چارچوب قانونی تاب‌آوری عملیاتی دیجیتال

به همراه راهنمای عملی و چک‌لیست‌های کنترلی آن

ترجمه و گردآوری: حسابرسان IT بانک ملت

دیماه ۱۴۰۴

فهرست

به نام آنکه جان را فکرت آموخت

پیشگفتار

تحول دیجیتال در سال‌های اخیر، صنعت خدمات مالی را به‌صورت بنیادین دگرگون ساخته و وابستگی فرآیندهای مالی به زیرساخت‌های فناوری اطلاعات، سامانه‌های نرم‌افزاری و زنجیره‌های پیچیده خدمات دیجیتال را به‌شدت افزایش داده است. در چنین شرایطی، وقوع اختلالات فناورانه، حملات سایبری یا ضعف در مدیریت خدمات فناوری اطلاعات می‌تواند آثار گسترده‌ای بر تداوم خدمات حیاتی، اعتماد مشتریان و ثبات سازمانی داشته باشد. از این رو، "تاب‌آوری عملیاتی دیجیتال" به یکی از مهم‌ترین دغدغه‌های نهادهای مالی، رگولاتورها و متخصصان حوزه فناوری اطلاعات و مدیریت ریسک تبدیل شده است.

در پاسخ به این ضرورت، اتحادیه اروپا قانون تاب‌آوری عملیاتی دیجیتال (**Digital Operational Resilience Act**) یا **DORA** را به‌عنوان نخستین چارچوب جامع و یکپارچه تاب‌آوری عملیاتی دیجیتال در صنعت مالی تدوین و ابلاغ کرده است. این قانون، سازمان‌های مالی را ملزم می‌سازد تا توانمندی خود را در پیشگیری، شناسایی، پاسخ‌گویی، بازیابی و انطباق‌پذیری در برابر اختلالات دیجیتال و رخدادهای سایبری به‌صورت ساختاریافته ارزیابی و تقویت کنند. DORA حوزه‌هایی نظیر مدیریت ریسک فناوری اطلاعات و ارتباطات، مدیریت رخدادها، آزمون‌های تاب‌آوری دیجیتال و مدیریت ریسک اشخاص ثالث فناوری اطلاعات را پوشش می‌دهد.

با وجود جامعیت DORA، این مقرره بیشتر بر بیان الزامات و انتظارات نظارتی تمرکز دارد و جزئیات اجرایی پیاده‌سازی را ارائه نمی‌کند. در همین راستا، مستند **DORA in Control** که توسط موسسه **NOREA** تدوین شده، به‌عنوان راهنمایی کاربردی برای تبدیل الزامات DORA به چک‌لیست‌های کنترلی، فرآیندها و سازوکارهای قابل ارزیابی مورد استفاده قرار می‌گیرد.

ترجمه و تجمیع دو مستند "تاثیر قانون تاب‌آوری عملیاتی دیجیتال (DORA) بر عملکرد حسابرسی داخلی"، و "راهنمای عملی و چک‌لیست‌های کنترلی دستیابی به تاب‌آوری عملیاتی دیجیتال"، در جریان انجام مأموریت حسابرسی فناوری اطلاعات با موضوع "ارزیابی بلوغ تاب‌آوری عملیاتی دیجیتال" در بانک ملت انجام شد. تجربه این مأموریت نشان داد که کمبود منابع فارسی تخصصی در این حوزه، یکی از چالش‌های مهم مدیران، متخصصان و حسابرسان فناوری اطلاعات کشور است. این کتاب با هدف فراهم‌سازی منبعی کاربردی و قابل اتکا برای آشنایی با الزامات DORA و رویکردهای اجرایی DORA in Control تدوین شده و امید است بتواند در ارتقای ادبیات تخصصی و افزایش آمادگی سازمان‌های مالی کشور در برابر تهدیدات و اختلالات دیجیتال مؤثر واقع شود.

در خاتمه لازم می‌دانم از تلاش‌های همکاران گرامی جناب آقای طوبایی، جناب آقای ماموری، جناب آقای اکـرامی، جناب آقای حسینیان، جناب آقای هیوه‌چی و سرکار خانم مهتابی که در برگردان، ویرایش و نظارت بر کیفیت این مجلد کوشش فراوان نمودند تشکر نمایم.

سیّد کاظم چاوشی

نایب رییس هیأت مدیره و رییس کمیته حسابرسی

هدف قانون DORA

قانون تاب‌آوری عملیاتی دیجیتال اتحادیه اروپا[1] بر کارآیی حسابرسی داخلی انجام شده در حوزه مالی تأثیرگذار است؛ چرا که استانداردهای مستقیم و غیرمستقیمی را برای آن تعیین می‌نماید. مهلت مقرر شده برای رعایت الزامات DORA تا تاریخ ۱۷ ژانویه ۲۰۲۵ بوده که تطابق با آن، مؤسسات مالی و تأمین‌کنندگان خدمات، سراسر صنعت را تحت فشار قرار داده است. هدف این مستند، ارائه نمایی کلی از وضعیت شش ماه پیش از تاریخ اجرای این مقررات بر پایه مطالعات صورت‌پذیرفته[2] است و توضیح می‌دهد که کدام فعالیت‌ها می‌بایست به‌طور مستقیم توسط حسابرسی داخلی انجام شود، شرکت‌ها چه اقداماتی را برای انطباق با DORA انجام می‌دهند و نیز شرح می‌دهد که حسابرسی داخلی چگونه می‌تواند اطمینان لازم را در این زمینه فراهم نماید.

