# چک لیست ممیزی سیستم مدیریت امنیت اطلاعات (ISMS)

## مبتنی بر استاندارد ISO/IEC 27001:2013


## راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات

تألیف:

محمد مهدی واعظی نژاد

انتشارات آتی‌نگر

.

.

# چک لیست ممیزی سیستم مدیریت

# امنیت اطلاعات (ISMS)

## مبتنی بر استاندارد ISO/IEC 27001:2013

راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات


تألیف:

محمد مهدی واعظی نژاد

مدیر تولید و ناظر چاپ: حسین رعدشندی صفحه‌آرایی: همتا بیداریان
طراحی جلد: فاطمه نژادعباسی

# چک‌لیست ممیزی سیستم مدیریت امنیت اطلاعات (ISMS)
# مبتنی بر استاندارد ISO/IEC 27001:2013
# راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات

مؤلف: محمد مهدی واعظی‌نژاد
ناشر: انتشارات آتی‌نگر
چاپ اول، ۱۳۹۵
شمارگان: ۱۰۰۰ نسخه
قیمت: ۱۸۰,۰۰۰ ریال
شابک: ۱-۲۰-۷۶۳۱-۶۰۰-۹۷۸
ISBN: 978-600-7631-20-1



**نشانی دفتر فروش:** خیابان جمالزاده جنوبی، روبه‌روی کوچه رشتچی، پلاک ۱۴۴، واحد ۲
**تلفن:** ۸-۶۶۵۶۵۳۳۶- ۰۹۳۶۰۸۹۵۸۴۸ نمابر: ۶۶۵۶۵۳۳۷
www.ati-negar.com*info@ati-negar.com

واعظی‌نژاد، محمد مهدی، ۱۳۶۱-
چک‌لیست ممیزی سیستم مدیریت امنیت اطلاعات (ISMS)- مبتنی بر استاندارد ISO/IEC 27001:2013 (راهنمای عملی و کاربردی ممیزی سیستم مدیریت امنیت اطلاعات)/
مؤلف: محمد مهدی واعظی‌نژاد. - تهران: آتی‌نگر، ۱۳۹۵
۲۷۲ص.: مصور، جدول، نمودار.
ISBN: 978-600-7631-20-1
فیپا.
موضوع:
رده‌بندی کنگره
رده‌بندی دیویی
شماره کتابشناسی ملی

.

**به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید، از روح خود در او دمید و او را خلیفه خویش بر روی زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.**

تقدیم به ساحت مقدس

حضرت قاسم بن الحسن علیه السلام

.

**نام سازمان / شرکت ممیزی شونده:**

.....

**آدرس:** .....

**تلفن:** ..... **نمابر:** .....

**دامنه ممیزی:** .....

**تاریخ آخرین بازنگری بیانیه کاربست‌پذیری:** .....

**تاریخ انجام ممیزی:** .....

**سرممیز:** .....

**ممیزان:** .....

**کارشناسان فنی:** .....

.

# فهرست مطالب

.

.

# مقدمه

امروزه با گسترش روز افزون فناوری اطلاعات در سازمان‌ها و بهره‌گیری از ابعاد گسترده آن در امر خدمات‌رسانی و حتی تولید محصولات، عنصر ارزشمندی به نام «اطلاعات» در سازمان‌ها پدید آمده است که مهمترین دارایی سازمانی هم به شمار می‌رود. استفاده از فناوری اطلاعات و بهره‌مندی از سیستم‌های ذخیره و پردازش اطلاعات، به عنوان ابزاری قدرتمند، باعث متمایز شدن سازمان‌ها از یکدیگر شده است و آن‌هایی که از این فرصت بی‌بدیل فناورانه توانسته‌اند در زمان مناسب خویش، به بهترین نحو ممکن بهره‌برداری کنند، گوی سبقت را از سایر رقبا ربوده و موجب سودآوری کسب و کار خود شده‌اند. بنابراین در دنیای رقابتی امروز، اطلاعات به عنوان گوهری حیاتی که بقای سازمان‌ها به شدت به آن وابسته است نیازمند راهکارهای حفاظتی مناسب جهت جلوگیری از تخریب، دستکاری، تغییر، حذف یا افشا است.

استاندارد ISO/IEC 27001:2013 زمینه مناسبی را برای بهره‌گیری از این رویکرد و حفاظت از اطلاعات سازمانی فراهم کرده است و به تمام سازمان‌ها با هر حجم، اندازه، ساختار، فرهنگ سازمانی و سطح بلوغی کمک می‌کند با پیاده‌سازی و استقرار سیستم مدیریت امنیت اطلاعات[1]، فرایندهای امنیتی خود را متناسب با الزامات خویش، به نحو مطلوبی بهبود بخشند.

پس از پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان، لازم است انطباق آن با کنترل‌ها و الزامات این استاندارد بین‌المللی بررسی شود تا از کارایی هر چه بهتر و بهبود مستمر این سیستم اطمینان حاصل شود. کتاب حاضر که چک‌لیست ممیزی سیستم مدیریت امنیت اطلاعات است با هدف آشنایی ممیزان با فرایندهای ممیزی این سیستم مدیریتی تدوین شده است و با استانداردهای ISO 19011:2011[2] و ISO/IEC 17021:2011[3] انطباق کامل دارد.

از این کتاب می‌توان برای انجام ممیزی‌های داخلی و شخص سوم (صدور گواهی) سیستم مدیریت امنیت اطلاعات یا هرگونه ارزیابی‌های درون سازمانی استفاده کرد. ممیزان داخلی با استفاده از این کتاب می‌توانند از طریق فرایند خودارزیابی، وضعیت سیستم مدیریت امنیت اطلاعات در حال پیاده‌سازی در سازمان مطبوع خویش را قبل از انجام ممیزی‌های شخص سوم، مورد

1- Information Security Management System (ISMS)
2- Guidelines for auditing management systems
3- Conformity assessment - Requirements for bodies providing audit and certification of management systems

ارزیابی قرار دهند.

در پایان، از تمام ممیزان سیستم مدیریت امنیت اطلاعات، کارشناسان امنیت و خوانندگان گرامی درخواست می‌کنم نظرها و پیشنهادهای اصلاحی یا تکمیلی خود را از طریق ایمیل Info@mvaezi.ir با اینجانب در میان گذارند تا در اصلاح‌های بعدی این کتاب مد نظر قرار گیرد.

