیت فناوری اطلاعات بوده و پاسخگوی کاربرد اثربخش، کارآمد و قابل قبول فناوری اطلاعات در سازمان هستند؛

ب) **فرموله کردن راهبرد و اشراف:** حاکمیت ابزارهایی را فراهم می‌کند که از طریق آن نهاد حکمرانی، مسیری را برای سازمان، نسبت به استفاده از فناوری اطلاعات تنظیم کرده و وضعیت سازمان و کارکرد مدیران آن را در حصول دستاوردهای لازم، پایش می‌کند

پ) **تفویض:** ابعاد حاکمیت فناوری اطلاعات ممکن است توسط مدیران تقبل شود، اگر مسئولیت‌های مناسب به آنها، به همراه اختیار تفویض شده توسط نهاد حکمرانی را داشته باشند.

ت) **مسئولیت‌پذیری مدیران:** مدیران، مسئول دستیابی به اهداف راهبردی سازمانی در چارچوب راهبردها و خط‌مشی‌هایی برای استفاده از فناوری اطلاعات بوده، که توسط نهاد حکمرانی تنظیم شده است.

ث) **حکمرانی و واپایش داخلی:** حاکمیت اثربخش فناوری اطلاعات نیازمند ایجاد یک سامانه اثربخش واپایش داخلی، به عنوان بخشی از سامانه‌های مدیریتی سازمان است.

هر کدام از این عناصر، در بند ۴: راهنمایی کاربرد مدل، مورد بحث قرار گرفته است.

۳-۳ عناصر کلیدی یک چارچوب حاکمیت فناوری اطلاعات

سامانه‌های مدیریتی فناوری اطلاعات سازمان و کاربرد فناوری اطلاعات آن باید مبتنی بر یک چارچوب حاکمیتی ایجاد شده برای سازمان باشد.

چارچوب واقعی حاکمیت، توسط خود سازمان تعیین شده و بستگی به اندازه و عملکرد سازمان و تصمیم‌ها اتخاذ شده توسط بدنه حکمرانی و نیز مرزهای مسئولیت‌پذیری دارد، امّا عناصر کلیدی باید مانند چیزی باشد که در شکل ۲ نشان داده شده است. ناحیه خاکستری نشان‌دهنده عناصر مدیریتی وابسته است.

شکل ۲- عناصر کلیدی یک چارچوب حاکمیت فناوری اطلاعات

عناصر کلیدی برای چارچوب حاکمیت فناوری اطلاعات باید با موارد زیردرگیر باشد:

الف) **اصول حاکمیت خوب فناوری اطلاعات.** چارچوب حاکمیت باید مبتنی بر اصول حاکمیت خوب فناوری اطلاعات، مانند اصول ذکر شده در ISO/IEC 38500، باشد (پیوست الف). این اصول باید سازمان‌ها را راهنمایی کند که چگونه ترتیب‌های حاکمیت برای استفاده از فناوری اطلاعات را ایجاد کنند.

ب) **راهبردها و خط‌مشی‌هایی برای استفاده از فناوری اطلاعات.** راهبردها و خط‌مشی‌های استفاده از فناوری اطلاعات که توسط بدنه حکمرانی تنظیم و به مدیران اطلاع‌رسانی شده، باید مبنایی را برای اعمال حاکمیت سامانه‌های مدیریتی سازمان فراهم کند. راهبردها و خط‌مشی‌ها باید نیازمندی‌های ویژه سازمان که توسط هیئت‌های اداری و مدیران تنظیم شده را مورد تاکید قرار دهند، ضمن آن‌که این راهبردها و خط‌مشی‌ها بخشی مبتنی بر الزامات اجباری تنظیم شده توسط قوانین و مقررات در حوزه‌های قضایی مختلف یا رهنمودهای سیاسی برای سازمان‌های بخش عمومی است. راهبردها و خط‌مشی‌هایی که اصول رفتاری ذکر شده در ISO/IEC 38500 را مد نظر قرار می‌دهد، باید تعریف شده، اطلاع‌رسانی شده و دستاوردهای آن پایش شود. این‌ها ممکن است شامل موارد زیر باشد:

- اهداف کسب وکار استفاده از فناوری اطلاعات؛
- اولویت‌ها و تخصیص منابع؛

- سطح اختیارها و حقوق تصمیم‌گیری، از جمله اینکه کدام حقوق تصمیم‌گیری برای بدنه حکمرانی محفوظ است؛
- ترتیب های لازم برای تصمیم‌گیری، مبتنی بر راهبردها و خط‌مشی‌های توافق‌شده برای استفاده از فناوری اطلاعات، از جمله مسئولیت‌ها، مرزها، اختیار، ترتیب های استثنایی و ترتیب های گزارش‌دهی؛
- اشتیاق مخاطره مرتبط با استفاده از فناوری اطلاعات و الزامات خاص واپایشی؛ و
- خط‌مشی‌هایی که رفتارهای لازم در خصوص استفاده از فناوری اطلاعات را تعریف می‌کند.

پ) **برنامه‌ریزی کسب‌وکار فناوری اطلاعات**. فرآیندهای برنامه‌ریزی کسب‌وکار باید شامل قابلیت‌های حال و آتی فناوری اطلاعات بوده تا این اطمینان حاصل شود که برنامه‌های راهبردی فناوری اطلاعات، نیازهای فعلی و مداوم راهبرد کسب وسازمان را برآورده می‌سازد. این در بردارنده نوآوری‌های کسب وکار است که توسط فناوری اطلاعات میسر شده است. بنابراین، برنامه‌ریزی تجاری برای فناوری اطلاعات بخش جدایی‌ناپذیر چارچوب حاکمیت سازمانی برای فناوری اطلاعات است.

ت) **مدیریت مخاطره**. چارچوب حاکمیت فناوری اطلاعات باید شامل تجارب قوی مدیریت مخاطره در کل فعالیت‌های فناوری اطلاعات و تصمیم‌گیری باشد. مدیریت مخاطره برای استفاده از فناوری اطلاعات باید مبتنی بر کاربرد فرآیندهای مدیریت مخاطره سازمان باشد.

ث) **پاسخ‌گویی**. سازوکارهایی که از طریق آنها، افراد دارای مسئولیت‌پاسخگو باشند، باید تعریف و مورد توافق قرار گیرد. این امر ممکن است شامل مواردی همچون ارزیابی مداوم، کارکرد (هم کارکرد و هم انطباق) راهبردهای فناوری اطلاعات، طرح‌ها و واحدهای کسب وکاری در سراسر سازمان باشد.

ج) **سامانه‌های مدیریتی برای فناوری اطلاعات**. سامانه‌های مدیریتی برای فناوری اطلاعات باید در قالب راهبردها و خط‌مشی‌های تنظیمی توسط نهاد حکمرانی عمل کرده، تا اهداف راهبردی و عملیاتی سازمان محقق شود. این دربرگیرنده سامانه‌هایی است که با تقاضای تامین فناوری اطلاعات برای واحدهای داخلی تجاری، واحدهای تخصصی فناوری اطلاعات یا تأمین‌کنندگان خارجی و خدمات عمومی سر و کار دارد. مسئولیت پیاده‌سازی سامانه‌های مدیریتی برای تحقق اهداف سازمان‌ها، بر عهده مدیران سازمان است.

چ) چارچوب حاکمیت باید مدیران را قادر سازد تا بر یک مبنای روزانه با بالاترین خودمختاری ممکن عمل کند. حاکمیت نیازمند توسعه ارزش‌ها و اهداف مشترک، تنظیم رهنمودها، ارائه منابع و اختیارها تفویض شده است تا مدیران را قادر سازد با خودمختاری و پاسخگویی مناسب در محیط در حال تغییر عمل کنند.