دیدگاه‌ها و نظرات بیان‌شده در این مستند لزوماً منعکس‌کننده سیاست یا موضع رسمی هیچ نهاد یا سازمانی در خصوص DORA نمی‌باشد؛ بلکه، اطلاعات ارائه‌شده، تنها به‌عنوان یک نگاه کلی و اطلاع‌رسانی به تأثیرات احتمالی DORA بر عملکرد حسابرسی داخلی است.

خلاصه مدیریتی

DORA یک مقرره از سوی کمیسیون اروپا است که هدف آن تقویت تاب‌آوری عملیاتی دیجیتال در بخش مالی است. این قانون دربرگیرنده موسسات بیمه‌ای هم بوده اما محدود به آن‌ها نمی‌شود؛ موسسات مشمول حوزه مذکور عبارتند از: مؤسسات بیمه و بیمه اتکایی، شرکت‌های فعال در زمینه بیمه و بیمه اتکایی، واسطان صنعت بیمه، بیمه‌های اتکایی و بیمه‌های کمکی و نیز نمایندگان و دلالان بیمه (DORA ماده ۲- دامنه قانون تاب‌آوری عملیاتی دیجیتال). تنها استثنائات مربوط به بیمه در DORA در دستورالعمل (Solvency II) 2009/138/EC ماده ۴ آمده است؛ این استثنائات، تحت شرایط خاصی بیمه‌ها را از شمول DORA مستثنا می‌کنند؛ یکی از این شرایط آن است که حق بیمه ناخالص تکلیفی نباید از ۵ میلیون یورو بیشتر باشد.

هدف DORA ایجاد یک چارچوب مشترک برای مدیریت ریسک فناوری اطلاعات و ارتباطات[3]، گزارش حوادث، آزمون تاب‌آوری، نظارت بر اشخاص ثالث و تبادل اطلاعات است. DORA از پنج رکن تشکیل شده است که هر یک، جنبه‌های مختلف تاب‌آوری عملیاتی دیجیتال را پوشش می‌دهند. رکن اول، مدیریت ریسک فناوری اطلاعات و ارتباطات است و از مؤسسات مالی می‌خواهد یک چارچوب حاکمیتی و کنترل داخلی برای ریسک‌های فاوا پیاده‌سازی کنند. رکن دوم، مدیریت، طبقه‌بندی و گزارش‌دهی حوادث مرتبط با فناوری اطلاعات و ارتباطات است که مؤسسات مالی را موظف می‌سازد، حوادث عمده فاوا را به مقامات ذی‌صلاح گزارش دهند. رکن سوم، آزمون تاب‌آوری عملیاتی دیجیتال است که از مؤسسات مالی می‌خواهد آزمایش‌های منظمی بر روی سیستم‌ها و برنامه‌های فناوری اطلاعات و ارتباطات خود انجام دهند. رکن چهارم، مدیریت ریسک اشخاص ثالث فناوری اطلاعات و ارتباطات است که مقرر می‌سازد مؤسسات مالی بر ریسک‌های ناشی از تأمین‌کنندگان خدمات فاوا ارزیابی و نظارت داشته باشند. رکن پنجم، ملاحظات تبادل اطلاعات است که مؤسسات مالی را تشویق می‌نماید اطلاعات خود را در خصوص بهترین شیوه‌ها و تهدیدات سایبری به اشتراک بگذارند.

در چارچوب مدل سه‌خطی (خط اول: کسب‌وکار، خط دوم: مدیریت ریسک و انطباق، خط سوم: حسابرسی داخلی)، حسابرسی داخلی موظف است بر رعایت تمامی الزامات DORA نظارت داشته باشد و از اجرای کامل وظایف مربوط به خطوط اول و دوم اطمینان حاصل نماید.

به‌طور کلی، نتایج کلیدی این مستند برای حسابرسی داخلی در صنعت مالی به شرح زیر است:

---

[1] Digital Operational Resilience Act (DORA)

[2] تمرکز مورد مطالعه موسسات مالی بیمه‌ای بوده است که از نتایج آن، در بخش دوم این مستند استفاده شده است.

[3] Information and Communication Technology (ICT)

عملکرد حسابرسی داخلی باید برای الزامات مستقیم پیش‌بینی‌شده آماده باشد:

- چارچوب مدیریت ریسک فناوری اطلاعات و ارتباطات باید به‌طور منظم در فعالیت‌های حسابرسی داخلی گنجانده و به‌عنوان بخشی از برنامه حسابرسی قرار گیرد. همچنین، حسابرسان باید دارای مهارت‌های لازم برای انجام این وظایف باشند. ضروری است، فرآیند پیگیری نتایج حسابرسی تضمین‌کننده اصلاح به‌موقع و تأیید یافته‌های بحرانی حسابرسی فناوری اطلاعات و ارتباطات باشد.
- برنامه‌های پاسخ به حوادث و بازیابی فناوری اطلاعات و ارتباطات باید تحت بررسی حسابرسی داخلی قرار گیرند.
- آزمون‌های نفوذ تهدید محور[۴] باید در یک گزارش کیفی مستند شوند. هرچند، این آزمایش‌ها نباید توسط حسابرسی داخلی انجام شوند و گزارش مربوطه ممکن است توسط حسابرسی داخلی تهیه نشود.
- تأمین‌کنندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث باید بر اساس رویکردی مبتنی بر ریسک ارزیابی و بازرسی شوند. این ارزیابی‌ها باید توسط حسابرسان متخصص انجام شوند. همچنین، حسابرسی مشترک (تجمیعی)[۵] گزینه‌ای است که ممکن است در آینده بسیار مفید واقع شود.
- قراردادها با تأمین‌کنندگان خدمات فناوری اطلاعات و ارتباطات پیمانکاران باید از نظر کلیه مفاد کلیدی قراردادی که برای حسابرسی داخلی حائز اهمیت است، بررسی شوند.