***خدایا چنان کن سرانجام کار، تو خشنود باشی و ما رستگار***

**محمد مهدی واعظی نژاد**
**بهار ۱۳۹۵**

.

.

# دستورالعمل استفاده از این چک‌لیست

هدف از تدوین و انتشار عمومی این چک‌لیست، کمک به ممیزان جهت بررسی صحیح میزان انطباق سیستم مدیریت امنیت اطلاعات پیاده‌سازی شده در سازمان‌ها و شرکت‌های کشورمان با کنترل‌ها و الزامات استاندارد ISO/IEC 27001:2013 و همچنین صرف کمترین هزینه مالی (فقط هزینه خرید این کتاب!) برای انجام خودارزیابی‌های درون سازمانی است.

از ممیزان درخواست می‌شود برای تکمیل بندهای این چک‌لیست، وقت کافی را اختصاص دهند و به بهترین وجه، بر اساس موارد مشاهده شده خود و با در نظر گرفتن اصول بی‌طرفی و استقلال، به سؤال‌ها پاسخ دهند.

ممیزان برای انجام یک ممیزی اصولی و قاعده‌مند، ابتدا لازم است برنامه ممیزی که یک نمونه از آن در بخش صفر – جدول ۱ آمده است را با راهنمایی سازمان ممیزی شونده تکمیل کرده، سپس ضمن بررسی مستندات الزامی استاندارد (بخش اول – جدول ۲)، الزامات کلیدی سیستم مدیریت امنیت اطلاعات که در بخش اول – جدول ۳ آمده است را مورد ارزیابی قرار دهند (ممیزی مرحله اول: بررسی مستندات[1]). پس از این مراحل، چنانچه سازمان یا شرکت ممیزی شونده، به تشخیص سرممیز از شرایط لازم برای ادامه ممیزی برخوردار باشد، کنترل‌های کلیدی استاندارد ISO/IEC 27001:2013 که در بخش دوم – جدول ۴ آمده است، مورد بررسی قرار می‌گیرند (ممیزی مرحله دوم: بازدید محلی[2]).

پس از تکمیل تمامی جداول این کتاب و تأیید آن توسط سرممیز و نیز برطرف‌سازی همه عدم انطباق‌های اصلی[3] و جزئی[4] شناسایی شده، سازمان یا شرکت ممیزی شونده دارای شرایط دریافت گواهینامه سیستم مدیریت امنیت اطلاعات است و می‌تواند از طریق مراکز صدور گواهی[5] این سیستم مدیریتی، اقدام به درخواست ممیزی شخص سوم و صدور گواهی آن برای سازمان خود کند.

1- Document Reviwe
2- Site Visit
3- Major
4- Minor
5- Certification Body (CB)

.

.

# بخش دوم

## ممیزی مرحله دوم یا بازدید محلی

## کنترل‌های کلیدی پیوست الف استاندارد

کنترل‌های کلیدی پوشش داده شده توسط استاندارد ISO/IEC 27001:2013، مشتمل بر ۱۱۴ کنترل است که در ۱۴ بند و ۳۵ هدف کنترلی دسته‌بندی شده‌اند. این کنترل‌ها شامل بندهای زیر است که باید در بیانیه کاربست‌پذیری درج شده و توسط مدیر ارشد صحه‌گذاری شود. در صورت عدم رعایت هر یک از این موارد، ممیزی شونده دارای عدم انطباق جزئی بوده و بر اساس نظر ممیز ارشد در خصوص آن عدم انطباق(ها)، تصمیم‌گیری می‌شود:

- *پیوست الف: اهداف کنترلی و کنترل‌ها*
  - *الف ۵: خط‌مشی‌های امنیت اطلاعات*
    - الف۱.۵: هدایت مدیریت برای امنیت اطلاعات
  - *الف ۶: سازمان امنیت اطلاعات*
    - الف ۱.۶: سازمان داخلی
    - الف ۲.۶: دستگاه‌های قابل حمل و دورکاری
  - *الف ۷: امنیت منابع انسانی*
    - الف ۱.۷: پیش از اشتغال
    - الف ۲.۷: حین خدمت
    - الف ۳.۷: خاتمه اشتغال یا تغییر شغل
  - *الف ۸: مدیریت دارایی‌ها*
    - الف ۱.۸: مسئولیت دارایی‌ها
    - الف ۲.۸: طبقه‌بندی اطلاعات
    - الف ۳.۸: اداره کردن رسانه‌ها
  - *الف ۹: کنترل دسترسی*
    - الف ۱.۹: الزامات کسب و کار برای کنترل دسترسی
    - الف ۲.۹: مدیریت دسترسی کاربر
    - الف ۳.۹: مسئولیت‌های کاربر
    - الف ۴.۹: کنترل دسترسی به سیستم و برنامه
  - *الف ۱۰: رمزنگاری*
    - الف ۱.۱۰: کنترل‌های رمزنگاری
  - *الف ۱۱: امنیت فیزیکی و محیطی*
    - الف ۱.۱۱: نواحی امن

- الف ۲.۱۱: تجهیزات
- *الف ۱۲: امنیت عملیات*
  - الف ۱.۱۲: رویه‌های عملیاتی و مسئولیت‌ها
  - الف ۲.۱۲: حفاظت در برابر بدافزارها
  - الف ۳.۱۲: پشتیبان‌گیری
  - الف ۴.۱۲: واقعه‌نگاری و پایش
  - الف ۵.۱۲: کنترل نرم افزارهای عملیاتی
  - الف ۶.۱۲: مدیریت آسیب‌پذیری فنی
  - الف ۷.۱۲: ملاحظات ممیزی سیستم‌های اطلاعاتی
- *الف ۱۳: امنیت ارتباطات*
  - الف ۱.۱۳: مدیریت امنیت شبکه
  - الف ۲.۱۳: انتقال اطلاعات
- *الف ۱۴: اکتساب، توسعه و نگهداری از سیستم*
  - الف ۱.۱۴: الزامات امنیتی سیستم‌های اطلاعاتی
  - الف ۲.۱۴: امنیت در فرایندهای توسعه و پشتیبانی
  - الف ۳.۱۴: داده‌های آزمون
- *الف ۱۵: روابط تأمین کنندگان*
  - الف ۱.۱۵: امنیت اطلاعات در روابط با تأمین کنندگان
  - الف ۲.۱۵: مدیریت تحویل خدمت تأمین کنندگان
- *الف ۱۶: مدیریت رخدادهای امنیت اطلاعات*
  - الف ۱.۱۶: مدیریت و بهبود رخدادهای امنیت اطلاعات
- *الف ۱۷: جوانب امنیت اطلاعات در مدیریت تداوم کسب و کار*
  - الف ۱.۱۷: تداوم امنیت اطلاعات
  - الف ۲.۱۷: افزونگی‌ها
- *الف ۱۸: انطباق*
  - الف ۱.۱۸: انطباق با الزامات قانونی و قراردادی
  - الف ۲.۱۸: بازنگری‌های امنیت اطلاعات