۴ راهنمایی در مورد کاربرد مدل

۴-۱ مسئولیت‌های نهاد حکمرانی

۴-۱-۱ کلیات

اعضای نهاد حکمرانی، مسئول حاکمیت فناوری اطلاعات بوده و پاسخگوی کاربرد اثربخش، کارآمد و قابل قبول فناوری اطلاعات در سازمان هستند. [۳-۲ الف]

اقتدار و مسئولیت پذیری هیئت مدیره برای استفاده موثر و کار آمد فناوری اطلاعات از مسئولیت پذیری کلی آن برای اداره سازمان برمی آید.

تمرکز اصلی نقش نهاد حکمرانی در حاکمیت فناوری اطلاعات، حصول اطمینان از این امر است که سازمان از سرمایه‌گذاری در فناوری اطلاعات، ضمن مدیریت مخاطره، کسب ارزش می‌کند.

۴-۱-۲ نهاد حکمرانی و سازوکارهای نظارت

الف) نهاد حکمرانی باید سازوکارهای سهوی برای حاکمیت فناوری اطلاعات ایجاد کرده، که برای سطح وابستگی کسب‌وکار به فناوری اطلاعات، مناسب است.

ب) نهاد حکمرانی باید درک روشنی از اهمیت فناوری اطلاعات برای راهبردهای تجاری سازمان و همچنین مخاطره راهبردی بالقوه برای سازمان، ناشی از استفاده از فناوری اطلاعات، داشته باشد. سطح توجهی که نهاد حکمرانی به فناوری اطلاعات دارد، باید مبتنی بر آن عوامل باشد.

پ) ممکن است نهاد حکمرانی، کمیته فرعی را برای کمک به خود در امر نظارت بر استفاده سازمان از فناوری اطلاعات از نقطه نظر راهبردی، ایجاد کند. نیاز به یک زیرکمیته، بستگی به اهمیت فناوری اطلاعات برای سازمان و اندازه آن خواهد داشت.

ت) نهاد حکمرانی باید اطمینان حاصل کند که اعضای آن و نیز سازوکارهای اداری وابسته (مثل کمیته‌های ممیزی، مخاطره و فناوری اطلاعات) دانش و درک لازم از استفاده از فناوری اطلاعات، گرایش‌ها و روندهای آتی فناوری اطلاعات و همچنین اختیارهای مناسب برای بیان مسئولیت‌های خود را دارد.

ث) نهاد حکمرانی باید اثربخشی حاکمیت فناوری اطلاعات و سازوکارها را از طریق درخواست فرآیندهای لازم، مانند ممیزی و ارزیابی‌های مستقل مورد پایش قرار داده تا به این اطمینان برسد که حاکمیت فناوری اطلاعات اثربخش است. برای مثال، نهاد حکمرانی باید اطمینان حاصل کند که پوشش ممیزی کافی در حوزه مدیریت مخاطره مرتبط با فناوری اطلاعات، فرآیندهای واپایشی و اداری، به عنوان بخشی از فرآیند ممیزی، وجود دارد.

۴-۲ فرموله کردن راهبرد و نظارت

۴-۲-۱ کلیات

حاکمیت فناوری اطلاعات ابزاری را فراهم می‌آورد که بـه واسـطه‌ی آن هیئـت مـدیره، مسـیری را بـرای سازمان در استفاده از فناوری اطلاعات تنظیم کرده و وضعیت سازمان و عملکرد مدیران آن را در دستیابی به دستاوردهای لازم، پایش می‌کند.[شماره۲-۳ ب]

به طور کلی، نهاد حکمرانی برای هدایت سازمان از طریق فرموله کردن راهبرد و از طریق نظارت بر کارکرد مدیران در پیاده‌سازی راهبرد، عمل می‌کند. در بسیاری از سازمان‌ها، این امر نیازمند آن است که نهادحکمرانی با مدیران اجرایی کار کرده و از آنها مشاوره بگیرد. آنها در کنار هم، باید دیدگاه روشنی از این که چگونه فناوری اطلاعات می‌تواند به بهترین شکلی به نفع سازمان هم در حال و هم در آینده، مورد بهره-برداری قرار گیرد.