حسابرسی داخلی باید به کمک آموزش، مهارت‌های خود را به‌روزرسانی نموده تا بتواند الزامات DORA را برآورده سازد؛ همچنین، با شیوه‌های معمول فناوری اطلاعات در زمینه‌هایی مانند مدیریت ریسک و مدیریت حوادث فاوا، مدیریت تداوم کسب‌وکار و مدیریت اشخاص ثالث آشنایی کافی داشته باشد.

مقرره DORA هنوز در مراحل ابتدایی خود قرار دارد و تمامی مستندات پشتیبانی‌کننده آن منتشر نشده‌اند؛ بنابراین، شیوه‌های مناسب پیاده‌سازی این مقررات باید به تدریج و به مرور زمان شکل بگیرند. در هر صورت، تلاش‌ها برای تقویت دفاع سایبری و آمادگی در صنعت مالی و همچنین توسعه یک چارچوب کنترلی داخلی فناوری اطلاعات و ارتباطات و امنیتی مقاوم، به‌طور مشخص گامی در راستای مسیر صحیح است. رعایت الزامات DORA نه تنها به‌دلیل پیامدهای احتمالی جریمه‌های اداری، توبیخ‌های عمومی، برنامه‌های اصلاحی پیشنهاد شده یا جبران خسارت به مشتریان و اشخاص ثالث، بلکه به دلیل آن که این الزامات با هدف نفع کل بازار مالی و مصرف‌کنندگان، به ایجاد یک بازار مالی دیجیتال مقاوم در برابر بحران در اروپا کمک می‌کند، توصیه شده است.

[۴] Threat Led Penetration Test
[۵] Pooled Audit

راهنمای عملی و چک‌لیست‌های کنترلی DORA

۱. مقدمه‌ای بر مقررات DORA

۱,۱. زمینه- بسته مالی دیجیتال اتحادیه اروپا

تغییرات و تحولات مداوم در بخش مالی، مانند ارائه محصولات مالی جدید، تحول در امور مالی دیجیتال، دارایی‌های رمزنگاری‌شده و فناوری دفتر کل توزیع‌شده، موجب ضرورت تدوین مقررات قوی‌تر و هماهنگ‌تر در اتحادیه اروپا گردیده است. در سپتامبر ۲۰۲۰، کمیسیون اروپا اولین اقدامات خود را با پذیرش "بسته مالی دیجیتال اتحادیه اروپا[۶]" آغاز کرد و خطوط کلی چگونگی پشتیبانی اتحادیه اروپا از تحول دیجیتال در بخش مالی را در پنج سال آینده تعیین نمود. اهداف اصلی این بسته به شرح زیر است:

- توانمندسازی و حمایت از پتانسیل امور مالی دیجیتال از نظر نوآوری و رقابت، به‌طوریکه ریسک‌های مصرف‌کنندگان، کسب‌وکارها و به‌طور کلی ثبات مالی اتحادیه اروپا کاهش یابد.
- اطمینان از اینکه شرکت‌های فین‌تک از طریق پیاده‌سازی اقدامات حاکمیتی، امنیت سایبری و مدیریت ریسک فاوا و گزارش‌گیری حوادث، قادر به مقابله با حملات سایبری و اختلالات عملیاتی هستند.

این بسته استراتژی پنج‌سال آینده را پوشش می‌دهد و شامل سه پیشنهاد قانونی است:

۱- مقررات بازار دارایی‌های رمزنگاری‌شده[۷]
۲- مقررات فناوری دفتر کل دیجیتال[۸]
۳- مقررات تاب‌آوری عملیاتی دیجیتال[۹]

۱,۲. اهداف و زمان‌بندی DORA

این مستند بر روی DORA که اولین قانون در سطح اتحادیه اروپا است و تاب‌آوری عملیاتی دیجیتال را برای خدمات مالی تنظیم می‌کند، تمرکز دارد. در اینجا، اصطلاح تاب‌آوری به معنای توانایی ادامه عملیات در صورت وقوع حوادث یا رویدادهای مخرب ناشی از حوزه دیجیتال است. DORA یک چارچوب قانونی برای پیاده‌سازی قوانینی که شرکت‌ها باید برای کاهش آسیب‌پذیری‌های خود رعایت کنند، ایجاد می‌کند تا شرکت‌ها بتوانند به اختلالات و تهدیدات مختلف مرتبط با فناوری اطلاعات و ارتباطات پاسخ داده و از اثرات آن‌ها به‌خوبی بهبود یابند. اهداف اصلی این مقررات عبارتند از:

- حاکمیت مؤثر بر ریسک‌های فناوری اطلاعات و ارتباطات و ریسک‌های سایبری؛
- تقویت نقش مقامات نظارتی؛
- ارتقای استاندارد امنیت سایبری در اروپا؛
- هماهنگ‌سازی مقررات مدیریت ریسک فاوا که در حال حاضر در کشورهای عضو اتحادیه اروپا وجود دارد؛

اجرای DORA، پس از چهار سال دوره مستمر انتشار و مشاوره، از تاریخ ۱۷ ژانویه ۲۰۲۵ اجباری شده است.