**تذکر ۱:** سؤال‌های ممیزی هر یک از کنترل‌های مربوط به بندها و زیربندهای بالا، در همین بخش – جدول ۴ آمده است.

**تذکر ۲:** چنانچه به تشخیص سرممیز، پس از تکمیل جدول ۳ (در بخش اول)، سازمان یا شرکت ممیزی شونده از شرایط لازم برای ادامه ممیزی برخوردار نباشد، فرایند ممیزی در این مرحله خاتمه یافته و نباید جدول ۴ تکمیل شود.

**یادآوری:** این چک‌لیست پس از تکمیل آن، به وضعیت *خیلی محرمانه* تغییر می‌کند.

| د / کنترل استاندارد | سؤال ممیزی |
|---|---|
| **الف.۹** | **کنترل دسترسی** |
| **الف.۱.۹** | **الزامات کسب و کار برای کنترل دسترسی**<br>*هدف: محدودسازی دسترسی به اطلاعات و امکانات پردازش اطلاعات.* |
| **الف.۱.۱.۹** | **خط‌مشی کنترل دسترسی** |
| 02C01-01 | آیا یک خط‌مشی مدیریت کنترل دسترسی به محدوده سازمانی، بر مبنای تجزیه و تحلیل نیازمندی‌های امنیتی هر نوع از مخاطرات کسب و کار ایجاد شده است؟ |
| 05B01-01 | آیا یک خط‌مشی مدیریت کنترل دسترسی به شبکه محلی، بر مبنای تجزیه و تحلیل نیازمندی‌های امنیتی هر نوع از مخاطرات کسب و کار ایجاد شده است؟ |
| 06C01-01 | آیا یک خط‌مشی مدیریت کنترل دسترسی ویژه به تجهیزات شبکه، بر مبنای تجزیه و تحلیل نیازمندی‌های امنیتی هر نوع از مخاطرات کسب و کار ایجاد شده است؟ |
| 07A01-01 | آیا یک خط‌مشی مدیریت کنترل دسترسی به سیستم‌ها، بر مبنای تجزیه و تحلیل نیازمندی‌های امنیتی هر نوع از مخاطرات کسب و کار ایجاد شده است؟ |
| 09A01-01 | آیا یک خط‌مشی مدیریت کنترل دسترسی به داده‌ها و اطلاعات، بر مبنای تجزیه و تحلیل نیازمندی‌های امنیتی هر نوع از مخاطرات کسب و کار ایجاد شده است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| **الف.۹** | **کنترل دسترسی** |
| **الف.۱.۹** | **الزامات کسب و کار برای کنترل ...**<br>*هدف: محدودسازی دسترسی به اطلاعات و امکانات پردازش اطلاعات.* |
| **الف.۱.۱.۹** | **خط‌مشی کنترل دسترسی** |
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| ISO-9.1.1-01 | آیا یک خط‌مشی کنترل دسترسی، بر مبنای الزامات کسب و کار و اصول امنیتی، ایجاد، مدون و بازنگری شده است؟ |
| **الف.۹.۱.۲** | **دسترسی به شبکه‌ها و سرویس‌های شبکه** |
| 01B02-05 | آیا سندی برای تعریف قوانین کلی استفاده از منابع محاسباتی (شبکه، سرور و غیره) و تجهیزات ارتباطی وجود دارد؟ |
| ISO-9.1.2-01 | آیا کاربران فقط به شبکه و سرویس‌هایی از شبکه که مشخصاً استفاده از آنها برایشان مجاز است، دسترسی دارند؟ |
| **الف.۹.۲** | **مدیریت دسترسی کاربر**<br>*هدف: حصول اطمینان از دسترسی کاربر مجاز شده و جلوگیری از دسترسی غیرمجاز به سیستم‌ها و سرویس‌ها.* |
| **الف.۹.۲.۱** | **ثبت و حذف کاربر** |
| 01C06-01 | آیا رویه‌هایی برای استخدام رسمی و فسخ آن برای افراد وجود دارد؟ |
| 01C06-02 | آیا این رویه‌ها مدیران و سلسله مراتب سازمانی را هم شامل می‌شود؟ |
| 01C06-03 | آیا یک شناسه یکتا به هر کاربر (کارمند، کاربر بیرونی و غیره) که می‌تواند به اطلاعات سیستم دسترسی داشته باشد، اختصاص داده شده است؟ |
| 01C06-04 | آیا حقوق دسترسی واگذار شده به کاربران در هنگام استخدام (خدمات مشترک، پیام‌رسانی و غیره) به تأیید مالکان دارایی‌های مربوطه رسیده است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| **الف.۲.۱.۹** | **دسترسی به شبکه‌ها و ...** |
| | |
| | |
| **الف.۲.۹** | **مدیریت دسترسی کاربر** |
| | *هدف: حصول اطمینان از دسترسی کاربر مجاز شده و جلوگیری از دسترسی غیرمجاز به سیستم‌ها و سرویس‌ها.* |
| **الف.۱.۲.۹** | **ثبت و حذف کاربر** |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| 01C06-05 | آیا تمام کاربران در هنگام استخدام، از حقوق دسترسی واگذار شده (در زمان استخدام یا پس از آن) و وظایف خویش در این خصوص آگاه شده‌اند؟ |
| 01C06-06 | آیا رویه‌های واگذاری حقوق دسترسی، کنترل شده‌اند و آیا نقص‌های احتمالی، ثبت شده و در زمان کوتاهی اصلاح می‌شوند؟<br>رویه‌های استثنا در این خصوص که ممکن است از تأخیر در پروسه استخدام ناشی شود باید توسط مدیریت سازمان ممنوع شود. |
| 07A04-01<br>09A04-01 | آیا هر گونه دسترسی به سیستم‌ها نیازمند شناسه‌ای است که توسط آن سیستم، به رسمیت شناخته شده باشد؟ |
| 09A04-02 | آیا مطابقت مستقیم یا غیرمستقیم بین هر شناسه و فرد حقیقی وجود دارد؟<br>هنگامی که یک برنامه خواستار اجرای برنامه‌ای دیگر یا یک درخواست سیستمی است، ممکن است برنامه به سیستم مورد نظری که در اصل، درخواست را مطرح کرده، انتقال نیابد. ارتباط بین درخواست، شناسه و کاربر باید پس از این ماجرا قابل ردگیری باقی بماند. |
| 07A04-03<br>09A04-03 | آیا همه حساب‌های کاربری عمومی یا پیش فرض حذف شده‌اند؟ |
| 07A04-04<br>09A04-04 | آیا پذیرش شناسه توسط سیستم، وابسته به احراز هویت آن شناسه است؟<br>به منظور احراز هویت نظام‌مند لازم است روند انجام این کار برای تمام زیرسیستم‌ها (نظارت بر فرایندهای |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| | از راه دور، سیستم‌های مدیریت پایگاه داده و غیره)، جهت تمام درخواست‌های برنامه‌ها و برای همه مسیرهای دسترسی، از جمله پورت‌های رزرو شده برای تعمیر و نگهداری از راه دور اجرا شده باشد. |