۴-۲-۲ نقش نهاد حکمرانی در قاعده‌مند کردن راهبرد

الف) نهاد حکمرانی که با نهاد حکمرانان اجرایی کار کرده و از آنها مشاوره می‌گیرد باید رهبری توسعه راهبردی به منظور حصول ارزش از استفاده از فناوری اطلاعات را فراهم کند.

ب) نهاد حکمرانی باید راهبرد کسب‌وکار سازمان برای فناوری اطلاعات را با لحاظ کردن تبعات راهبرد برای دستیابی به اهداف تجاری و مخاطراتی که امکان بروز دارد، را تصویب کند.

پ) نهاد حکمرانی باید اطمینان حاصل کند که محیط داخلی و خارجی سازمان، به طور منظم مورد پایش و تحلیل قرار گرفته تا تعیین شود آیا نیازی به بازنگری آن هست، و در زمان مناسب، راهبرد فناوری اطلاعات و هر گونه خط‌مشی مرتبط با آن، بازنگری شود. این شامل نیازها و انتظارهای مشتری، وضعیت رقابتی، نقاط قوت، نقاط ضعف و فرصت‌های آن، فناوری‌های جدید، درخواست‌های مقرراتی، تغییرات سیاسی، پیش‌بینی‌های اقتصادی و عوامل اجتماعی است

ت) نهاد حکمرانی باید اطمینان حاصل کند که خط‌مشی‌هایی برای هدایت رفتار سازمانی تدوین و توسعه یافته است. چنین خط‌مشی‌هایی باید نیل به اهداف تجاری را پشتیبانی کرده، که شامل الزامات مربوط به مقررات و قوانین اجباری است. موارد دیگر، مبتنی بر به‌روش‌ها[1] خواهد بود و سازمان‌ها را بر حسب مدیریت مخاطره و بهبود، در مسیر اثربخشی و کارایی هدایت خواهد کرد

ث) نهاد حکمرانی باید اطمینان حاصل کند که سازوکارهایی برای شفاف‌سازی و تفسیر اهداف، راهبردها و خط‌مشی‌ها، هنگامی‌که مسائل جدید به روز می‌کند، وجود دارد.

ح) نهاد حکمرانی باید آمادگی کسب وکار را برای هرگونه تغییر عمده پیشنهاد شده، به عنوان بخشی از راهبرد سازمانی برای فناوری اطلاعات، درک کرده و اطمینان حاصل کند که تعهدی و قابلیتی در سازمان برای پذیرش تغییرهای لازم وجود دارد.

1-Best Practice

۴-۳ تفویض

۴-۳-۱ کلیات

ابعاد حاکمیت فناوری اطلاعات ممکن است توسط مدیران تقبل شود اگر، مسئولیت واگذار شده به خود، توسط نهاد حکمرانی به همراه اختیارهای تفویض شده را داشته باشد.[۳-۲ پ]

نهاد حکمرانی اهداف سازمان را از طریق و توسط کار با مدیران سازمان محقق می‌کند. یک نهاد حکمرانی ممکن است اختیارها را به یک یا چند مدیر، حسب اساسنامه سازمان و قوانین و مقررات قابل کاربرد، تفویض کند.

حاکمیت فناوری اطلاعات، به طور عموم هم با نهاد حکمرانی و هم با مدیران تمرین خواهد شد. در بسیاری از سازمان‌ها، مسئولیت استفاده از فناوری اطلاعات به مدیران به همراه اختیارها تفویض شده، برای پیشبرد یک سازمان به منظور تحقق اهداف کسب‌وکار، به جای بودن یک اختیار تفویض‌شده صریح، تخصیص پیدا - کند.

در اصل، هیچ‌گونه محدودیتی در آنچه می‌تواند به مدیران اجرایی تفویض شود و آنچه توسط نهاد حکمرانی برای اتخاذ ادامه خواهد داشت، وجود ندارد. نهاد حکمرانی پاسخگوی کارکرد و انطباق سازمان باقی می‌ماند، حتی زمانی که ابعاد حاکمیت و مدیریت همچون تصمیم‌گیری تفویض شده باشد. این امر شامل اثر موفقیت یا شکست استفاده از فناوری اطلاعات است.