---

[۶] EU Digital Finance Package: https://finance.ec.europa.eu/publications/digital-finance-package_en
[۷] Markets in Crypto-Assets Regulation
[۸] Digital Ledger Technology Regulation
[۹] Digital Operational Resilience Regulation

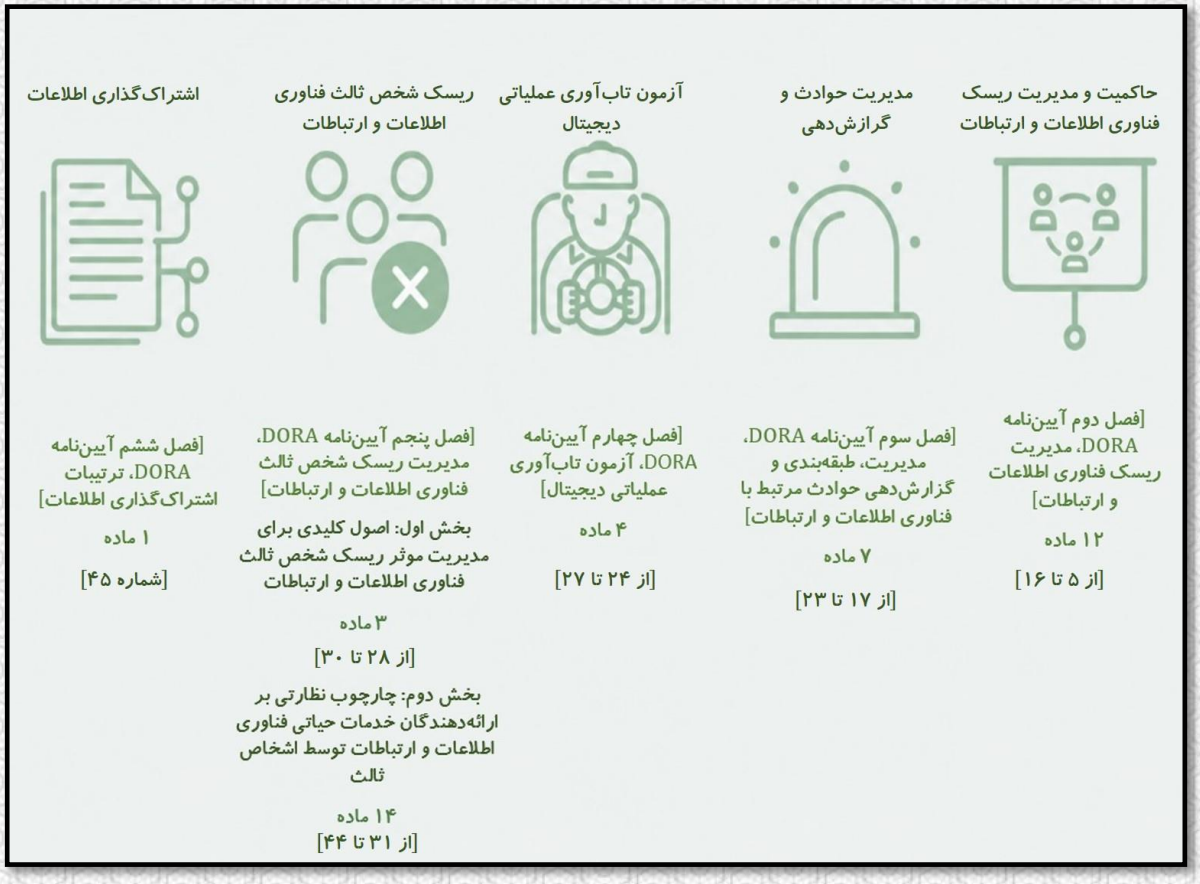
شکل شماره ۱- خط سیر DORA

۱,۳. پیامدهای عدم تطابق با مقرراتDORA

شرکت‌ها در صورت عدم پیروی از مقررات DORA، ممکن است با پیامدهای مختلفی مانند جریمه‌های سازمانی مواجه شوند. علاوه بر این، مقامات نظارتی مجاز هستند مؤسسات مالی را به‌طور علنی توبیخ نموده و آنها را به اجرای برنامه‌های اصلاحی که به رفع هرگونه ضعف یا نقصی که بر تاب‌آوری عملیاتی آنها تأثیر می‌گذارد، ملزم نمایند. شرکت‌هایی که الزامات قانونی را رعایت نمی‌کنند، ممکن است موظف به جبران خسارت مشتریان مستقیم و اشخاص ثالث تحت تأثیر عدم رعایت مقررات شوند. علاوه بر این، در موارد عدم تطابق مکرر با الزامات DORA، مقامات نظارتی ممکن است از شرکت‌های مالی درخواست سرمایه‌گذاری‌های اضافی داشته و نیز شروطی را برای لغو مجوز فعالیت این شرکت‌ها در نظر بگیرند.

۱,۴. پنج رکن مقررات DORA

مقررات DORA شامل ۶۴ ماده است؛ ۴۱ ماده از آن به پنج رکن اصلی تقسیم می‌شوند که در زیر به تفصیل آمده است. سایر ۲۳ ماده به‌طور خاص به وظایف نهادهای مالی ارتباط نداشته و به حوزه‌های ساختاری مانند دامنه کاربرد، مقامات ذی‌صلاح، مقررات واگذاری، مقررات موقت و نهایی، و اصلاحات اشاره دارند.