| ISO-9.2.1-01 | آیا یک رویه رسمی ثبت و حذف کاربر برای اعطا یا لغو دسترسی کاربران به سیستم‌ها و خدمات اطلاعاتی وجود دارد؟ |
| ISO-9.2.1-02 | آیا تمام کاربران، یک شناسه کاربری یکتا برای استفاده شخصی‌شان دارند؟ |
| ISO-9.2.1-03 | آیا یک فرایند مناسب احراز اصالت، به منظور اثبات هویت ادعا شده کاربر، ایجاد و پیاده‌سازی شده است؟ |
| **الف.۹.۲.۲** | **تأمین مجوز دسترسی کاربر** |
| ISO-9.2.2-01 | آیا یک رویه رسمی برای تأمین مجوز دسترسی کاربران، جهت اعطا یا لغو حقوق دسترسی به تمام سیستم‌ها و خدمات اطلاعاتی ایجاد و پیاده‌سازی شده است؟ |
| **الف.۹.۲.۳** | **مدیریت حق دسترسی ویژه** |
| 05B01-02 | آیا خط‌مشی مدیریت حق دسترسی ویژه که به تأیید مدیران مسئول رسیده است، ایجاد شده و به طور منظم مورد بازنگری قرار می‌گیرد؟ |
| 05B02-03 | آیا رویه اعطا، اصلاح یا لغو مجوز دسترسی شبکه محلی به یک فرد (چه به صورت مستقیم یا از طریق پروفایل آن شخص) به شدت کنترل می‌شود؟<br>یک کنترل سختگیرانه، نیازمند به رسمیت شناختن امضای (الکترونیکی یا نوع دیگر) درخواست کننده است که پیاده‌سازی نمایه نسبت داده شده به کاربران در قالب جداول، در زمان انتقال و ذخیره‌سازی بسیار |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |
| **الف.۲.۲.۹** | **تأمین مجوز دسترسی کاربر** |
| | |
| **الف.۳.۲.۹** | **مدیریت حق دسترسی ویژه** |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| | امن باشد و یک کنترل دسترسی تقویت شده‌ای وجود داشته باشد که هر گونه تغییر یا تعدیل در این اسناد، ثبت شده و حسابرسی شوند. |
| 06C01-03 | آیا نمایه‌ها به عنوان بخشی از عملیات شبکه، مرتبط با هر نوع فعالیتی (مدیریت سیستم، مدیریت تجهیزات امنیتی، مدیریت شبکه، مدیریت رسانه‌های ذخیره‌ساز داده‌ها و نسخه‌های پشتیبان و غیره) ایجاد شده‌اند؟ |
| 06C01-07<br>08F01-05<br>11E01-05<br>12E01-05 | آیا روند اعطا، اصلاح یا ابطال حق دسترسی ویژه به یک فرد، به شدت کنترل می‌شود؟<br>یک کنترل سختگیرانه، نیازمند به رسمیت شناختن امضای (الکترونیکی یا نوع دیگر) درخواست کننده است و یک کنترل دسترسی به منظور اعطا یا تغییر چنین حقوقی را نیاز دارد و این که هر گونه اصلاح حقوق ویژه، ثبت شده و حسابرسی شود. |
| 07A01-02 | آیا دسترسی به بخش‌های مختلف سیستم اطلاعاتی (برنامه‌های کاربردی، پایگاه‌های داده، سیستم‌ها، تجهیزات و غیره) بر اساس نمایه‌های شغلی که نقش‌ها یا وظایف درون سازمانی را شامل می‌شود (نمایه‌هایی که حقوق دسترسی دارندگان آن نمایه را تعریف می‌کند)، امکان‌پذیر است؟<br>توجه: در شرایط خاص، مفهوم «نمایه» ممکن است با مفهوم «گروه» جایگزین شود. |
| 07A02-03<br>09A02-03 | آیا روند اعطا، اصلاح یا ابطال حق دسترسی به یک فرد (چه به صورت مستقیم یا از طریق نمایه آن شخص)، به شدت کنترل می‌شود؟<br>یک کنترل سختگیرانه، نیازمند به رسمیت شناختن امضای (الکترونیکی یا نوع دیگر) درخواست کننده |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| | است که پیاده‌سازی نمایه نسبت داده شده به کاربران در قالب جداول، در زمان انتقال و ذخیره‌سازی بسیار امن باشد و یک کنترل دسترسی تقویت شده‌ای وجود داشته باشد که هر گونه تغییر یا تعدیل در این اسناد، ثبت شده و حسابرسی شود. |
| 08F01-01 | آیا نمایه‌هایی برای کارکنان عملیات فناوری اطلاعات، مرتبط با هر نوع فعالیتی (مدیریت سیستم، مدیریت تجهیزات امنیتی، سیستم کنترلی، مدیریت رسانه‌های ذخیره‌ساز داده‌ها و نسخه‌های پشتیبان و غیره)، تعریف شده است؟ |
| 09A01-02 | آیا دسترسی به برنامه‌های کاربردی و داده‌های مرتبط با آنها، بر اساس نمایه‌های شغلی که نقش‌ها یا وظایف درون سازمانی را شامل می‌شود (یک نمایه حقوقی، امکان دسترسی برای دارندگان آن نمایه را تعریف می‌کند)، امکان‌پذیر است؟<br>توجه: در شرایط خاص، مفهوم «نمایه» ممکن است با مفهوم «گروه» جایگزین شود. |
| 11E01-01 | آیا نمایه‌های برای کارکنان و کاربران عملیات ایستگاه‌های کاری، مرتبط با هر نوع فعالیتی (کمک، نصب و راه‌اندازی، تعمیر و نگهداری و غیره)، تعریف شده است؟ |
| 12E01-01 | آیا نمایه‌هایی برای کارکنان عملیات ارتباطات، مرتبط با هر نوع فعالیتی (مدیریت سیستم، مدیریت تجهیزات امنیتی، سیستم کنترلی، مدیریت رسانه‌های ذخیره‌ساز داده‌ها و نسخه‌های پشتیبان و غیره) تعریف شده است؟ |
| ISO-9.2.3-01 | آیا تخصیص و استفاده از حق دسترسی ویژه، محدود و کنترل شده است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| **الف.۹.۲.۴** | **مدیریت اطلاعات محرمانه احراز هویت کاربران** |
| 05B03-02<br>07A03-02<br>09A03-02<br>11B01-02 | آیا فرایند تعریف یا اصلاح اعتبارنامه یک کاربر، بر پایه قوانینی است که اعتبار اولیه آن را تضمین کند؟<br>در مورد کلمه عبور: داشتن طول کافی (۸ حرف یا بیشتر)، لزوم ترکیبی از انواع حروف و نویسه‌ها، تغییر مکرر (یک بار در ماه)، عدم امکان استفاده دوباره از رمزهای عبور قبلی، استفاده نکردن از کلمه‌های ساده، ممنوع بودن استفاده از سیستم‌های استاندارد و نام اشخاص، ترکیبی از نام کاربری، تاریخ و غیره.<br>در مورد گواهینامه و احراز هویت بر اساس سازوکارهای رمزنگاری: قابل ارزیابی نبودن فرایند تولید کلید یا به طور عمومی ناشناخته بودن آن، کلید با طول کافی و غیره. |