۴-۳-۲ تفویض توسط نهاد حکمرانی

الف) نهاد حکمرانی ممکن است ابعادی از حاکمیت فناوری اطلاعات را به مدیران سازمان تفویض کند

ب) هنگام تفویض اختیارها حاکمیت فناوری اطلاعات، نهاد حکمرانی باید موارد زیر را ایجاد کند:

- مسئولیت‌ها و مرزها برای تصمیم‌گیری که به روشنی تعریف و توافق شده است؛
- اختیارها متناسب با منابع مناسب و
- ساز وکارهایی برای حصول اطمینان از انطباق با راهبردها و خط‌مشی‌ها، و این که این اجرا در دستیابی به اهداف، پایش و ارزیابی شده است.

پ) نهاد حکمرانی باید اطمینان یابد که افراد تفویض اختیار شده، دارای لیاقت و شایستگی لازم بوده و نهاد حکمرانی، نظارت مناسب بر تصمیم های کلیدی را حفظ می‌کند.

ت) نهاد حکمرانی باید تعیین و روشن کند که چه تصمیم هایی لازم است به بدنه حکمرانی ارجاع داده شده، تا اینکه بدون ارجاع توسط مدیران اتخاذ شود

ث) نهاد حکمرانی باید اطمینان حاصل کند گستره‌ای که اختیار برای حاکمیت فناوری اطلاعات به مدیران تفویض شده، به روشنی در خط‌مشی‌های حاکمیت تنظیم شده است. در خصوص فناوری اطلاعات، نهاد حکمرانی به طور نوعی درگیر در مواردی مانند زیر، باقی می‌ماند:

- تصویب اهداف، راهبردها و خط مشی‌ها برای استفاده از فناوری اطلاعات؛
- تصویب سرمایه‌گذاری‌های عمده درگیر استفاده از فناوری اطلاعات؛
- نظارت بر برنامه‌ها و پروژه‌های دارای تأثیر عمده روی کسب‌وکار؛ و
- تصویب تجربه‌های کلیدی مدیریت مخاطره، مانند آنهایی که مرتبط با امنیت و تداوم کسب‌وکار است.

ح) نهاد حکمرانی باید اطمینان حاصل کند که تناسب اختیارها تفویض شده، در معرض بازنگری بر یک مبنای مداوم است.

۴-۴ مسئولیت‌های مدیران

۴-۴-۱ کلیات

مدیران مسئول تحقق اهداف راهبردی سازمانی در محدوده راهبردها و خط‌مشی‌ها، برای استفاده از فناوری اطلاعات، که توسط بدنه حکمرانی تنظیم شده، هستند. [۳-۲ ت]

مدیران مسئول حصول اطمینان از این امر هستند که سازمان به دستاوردهای الزامی، در مرزهای ایجاد شده توسط راهبردها و خط‌مشی‌های فناوری اطلاعات، که توسط هیئت مدیران تصریح یا توافق شده، دست پیدا می‌کند. مدیران برای کسب این دستاوردها، در قبال نهاد حکمرانی پاسخگو هستند. مسئولیت‌ها، اختیارها و پاسخگویی مدیران، توسط نهاد حکمرانی تعیین شده است. در برخی از حوزه‌های اختیار، ممکن است پاسخگویی خاص و نیز الزامات گزارش‌دهی برای برخی نقش‌های سازمانی اعمال شود.
مدیران مسئول پیاده‌سازی راهبرد و خط‌مشی و نیز پیاده‌سازی نظارت بر سامانه‌های مدیریتی لازم برای تحقق اهداف تعیین شده توسط هیئت دولت، هستند.

۴-۴-۲ نقش مدیران

الف) مدیران باید از حصول دستاوردهای الزامی برای کسب‌وکار در محدوده راهبردها و خط‌مشی‌ها برای استفاده از فناوری اطلاعات، آن‌گونه که توسط نهاد حکمرانی تنظیم شده، اطمینان حاصل کنند.