شکل شماره ۲- پنج رکن DORA

رکن اول – حاکمیت و مدیریت ریسک فناوری اطلاعات و ارتباطات (ارجاع به فصل دوم مقررات DORA)

- تقویت مسئولیت‌های مدیریت ارشد، نیازمند توسعه سیاست‌ها برای مدیریت تاب‌آوری عملیاتی و تعریف استراتژی‌ها/ مدل‌ها برای کاهش تأثیرات رویدادهایی است که از دنیای دیجیتال ناشی شده و ممکن است محرمانگی، دسترس‌پذیری یا یکپارچگی خدمات و عملکردهای حیاتی را تحت‌الشعاع قرار دهد.
- مدیریت ارشد نباید تنها بر پایداری مالی تمرکز کند، بلکه باید به تاب‌آوری نیز توجه داشته باشد.
- بهبود مدل‌ها و ابزارهای مدیریت ریسک برای پاسخ مؤثر به محیطی که پیوسته در حال تغییر است، و برای کاهش تأثیرات ریسک‌های فناوری اطلاعات و ارتباطات نیازمند موارد زیر است:
  - ایجاد چارچوب حاکمیت و کنترل داخلی برای ریسک‌های فناوری اطلاعات و ارتباطات.
  - تخصیص منابع کافی برای برآورده‌سازی نیازهای تاب‌آوری عملیاتی.
  - شناسایی و طبقه‌بندی کارکردها (وظایف) و دارایی‌های پشتیبانی فناوری اطلاعات و ارتباطات بر اساس اهمیت و وابستگی‌های متقابل آن‌ها با اشخاص ثالث.
  - شناسایی منابع ریسک به صورت مستمر.
  - انجام ارزیابی ریسک سالانه برای سیستم‌های قدیمی.
  - توسعه برنامه‌های خاص آگاهی‌رسانی و آموزش در زمینه تاب‌آوری دیجیتال.
  - تعریف و اجرای سیاست‌نامه تداوم کسب‌وکار به همراه برنامه بازیابی از بحران[۱۰] به‌عنوان بخشی جدایی‌ناپذیر.

[۱۰] Disaster Recovery Plan (DRP)

رکن دوم – مدیریت حوادث مرتبط با فاوا، طبقه‌بندی و گزارش‌دهی (ارجاع به فصل سوم مقررات DORA)

- مدیریت یکپارچه‌ی طبقه‌بندی و گزارش‌دهی حوادث عمده فناوری اطلاعات و ارتباطات؛ مراجع نظارتی اروپا[۱۱] معیارهایی را برای شناسایی حوادث عمده و قالب‌های گزارش‌دهی مشترک/ استاندارد توسعه خواهند داد. این مراجع امکان هماهنگ‌سازی و متمرکزسازی بیشتر را با ارزیابی امکان ایجاد یک مرکز واحد اتحادیه اروپا برای گزارش‌دهی حوادث عمده مرتبط با فناوری اطلاعات و ارتباطات توسط نهادهای مالی تحلیل خواهد کرد. معیارهای طبقه‌بندی و گزارش‌دهی بر اساس تعداد کاربران تحت تأثیر، مدت زمان حادثه، مناطق جغرافیایی و اهمیت خدمات خواهد بود.
- تعریف و اجرای فرآیند مدیریت حوادث فناوری اطلاعات و ارتباطات.
- پذیرش شاخص‌های هشدار زودهنگام و تعریف معیارهای خاص برای طبقه‌بندی حوادث.
- نظارت بر حوادث و اجرای مکانیزم‌های پیگیری تا زمان رفع علت اصلی.
- گزارش‌دهی حوادث عمده فناوری اطلاعات و ارتباطات به نهاد ملی نظارتی.

رکن سوم – آزمون تاب‌آوری عملیاتی دیجیتال (ارجاع به فصل چهارم مقررات DORA)

- بررسی اثربخشی قابلیت‌های پیش‌بینی، شناسایی حادثه، پاسخ و بازیابی از طریق آزمون‌های دوره‌ای.
- انجام آزمون تاب‌آوری عملیاتی دیجیتال متناسب با اندازه کسب‌وکار و پروفایل ریسک نهادهای مالی، از طریق آزمون‌های پایه (برای همه مؤسسات مالی) و آزمون‌های پیشرفته (به عنوان مثال، TLPT[۱۲]– آزمون نفوذ تهدید محور) برای مؤسسات مهم با سطح مناسب بلوغ سایبری (توجه: مقامات ذی‌صلاح سطح بلوغ سایبری را بر اساس عواملی مانند اهمیت یا بحرانی بودن کارکردها نسبت به خدمات ارائه شده و فعالیت‌های انجام شده توسط نهاد مالی، همچنین پروفایل ریسک فناوری اطلاعات و ارتباطات خاص ارزیابی می‌کنند).
- انجام آزمون دوره‌ای برای تمام سیستم‌ها و برنامه‌های فناوری اطلاعات و ارتباطات حیاتی (آزمون آسیب‌پذیری، تحلیل کد، کارآیی، قابلیت‌ها و غیره).
- اختصاص منابع کافی و اطمینان از جلوگیری از تضاد منافع (به عنوان مثال، در حین طراحی و اجرای آزمون).