| ISO-9.2.4-01 | آیا تخصیص اطلاعات محرمانه احراز هویت، از طریق یک فرایند رسمی مدیریتی کنترل می‌شود؟ |
| **الف.۹.۲.۵** | **بازنگری حقوق دسترسی کاربر** |
| 05B01-08<br>07A01-08<br>07A02-08<br>09A01-08 | آیا حسابرسی منظمی (حداقل یک بار در سال) از حقوق دسترسی هر یک از نمایه‌ها و رویه‌های مدیریتی آنها انجام می‌شود؟ |
| 05B02-04<br>07A02-04<br>09A02-04 | آیا یک فرایند نظام‌مند برای به روز رسانی حقوق دسترسی کارکنان (اعم از داخلی یا خارجی)، در هنگام خاتمه اشتغال آنها وجود دارد؟ |
| 05B02-05<br>07A02-05<br>09A02-05 | آیا یک فرایند نظام‌مند برای به روز رسانی حقوق دسترسی کارکنان، در زمان تغییر شغل آنها وجود دارد (در هنگام خاتمه قرارداد کارکنان خارجی یا تغییر شغل کارمندان داخلی)؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| الف.۴.۲.۹ | مدیریت اطلاعات محرمانه احراز هویت کاربران |
| | |
| | |
| الف.۵.۲.۹ | بازنگری حقوق دسترسی کاربر |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| 05B02-07 | آیا حسابرسی منظمی (حداقل یک بار در سال) از حقوق دسترسی کارکنان و سایر کاربران، به شبکه محلی انجام می‌شود؟ |
| 06C01-08 | آیا یک فرایند نظام‌مند برای حذف حقوق مدیریتی، در هنگام خاتمه اشتغال یا تغییر شغل کارکنان وجود دارد؟ |
| 06C01-09 | آیا حسابرسی منظمی (حداقل یک بار در سال) از تمام حقوق مدیریتی اختصاص یافته انجام می‌شود؟ |
| 06C02-07 | آیا حسابرسی منظمی از نمایه‌هایی که حقوق مدیریتی دارند، انجام می‌شود؟ |
| 08F01-06<br>11E01-06 | آیا یک فرایند نظام‌مند برای حذف حقوق ویژه، در هنگام خاتمه اشتغال یا تغییر شغل کارکنان عملیات فناوری اطلاعات وجود دارد؟ |
| 08F01-07<br>11E01-07<br>12E01-08 | آیا حسابرسی منظمی (حداقل یک بار در سال) از تمام حقوق ویژه نسبت داده شده انجام می‌شود؟ |
| 08F02-06 | آیا حسابرسی منظمی از نمایه‌هایی که حقوق ویژه و مؤثری دارند، انجام می‌شود؟ |
| 09A02-08 | آیا حسابرسی منظمی (حداقل یک بار در سال) از نمایه‌ها و مجوزهای اعطا شده به تمام کاربران و رویه‌های مدیریتی آنها انجام می‌شود؟ |
| 12E01-06 | آیا یک فرایند نظام‌مند برای حذف حقوق ویژه، در هنگام خاتمه اشتغال کارکنان عملیات ارتباط از راه دور وجود دارد؟ |
| 12E01-07 | آیا یک فرایند نظام‌مند برای حذف حقوق ویژه، در هنگام تغییر شغل کارکنان عملیات ارتباط از راه دور وجود دارد؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| ISO-9.2.5-01 | آیا مدیریت، حقوق دسترسی کاربران را با استفاده از یک فرایند رسمی، در فاصله‌های زمانی منظم بازنگری می‌کند؟ |
| **الف.۹.۲.۶** | **حذف یا اصلاح حقوق دسترسی** |
| 01B01-10 | آیا یک رویه (یا سندی معادل آن) برای حذف یا اصلاح حقوق دسترسی به همه قسمت‌های سیستم اطلاعاتی وجود دارد؟ |
| ISO-9.2.6-01 | آیا حقوق دسترسی تمام کارکنان، پیمانکاران و کاربران شخص سوم به اطلاعات و امکانات پردازش اطلاعات، به محض خاتمه اشتغال، قرارداد یا توافق‌نامه‌شان حذف شده یا در صورت تغییر وضعیت، اصلاح می‌شود؟ |
| **الف.۹.۳** | **مسئولیت‌های کاربر** |
| | *هدف: پاسخگو بودن کاربران در برابر حفاظت از اطلاعات احراز هویت خود.* |
| **الف.۹.۳.۱** | **استفاده از اطلاعات محرمانه احراز هویت** |
| 01B01-02 | آیا سندی که وظایف و مسئولیت‌های کارکنان در خصوص استفاده و حفاظت از ابزارهای احراز هویت (کلمه عبور، کلیدها، توکن‌ها (علامت‌های رمزی)، نشانه‌ها و غیره) را مشخص کند، تدوین شده است؟ |
| ISO-9.3.1-01 | آیا کاربران در انتخاب و استفاده از اطلاعات محرمانه احراز هویت، از شیوه‌های امنیتی صحیحی که به آن ملزم شده‌اند، پیروی می‌کنند؟ |
| **الف.۹.۴** | **کنترل دسترسی به سیستم و برنامه** |
| | *هدف: جلوگیری از دسترسی غیرمجاز به سیستم‌ها و برنامه‌ها.* |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| **الف.۹.۲.۶** | **حذف یا اصلاح حقوق دسترسی** |
| | |
| | |
| **الف.۹.۳** | **مسئولیت‌های کاربر** |
| | *هدف: پاسخگو بودن کاربران در برابر حفاظت از اطلاعات احراز هویت خود.* |
| **الف.۹.۳.۱** | **استفاده از اطلاعات محرمانه ...** |
| | |
| | |
| **الف.۹.۴** | **کنترل دسترسی به سیستم و ...** |
| | *هدف: جلوگیری از دسترسی غیرمجاز به سیستم‌ها و برنامه‌ها.* |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| **الف.۹.۴.۱** | **محدودیت دسترسی به اطلاعات** |
| 09A01-02 | آیا دسترسی به برنامه‌های کاربردی و داده‌های مرتبط با آنها، بر اساس نمایه‌های شغلی که نقش‌ها یا وظایف درون سازمانی را شامل می‌شود (یک نمایه حقوقی، امکان دسترسی برای دارندگان آن نمایه را تعریف می‌کند)، امکان‌پذیر است؟<br>توجه: در شرایط خاص، مفهوم «نمایه» ممکن است با مفهوم «گروه» جایگزین شود. |
| 09A02-01 | آیا رویه اعطای مجوز دسترسی به برنامه‌های کاربردی، نیاز به مجوز رسمی از مدیریت ارشد (در یک سطح اعتبار بالا) دارد؟ |