ب) مدیران باید راهبردها، خط‌مشی‌ها و سامانه‌های مدیریتی را به منظور حصول اهداف کسب‌وکار تعیین شده توسط نهاد حکمرانان، پیاده‌سازی کنند. این ممکن است شامل موارد زیر باشد:

- توسعه و اطلاع‌رسانی خط‌مشی‌ها، راهنمایی‌ها و استانداردها برای فناوری اطلاعات، مبتنی بر اصول و خط‌مشی‌های عنوان شده توسط بدنه حکمرانان؛
- طرح‌ریزی راهبردی برای فناوری اطلاعات به عنوان بخش جدایی ناپذیرطرح‌ریزی راهبردی کسب‌وکار، اگر اختیارها توسط بدنه حکمرانانی تفویض شده است؛
- ایجاد سازوکارهایی برای مدیریت تقاضا و تامین فناوری اطلاعات برای پشتیبانی از نوآوری‌های تغییر کسب‌وکار؛

- ایجاد سازوکارهایی برای مدیریت تقاضا و تامین فناوری اطلاعات برای عملیات موجود کسب‌وکار؛
- اِعمال مدیریت مخاطره (یکپارچه شده با سامانه مدیریت مخاطره سازمانی) در استفاده از فناوری اطلاعات؛
- تضمین اینکه سرمایه‌گذاری‌ها در فناوری اطلاعات، همانند یک سبد برنامه[1] با گستره‌ی کاملی از فعالیت‌های لازم برای دستیابی به ارزش کسب‌وکار، مدیریت خواهد شد.
- پایش و ارزیابی کارکرد و انطباق سازمانی و نیز گزارش‌دهی به نهاد حکمرانی.

پ) مدیران باید تصمیم هایی را در زمینه راهبردها و خط‌مشی‌های تنظیمی توسط نهاد حکمرانی اتخاذ کنند.

۴-۵ حاکمیت و واپایش داخلی

۴-۵-۱ کلیات

حاکمیت اثربخش فناوری اطلاعات نیازمند ایجاد سامانه‌ای اثربخش برای واپایش داخلی، به عنوان بخشی از سامانه‌های مدیریت سازمان، است. [۳-۲ ث]

مدیران دارای مسئولیت ارزیابی مخاطره مربوط به سازمان و پیاده‌سازی یک سامانه مناسب واپایش داخلی هستند. نهاد حکمرانی، خط‌مشی‌هایی برای شناسایی یک مخاطره قابل پذیرش برای سازمان را، در واپایش داخلی ایجاد کرده است، که الزامات قانونی را، مد نظر قرار می‌دهد. مدیریت مخاطره، یک عنصر کلیدی در مدل حاکمیت است، بنابراین، مخاطره را باید در طی ارزیابی، هدایت و پایش مدنظر قرار داد.

۴-۵-۲ ایجاد واپایش داخلی

الف) نهاد حکمرانی باید خط‌مشی‌هایی را در مورد واپایش داخلی ایجاد کرده که آنچه یک مخاطره قابل قبول برای سازمان است، را شامل شود. این باید شامل اشتیاق مخاطره در ارتباط با استفاده از فناوری اطلاعات و الزامات خاص واپایشی باشد

ب) مدیران باید سامانه‌های مدیریتی را پیاده‌سازی کرده، که در محدوده قوانین ایجاد شده به عنوان یکی از عناصر موجود در چارچوب حاکمیت که در بردارنده‌ی اصول و تجاربه های مربوط به حاکمیت وواپایش درون سازمان است، عمل کند

پ) الزامات خاص برای واپایشی داخلی باید مبتنی بر دستیابی به اهداف کسب‌وکار و الزامات مقرراتی خارجی باشد.

ت) فعالیت‌های واپایشی متناسب سطح مخاطره، باید به نحوی طراحی شود که خطرهای وابسته به هر فرآیند یا پروژه که می‌تواند روی توانایی سازمان در حصول اهداف کسب‌وکار خود اثرگذار باشد، را کاهش دهد.