رکن چهارم – مدیریت ریسک‌های فناوری اطلاعات و ارتباطات اشخاص ثالث (ارجاع به فصل پنجم مقررات DORA)

- اعمال رویکرد استراتژیک برای مدیریت ریسک اشخاص ثالث به منظور نظارت بر وابستگی‌ها و تمرکز ریسک‌ها. DORA چارچوب نظارتی اتحادیه اروپا را برای تأمین‌کنندگان حیاتی[۱۳] معرفی می‌کند تا به ریسک‌های سیستمی و تمرکزی که وابستگی بخش مالی به تعداد کمی از تأمین‌کنندگان خدمات شخص ثالث فناوری اطلاعات و ارتباطات ایجاد می‌کند، پرداخته شود. ناظرین اصلی[۱۴] از قدرت نظارت بر فعالیت‌های تأمین‌کنندگان حیاتی در مقیاس اتحادیه اروپا و در ارتباط با خدمات فاوای آن‌ها به بخش مالی برخوردارند.
- توسعه سامانه اطلاعاتی (ثبت اطلاعات) حاوی نمای جامعی از تمام طرف‌های سوم حوزه فناوری اطلاعات و ارتباطات؛ تغییرات این سامانه باید به صورت سالانه به نهاد ناظر گزارش شود.

---

[۱۱] The ESAs are the European Supervisory Authorities: EBA (European Banking Authority), ESMA (European Securities and Markets Authority) and EIOPA (European Insurance and Occupational Pensions Authority).

[۱۲] Thread-Led Penetration Tests (TLPT)

[۱۳] ICT Critical Third-Party Provider (CTPP)

[۱۴] Lead Overseers

- گسترش دایره نظارتی به اشخاص ثالث حیاتی فاوا (با در نظر گرفتن تمام تأمین‌کنندگان پرخطر، نه فقط آن‌هایی که به‌عنوان برون‌سپاری شناخته می‌شوند).
- ایجاد چارچوب یکپارچه و یکسان جهت هماهنگ‌سازی جنبه‌های قراردادی به‌منظور امکان نظارت کامل نهاد مالی در تمام مراحل ارتباط با تأمین‌کنندگان شخص ثالث.
- ارزیابی ریسک تمرکز فناوری اطلاعات و ارتباطات (تحلیل هزینه/ سود راه‌حل‌های جایگزین).
- تدارک و تدوین استراتژی خروج در صورت برون‌سپاری کارکردهای حیاتی یا مهم.

رکن پنجم – توافقات به اشتراک‌گذاری اطلاعات (ارجاع به فصل ششم مقررات DORA)

DORA در خصوص تهدیدات سایبری، هوشمندی، اطلاعات امنیتی، تکنیک‌ها، رویه‌ها، هشدارها و ابزارها، و به‌منظور تقویت تاب‌آوری دیجیتال و مقابله با تهدیدات نسل جدید، نهادهای مالی را به تبادل اطلاعات میان خود تشویق می‌کند. اکوسیستم مالی به‌طور گسترده‌ای به یکدیگر متصل است و این اتصال می‌تواند حوادث را از یک عامل به عاملی دیگر منتقل کند. همچنین، این اکوسیستم به زیرساخت‌ها و فناوری‌های مشترک وابسته بوده و با تهدیداتی روبروست که نه تنها مؤسسات مالی منفرد، که به‌طور کلی اغلب بخش مالی را تحت تأثیر قرار می‌دهند.

مقرره DORA به‌منظور افزایش آگاهی در مورد ریسک‌های فاوا، کاهش تکثیر آن‌ها، پشتیبانی از قابلیت‌های دفاعی نهادهای مالی و بهبود تکنیک‌های شناسایی تهدیدها، توافقات خاصی را برای تبادل اطلاعات در خصوص تهدیدات سایبری تعریف می‌نماید. لازم به ذکر است، پیاده‌سازی چنین الزاماتی اجباری نیست و مؤسسات مالی می‌توانند تصمیم بگیرند که آیا این اطلاعات را با دیگر نهادهای مالی به اشتراک بگذارند یا خیر.

۱.۵. DORA و ابزارهای سیاست‌گذاری آن

علاوه بر خود قانون DORA به عنوان سند اصلی، آیین‌نامه‌ها و دستورالعمل‌های اجرایی بالادستی، در قالب ابزارهای سیاست‌گذاری[۱۵]، الزامات عملیاتی بیشتری را در مورد ارکان DORA مشخص می‌کنند تا چارچوب حقوقی یکپارچه و هماهنگ در حوزه‌های مختلف این قانون تضمین شود. از مراجع نظارتی اروپا (ESAs[۱۶]) خواسته شده است که مجموعه ۱۳ ابزار سیاست‌گذاری را برای کمیته مشترک تهیه نمایند. به‌طور دقیق‌تر، آن‌ها ۷ سند استاندارد فنی مقرراتی[۱۷]، ۲ استاندارد فنی اجرایی[۱۸]، ۲ رهنمود[۱۹]، ۱ گزارش امکان‌سنجی[۲۰] و ۱ فراخوان برای ارائه مشاوره[۲۱] تهیه کرده‌اند.

ابزارهای سیاست‌گذاری به دو دسته اصلی تقسیم شده‌اند که هر دو تحت یک مشاوره عمومی به مدت تقریباً سه ماه قرار گرفتند تا نظرات و بازخوردها جمع‌آوری شود. بر اساس نتایج این مشاوره‌ها، مراجع نظارتی اروپا مجموعه کامل اسناد را در دو بازه زمانی متفاوت به کمیسیون اروپا ارسال کرده‌اند: ۱۷ ژانویه ۲۰۲۴ (دسته اول) و ۱۷ ژوئیه ۲۰۲۴ (دسته دوم)

کمیسیون اروپا قبلاً اسناد دسته اول را در تاریخ ۲۵ ژوئن ۲۰۲۴ منتشر کرده است و اکنون با هدف تصویب این اسناد در ماه‌های آینده، بررسی دسته دوم را آغاز نموده است.