| 09A02-02 | آیا مجوزها تنها به عنوان یک کارکرد از نمایه، فقط برای افراد مربوطه صادر می‌شود؟ |
| 09A04-01 | آیا هر گونه دسترسی به سیستم‌ها نیازمند شناسه‌ای است که توسط آن سیستم، به رسمیت شناخته شده باشد؟ |
| 09A04-02 | آیا مطابقت مستقیم یا غیرمستقیم بین هر شناسه و فرد حقیقی وجود دارد؟<br>هنگامی که یک برنامه خواستار اجرای برنامه‌ای دیگر یا یک درخواست سیستمی است، ممکن است برنامه به سیستم مورد نظری که در اصل، درخواست را مطرح کرده، انتقال نیابد. ارتباط بین درخواست، شناسه و کاربر باید پس از این ماجرا قابل ردگیری باقی بماند. |
| 09A04-07 | آیا کنترل دسترسی به برنامه‌های کاربردی که بتواند امکان مشاهده و دسترسی به اطلاعات بسیار حساس را محدود کند، انجام شده است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| الف.۱.۴.۹ | محدودیت دسترسی به اطلاعات |
| | |
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| ISO-9.4.1-01 | آیا دسترسی کاربران و کارکنان پشتیبانی کننده به اطلاعات و کارکردهای سیستم‌های کاربردی، مطابق با خط‌مشی کنترل دسترسی، محدود شده است؟ |
| **الف.۹.۴.۲** | **رویه‌های ورود امن** |
| 07A03-03 | آیا فرایند ارایه رمز عبور به کاربران، امنیت آن را تضمین می‌کند؟<br>استفاده از رمز عبور همیشه یک نقطه ضعف است. تنها فرایندی که اطلاعات قابل مشاهده را افشا نمی‌کند استفاده از یک شیء حاوی راز (کارت هوشمند) یا وارد کردن یک کد عبور که در هر لحظه تغییر می‌کند (کارت رمزدار امن) یا استفاده از ویژگی‌های زیست‌سنجی است. |
| 07A03-04 | آیا فرایند ورود به سیستم، امن است؟<br>ورود امن به سیستم باید به گونه‌ای باشد که قبل از وارد کردن رمز عبور، هیچ گونه اطلاعاتی را نمایش ندهد، تاریخ و زمان آخرین اتصال را نشان دهد، تلاش برای ورودهای ناموفق احتمالی را به کاربر اطلاع دهد و غیره. |
| 07A03-05 | آیا سازوکارهایی برای حفظ و استفاده از اعتبارنامه به وسیله کاربران (یا توسط تجهیزات، به نمایندگی از کاربران) وجود دارد یا توسط سیستم مربوطه‌ای، ایمنی و صحت این اعتبارنامه تضمین می‌شود؟<br>رمز عبور باید به صورت رمز شده، ذخیره شود و کنترل دسترسی اولیه‌ای قبل از دسترسی کاربر، ایجاد شده باشد.<br>در مورد احراز هویت با استفاده از روش‌های رمزنگاری، سازوکار آن باید توسط یک سازمان که به رسمیت شناخته شده است، ارایه شود. |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| **الف.۲.۴.۹** | **رویه‌های ورود امن** |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| 07A03-06 | آیا سازوکار مورد استفاده برای انتقال اعتبارنامه بین کاربران و تجهیزات مربوطه، ایمنی و صحت این اعتبارنامه را تضمین می‌کند؟<br>کلمه عبور باید در هنگام انتقال، رمزنگاری شده یا از الگوریتمی که از یک متغیر در هر انتقال استفاده می‌کند، استفاده شود.<br>در مورد احراز هویت با استفاده از روش‌های رمزنگاری، سازوکار آن باید توسط یک سازمان که به رسمیت شناخته شده است، ارایه شود. |
| 07A03-07 | در مواقعی که چندین بار تلاش برای رمزگشایی با شکست مواجه می‌شود، آیا یک فرایند خودکار وجود دارد که آن شناسه را به طور موقت، باطل کند یا رایانه کاربر را غیرفعال کرده یا روند احراز هویت را کندتر کند تا از هر گونه روال خودکار برای اتصال جلوگیری شود؟ |
| 07A04-06<br>09A04-06 | آیا در صورت عدم وجود ترافیک بعد از یک مدت زمان تعریف شده، باطل‌سازی خودکار نشست کاربر انجام می‌شود و در این صورت، نیاز به شناسایی و احراز هویت دوباره آن کاربر وجود دارد؟ |
| 07A01-04 | آیا در نمایه‌ها محدودیت‌های زمان کاری (همچون ساعت در روز، دوره‌های روزانه در تقویم کاری، تعطیلات آخر هفته، تعطیلات رسمی و غیره) تعریف شده است؟ |
| 07A01-05 | آیا نمایه‌ها و حقوق دسترسی نسبت داده شده به آنها، به عنوان تابعی از عملکرد افراد، توسط مالکان اطلاعات و مأمور امنیت اطلاعات سازمان تأیید شده است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| 09A01-04 | آیا در حقوق دسترسی نمایه‌ها، امکان تعریف محدودیت‌های زمانی و دوره‌ای (همچون ساعت در روز، دوره‌های روزانه در تقویم کاری، تعطیلات آخر هفته، تعطیلات رسمی و غیره) وجود دارد؟ |
| 09A04-05 | آیا امکان بازبینی روند احراز هویت در طول یک نشست، برای تراکنش‌های حساس وجود دارد؟ |
| ISO-9.4.2-01 | آیا دسترسی به سیستم‌ها و برنامه‌ها، در صورت الزام در خط‌مشی کنترل دسترسی، از طریق یک رویه ورود امن، کنترل شده است؟ |
| **الف.۹.۴.۳** | **سیستم مدیریت کلمه عبور** |
| 07A03-01<br>09A03-01 | آیا روند توزیع یا اصلاح اعتبارنامه کاربران تضمین می‌کند که تنها دارندگان یک شناسه، اجازه دسترسی به آن را دارند (مثلاً ارتباطات اولیه محرمانه، تغییر رمز عبور تحت کنترل کاربر و غیره)؟ |