1-Portfolio

ث) سامانه واپایشی داخلی باید از یک چارچوب حاکمیتی نشأت گرفته و موارد زیر را دارا باشد:

- تعریف روشنی از مسئولیت‌ها برای فناوری اطلاعات درون سازمان. این شامل مسئولیت‌ها، مرز مسئولیت‌ها، اختیارها، پاسخگویی و ترتیب های مربوط به گزارش‌دهی است؛
- اطلاع‌رسانی اطلاعات مرتبط و قابل اطمینان، به منظور امکان اجرای مناسب مسئولیت‌ها؛
- مدیریت مخاطره برای شناسایی و تحلیل مخاطرات فناوری اطلاعات در ارتباط با دستیابی به خط‌مشی-ها و اهداف تجاری سازمان، به منظور حصول اطمینان از این که رویه‌ها برای مدیریت آن مخاطرات وجود دارد؛ و
- پایش مداوم سامانه واپایش داخلی به همراه بازنگری‌های منظم روشی که واپایش داخلی برای فناوری اطلاعات در حال اجرا است.

پیوست الف

(اطلاعاتی)

اصول حاکمیت خوب فناوری اطلاعات

استاندارد ISO/IEC 38500، شش اصل را برای حاکمیت خوب فناوری اطلاعات به طور کلی بیان می‌کند. این اصول برای بیشتر سازمان‌ها قابل اجرا است. این پیوست، این اصول را فهرست کرده و جزئیات پایه‌ای را ارائه می‌کند. برای کسب اطلاعات بیشتربه استاندارد ISO/IEC 38500 مراجعه شود.

این اصول رفتارهای برتر را به منظور هدایت فرآیند تصمیم‌گیری بیان می‌کند. بیان هر کدام از این اصول، اشاره به آن چیزی دارد که باید انجام پذیرد اما تجویز نمی‌کند این اصول چگونه، چه زمانی و یا توسط چه کسی، پیاده‌سازی خواهد شد؛ چرا که این ابعاد وابسته به ماهیت سازمانی است که این اصول را پیاده‌سازی می‌کند. نهاد حکمرانی باید درخواست کند که این اصول اعمال شود.

اصل ۱- مسئولیت‌پذیری

افراد و گروه‌ها در سازمان، مسئولیت‌های خود را هم تامین و هم تقاضا برای فناوری اطلاعات درک کرده و می‌پذیرند. افراد دارای مسئولیت اقدام، اختیار اجرای این اقدام‌ها را دارند.

اصل ۲- راهبرد

راهبرد کسب‌وکار سازمان، قابلیت‌های آتی و فعلی فناوری اطلاعات و طرح‌های راهبردی برای فناوری اطلاعات به منظور برآورده کردن نیازهای جاری و مداوم راهبرد کسب‌وکار سازمان را مد نظر قرار می‌دهد.

اصل ۳- اکتساب

اکتساب‌های فناوری اطلاعات به دلایل معتبری بر مبنای تحلیل مقتضی و پیوسته و با تصمیم‌گیری‌های شفاف و روشن انجام می‌شود. توازن مناسبی بین مزایا، فرصت‌ها، هزینه‌ها و مخاطرها در کوتاه مدت و بلند مدت وجود دارد.

اصل۴- کارکرد

فناوری اطلاعات برای هدف پشتیبانی از سازمان در ارائه خدمت، سطوح خدمت و کیفیت خدمت به منظور تحقق الزامات جاری و آتی کسب‌وکار، متناسب شده است.

اصل۵- انطباق

فناوری اطلاعات با تمام مقررات و قوانین اجباری انطباق دارد. خط‌مشی‌ها و تجارب به روشنی تعریف، پیاده سازی واجبار شده است.

اصل ۶- رفتار انسانی

خط‌مشی‌ها، تجارب و تصمیم‌های حوزه‌ی فناوری اطلاعات، نشان‌دهنده‌ی احترام بـه رفتـار انسـانی، شـامل نیازهای جاری و در حال تکوین تمام افراد دخیل در فرآیند است.