---

[۱۵] Policy Instruments

[۱۶] The European System of Financial Supervision (ESFS) is a network centered around three European Supervisory Authorities (ESAs), the European Systemic Risk Board and national supervisors. Its main task is to ensure consistent and appropriate financial supervision throughout the EU.

[۱۷] Regulatory Technical Standards (RTS)

[۱۸] Implementing Technical Standards (ITS)

[۱۹] Guideline

[۲۰] Feasibility Report

[۲۱] Call for advice

شکل زیر نگاشتی از ارتباط میان مجموعه کامل ابزارهای سیاست‌گذاری و ارکان DORA را نشان می‌دهد[۲۲]:

شکل شماره ۳- نگاشت ابزارهای سیاست‌گذاری با پنج رکن DORA

۲. انگیزه تدوین راهنمای عملی و چک‌لیست‌های کنترلی DORA

چشم‌انداز تهدیدات دیجیتالی که به سرعت در حال تحول است، نیاز مبرم سازمان‌ها به چارچوب‌های قوی و انعطاف‌پذیری که تاب‌آوری عملیاتی را تضمین می‌کنند، تشدید کرده است. به ویژه، مؤسسات مالی نه تنها از جانب تهدیدات سایبری، بلکه از جانب محیط نظارتی پیچیده‌ای که برای محافظت از عملیات آنها طراحی شده است، با چالش‌های بی‌سابقه‌ای روبرو هستند.

یکی از این مقررات، قانون تاب‌آوری عملیاتی دیجیتال است که توسط اتحادیه اروپا معرفی شده، و یک ابتکار برجسته با هدف افزایش تاب‌آوری عملیاتی دیجیتال بخش مالی است. با این حال، هر چه با ذینفعان بیشتری در DORA تعامل داشته باشیم، بیشتر مشخص می‌گردد که الزامات این قانون، گاهی اوقات چالش‌های تفسیری قابل توجهی را برای مؤسسات مالی ایجاد می‌کند.

با مشاهده مشکلاتی که مؤسسات مالی در تبدیل مقررات این قانون به اقدامات عملی و قابل اجرا با آن مواجه هستند، انگیزه‌ای شد برای آنکه چارچوب کنترلی DORA را توسعه دهیم. وابستگی روزافزون بخش مالی به سیستم‌های دیجیتال، که با ماهیت بهم پیوسته امور مالی جهانی تشدید می‌شود، به این پیچیدگی می‌افزاید. در نتیجه، یک اختلال عملیاتی نسبتاً کوچک می‌تواند عواقب گسترده‌ای داشته باشد. علاوه بر این، اهمیت انطباق با تأثیر اجتماعی بالقوه شکست‌های دیجیتال که می‌تواند فراتر از مؤسسات منفرد گسترش یابد و خدمات ضروری برای عموم را مختل کند، افزایش می‌یابد.

[۲۲] Source: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

در زمان نگارش این متن، هیچ چارچوب جامعی برای راهنمایی مؤسسات مالی در جهت هدایت مؤثر الزامات DORA وجود نداشته است. اگرچه DORA گامی بزرگ در جهت حفاظت از بخش مالی است و الزامات دقیقی را ارائه می‌دهد، اما این قانون به گونه‌ای تدوین شده است که جای تفسیر دارد. با توجه به این موضوع، اقدام به ایجاد چارچوبی کردیم که تمام پیچیدگی‌های قانونی و فنی را ساده کند. هدف ما تبدیل الزامات نظارتی DORA به اقدامات عملی و قابل اجرا بود که مؤسسات مالی بتوانند آن را درک و اجرا کنند.

این مستند، برای خوانندگانی که به زمینه گسترده‌تر DORA و تاب‌آوری دیجیتال علاقه‌مند هستند، پیشینه ارزشمندی را ارائه می‌دهد. برای کسانی که مشتاق به شروع فرآیند پیاده‌سازی هستند، تمرکز بر بخش ۶ و کنترل‌های تلفیقی موجود در آن، مسیر روشنی را پیش روی آنها قرار می‌دهد.

ما چارچوب کنترلی DORA را به عنوان ابزاری زنده تصور می‌کنیم که قادر به تکمیل پاسخ به تغییرات نظارتی و ریسک‌های دیجیتال نوظهور است. برای اطمینان از اینکه تاب‌آوری عملیاتی دیجیتال نه تنها یک الزام نظارتی، بلکه سنگ بنای عملیات مالی پایدار در دنیای دیجیتال است، ما با همکاری یکدیگر از دریافت بازخورد و مشارکت ذینفعان در سراسر بخش مالی استقبال می‌کنیم.

از طرف نویسندگان،

Sandeep Gangaram Panday – sandeep@brightlyn.nl
Jeremy Oschmann – joschmann@schubergphilis.com

۳. خلاصه مدیریتی چک‌لیست‌های کنترلی (چارچوب کنترلی NOREA)

قانون تاب‌آوری عملیاتی دیجیتال در ۱۶ ژانویه ۲۰۲۳ لازم‌الاجرا شده و از ۱۷ ژانویه ۲۰۲۵ اعمال خواهد شد. پس از اعمال DORA، از سازمان‌هایی که برای بخش مالی فعالیت می‌کنند یا خدمات ارائه می‌دهند، انتظار می‌رود که تغییرات قابل توجهی را متحمل شده باشند و آماده رعایت الزامات جدید باشند. با توجه به پیچیدگی‌ها و چالش‌های مرتبط با تفسیر و اجرای چنین مقرراتی، ما یک چارچوب عملی طراحی کرده‌ایم که برای کمک به مؤسسات در پیمایش این شرایط نظارتی جدید طراحی شده است.