| 07A03-02 | آیا فرایند تعریف یا اصلاح اعتبارنامه یک کاربر، بر پایه قوانینی است که اعتبار اولیه آن را تضمین کند؟<br>در مورد کلمه عبور: داشتن طول کافی (۸ حرف یا بیشتر)، لزوم ترکیبی از انواع حروف و نویسه‌ها، تغییر مکرر (یک بار در ماه)، عدم امکان استفاده دوباره از رمزهای عبور قبلی، استفاده نکردن از کلمه‌های ساده، ممنوع بودن استفاده از سیستم‌های استاندارد و نام اشخاص، ترکیبی از نام کاربری، تاریخ و غیره.<br>در مورد گواهینامه و احراز هویت بر اساس سازوکارهای رمزنگاری: قابل ارزیابی نبودن فرایند تولید کلید یا به طور عمومی ناشناخته بودن آن، کلید با طول کافی و غیره. |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| **الف.۳.۴.۹** | **سیستم مدیریت کلمه عبور** |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| 07A03-03 | آیا فرایند ارایه رمز عبور به کاربران، امنیت آن را تضمین می‌کند؟<br>استفاده از رمز عبور، همیشه یک نقطه ضعف است. تنها فرایندی که اطلاعات قابل مشاهده را افشا نمی‌کند استفاده از یک شیء حاوی راز (کارت هوشمند) یا وارد کردن یک کد عبور که در هر لحظه تغییر می‌کند (کارت رمزدار امن) یا استفاده از ویژگی‌های زیست‌سنجی است. |
| 07A03-04 | آیا فرایند ورود به سیستم، امن است؟<br>ورود امن به سیستم باید به گونه‌ای باشد که قبل از وارد کردن رمز عبور، هیچ گونه اطلاعاتی را نمایش ندهد، تاریخ و زمان آخرین اتصال را نشان دهد، تلاش برای ورودهای ناموفق احتمالی را به کاربر اطلاع دهد و غیره. |
| 07A03-05<br>09A03-04 | آیا سازوکارهایی برای حفظ و استفاده از اعتبارنامه توسط کاربران (یا توسط تجهیزات، به نمایندگی از کاربران) وجود دارد یا توسط سیستم مربوطه‌ای، ایمنی و صحت این اعتبارنامه تضمین می‌شود؟<br>رمز عبور باید به صورت رمز شده، ذخیره شود و کنترل دسترسی اولیه‌ای قبل از دسترسی کاربر، ایجاد شده باشد.<br>در مورد احراز هویت با استفاده از روش‌های رمزنگاری، سازوکار آن باید توسط یک سازمان که به رسمیت شناخته شده است، ارایه شود. |
| 07A03-06<br>09A03-05 | آیا سازوکار مورد استفاده برای انتقال اعتبارنامه بین کاربران و تجهیزات مربوطه، ایمنی و صحت این اعتبارنامه را تضمین می‌کند؟<br>کلمه عبور باید در هنگام انتقال، رمزنگاری شده یا از |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| | الگوریتمی که از یک متغیر در هر انتقال استفاده می‌کند، استفاده شود.<br>در مورد احراز هویت با استفاده از روش‌های رمزنگاری، سازوکار آن باید توسط یک سازمان که به رسمیت شناخته شده است، ارایه شود.<br>در مورد احراز هویت با استفاده از روش‌های رمزنگاری، سازوکار آن باید توسط یک سازمان که به رسمیت شناخته شده است، ارایه شود. |
| 07A03-07<br>09A03-06 | در مواقعی که چندین بار تلاش برای رمزگشایی با شکست مواجه می‌شود، آیا یک فرایند خودکار وجود دارد که آن شناسه را به طور موقت، باطل کند یا رایانه کاربر را غیرفعال کرده یا روند احراز هویت را کندتر کند تا از هر گونه روال خودکار برای اتصال جلوگیری شود؟ |
| 07A03-08<br>09A03-07 | آیا در صورت تغییر یا فراموشی رمز عبور، رویه‌ای وجود دارد که به کاربر اجازه دهد حساب کاربری خود را سریعاً غیرفعال کند؟ |
| 07A03-09<br>09A03-08 | آیا در صورت تغییر یا فراموشی رمز عبور، رویه‌ای وجود دارد که به کاربر اجازه دهد نقش مؤثری در کنترل شناسه کاربری خود داشته باشد؟ |
| 09A03-02 | آیا فرایند تعریف یا اصلاح اعتبارنامه یک کاربر، بر پایه قوانینی است که اعتبار اولیه آن را تضمین کند؟<br>در مورد کلمه عبور: داشتن طول کافی (۸ حرف یا بیشتر)، لزوم ترکیبی از انواع حروف و نویسه‌ها، تغییر مکرر (یک بار در ماه)، عدم امکان استفاده دوباره از رمزهای عبور قبلی، استفاده نکردن از کلمه‌های ساده، ممنوع بودن استفاده از سیستم‌های استاندارد و نام اشخاص، ترکیبی از نام کاربری، تاریخ و غیره. |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| | در مورد گواهینامه و احراز هویت بر اساس سازوکارهای رمزنگاری: قابل ارزیابی نبودن فرایند تولید کلید یا به طور عمومی ناشناخته بودن آن، کلید با طول کافی و غیره. |
| 09A03-03 | آیا فرایند ارایه اعتبارنامه توسط کاربران، امنیت آن را تضمین می‌کند؟<br>استفاده از رمز عبور، همیشه یک نقطه ضعف است. تنها فرایندی که اطلاعات قابل مشاهده را افشا نمی‌کند استفاده از یک شیء حاوی راز (کارت هوشمند) یا وارد کردن یک کد عبور که در هر لحظه تغییر می‌کند (کارت رمزدار امن) یا استفاده از ویژگی‌های زیست‌سنجی است. |
| ISO-9.4.3-01 | آیا سیستم مدیریت کلمه عبور، تعاملی بوده و کیفیت کلمات عبور را تضمین می‌کند؟ |
| **الف.۹.۴.۴** | **استفاده از برنامه‌های کمکی ویژه** |
| 08A02-03 | آیا تمام ابزارها و قابلیت‌های حساس سیستم (مانند مدیریت حقوق دسترسی، مدیریت پیکربندی، پشتیبان‌گیری، کپی‌برداری، سیستم‌های فعال آماده به کار در صورت خرابی تجهیزات اصلی و غیره) به صورت جامعی حسابرسی شده و به طور جداگانه برای هر یک از نمایه‌ها تعریف شده است؟ |
| 08A02-04 | آیا امکان استفاده از ابزارها و قابلیت‌های سودمند مربوطه، فقط برای دارندگان نمایه خاصی و پس از احراز هویت قوی آن (توسط کارت هوشمند یا کارت رمزدار) فراهم می‌شود؟ |
| 08A02-05 | آیا ایجاد یا اضافه کردن ابزار و امکانات جدید، بدون داشتن مجوز رسمی ممنوع است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| الف.۴.۴.۹ | استفاده از برنامه‌های کمکی ویژه |
| | |
| | |
| | |

| بند / کنترل استاندارد | سؤال ممیزی |
|---|---|
| 08A02-06 | آیا روالی به صورت خودکار برای ایجاد هشدارهای مناسب به کاربران و مدیریت وجود دارد؟ |
| 08A02-07 | آیا تفکیک حقوق کارکنان عملیاتی سیستم، از تغییر بی‌مورد ابزارها یا امکانات حساس جلوگیری می‌کند یا حداقل، روال خودکاری وجود دارد که بررسی کند اصلاحی صورت نگیرد یا در صورت رخ دادن هر گونه تغییری به مدیر هشدار دهد؟ |
| ISO-9.4.4-01 | آیا استفاده از برنامه‌های کمکی که ممکن است توانایی ابطال کنترل‌های سیستم و برنامه‌ها را داشته باشند، محدود و به شدت کنترل می‌شود؟ |
| **الف.۹.۴.۵** | **کنترل دسترسی به کد منبع برنامه** |
| 10B02-04 | آیا کد منبع، کد اجرایی و مستندات مربوطه توسط یک رویه کنترل دسترسی شدید، به عنوان تابعی از فاز توسعه حفاظت می‌شوند؟ آیا نمایه‌های مجاز برای دسترسی به آنها و همچنین ذخیره‌سازی‌شان، بر اساس قوانین کنترل دسترسی ایجاد شده است؟<br>یک رویه کنترل دسترسی شدید باید تضمین کند تمام تغییرات در کدها یا اصلاح مستندات، توسط فرد مجاز و در شرایط مجاز ایجاد شود. |
| ISO-9.4.5-01 | آیا دسترسی به کد منبع برنامه، محدود شده است؟ |

| شواهد و یافته‌ها (ذکر موارد رعایت شده) | شرح عدم انطباق / فرصت بهبود (ذکر موارد رعایت نشده) |
|---|---|
| | |
| | |
| | |
| الف.۵.۴.۹ | کنترل دسترسی به کد منبع برنامه |
| | |
| | |