مفتخریم چارچوب کنترلی DORA را به‌عنوان ابزاری که متون حقوقی پیچیده را به کنترل‌های عملی و یکپارچه تبدیل نموده و به مؤسسات مالی در دستیابی به تاب‌آوری دیجیتال کمک می‌کند معرفی نماییم. چارچوب ما حول سه هدف کلیدی ساخته شده است تا اجرای موفقیت‌آمیز را ممکن سازد:

۱. ساده‌سازی و ترجمه‌ی DORA به گونه‌ای که مخاطبان گسترده‌تر بتوانند محتوای آن و منطق پشت مقررات را درک کنند.
۲. کمک به سازمان‌ها در اجرای ارزیابی‌های شکاف DORA و تهیه گزارش‌های مرتبط برای مقامات نظارتی.
۳. بررسی DORA از دیدگاه مهندسی، با هدف حل ریشه‌های واقعی مشکلات در محیط فناوری اطلاعات و ارتباطات (فاوا) و کمک به کسب‌وکارها برای دستیابی به تاب‌آوری عملیاتی پایدار.

علاوه بر این، چارچوب کنترلی DORA ممکن است برای سازمان‌هایی که در محدوده دستورالعمل (۲) امنیت شبکه و اطلاعات اتحادیه اروپا (NIS2) قرار می‌گیرند نیز مفید باشد. DORA و NIS2 هدف مشترکی دارند: ارتقای امنیت سایبری و تاب‌آوری عملیاتی. با این حال، از آنجا که NIS2 صرفاً اهداف سطح بالا[۲۳] را ترسیم می‌کند، سازمان‌های مشمول، در مورد اقدامات و نحوه اجرای آن، در ابهام بوده‌اند. در مقابل، DORA قوانین خاص و مفصلی ارائه می‌دهد که بسیاری از آنها سختگیرانه هستند و با اصول تکلیف وظیفه[۲۴] مراقبت که در NIS2 ذکر شده است، همسو می‌باشند. بنابراین، توصیه می‌کنیم سازمان‌هایی که مشمول مقررات NIS2 هستند، از چارچوب کنترلی DORA به عنوان منبعی برای کمک به دستیابی به انطباق با NIS2 استفاده کنند.

نسخه کامل اکسل چارچوب کنترلی DORA در وب‌سایت NOREA به آدرس زیر موجود است.
https://www.norea.nl/dora

ما شما را تشویق می‌کنیم که به چارچوب مراجعه کرده، فایل را دانلود کنید و با به اشتراک گذاشتن نظرات و بازخوردهای خود با نویسندگان، به افزایش ارتباط و دقت اطلاعات کمک کنید.

۴. پیشینه DORA

۴,۱. از امنیت تا تاب‌آوری

در سال‌های اخیر، تمرکز فناوری اطلاعات و ارتباطات در بخش مالی از امنیت سایبری به سمت تاب‌آوری جامع تغییر یافته است. این گذار، منعکس‌کننده چشم‌انداز در حال تحول تهدیدها و وابستگی‌ها در بازاری است که به‌طور فزاینده‌ای دیجیتال و به هم پیوسته می‌شود. از نظر تاریخی، نگرانی اصلی مؤسسات مالی، ایمن‌سازی سیستم‌های فناوری اطلاعات و ارتباطات در برابر دسترسی غیرمجاز، نقض داده‌ها و حملات سایبری بوده است. این رویکرد امنیت محور، اگرچه ضروری بود، اما اغلب در پرداختن به طیف کامل ریسک‌هایی که می‌توانستند عملیات تجاری را مختل کنند، ناکام می‌ماند.

تحول دیجیتال صنعت مالی همراه با تهدیدهای فزاینده از سوی مجرمان و بازیگران دولتی، سطح و پیچیدگی کلی تهدیدها را افزایش داده است. بر این اساس، استراتژی‌های تاب‌آوری امروزی نه تنها باید به تهدیدهای سایبری بپردازند، بلکه باید شامل اقدامات تداوم عملیاتی در تمام خدمات فناوری اطلاعات و ارتباطات که برای ثبات مالی حیاتی هستند، نیز باشند. گذشته از همه اینها، اکنون، مؤسسات مالی نه تنها برای پردازش تراکنش‌ها، بلکه برای بسیاری از عملکردهای حیاتی تجاری، از جمله کسب‌وکار، تشخیص کلاهبرداری و مدیریت خزانه‌داری، بسیار به سیستم‌های فناوری اطلاعات و ارتباطات متکی هستند.

چنین وابستگی به سیستم‌های فناوری اطلاعات و ارتباطات به این معنی است که هر نوع اختلالی، چه به دلیل حملات سایبری یا نقص فنی یا رویداد پیش‌بینی نشده دیگر، می‌تواند عواقب گسترده‌ای داشته باشد. اختلالات می‌توانند بر دسترسی، اصالت، یکپارچگی و محرمانگی خدمات مالی تأثیر بگذارند و منجر به خسارات مالی، آسیب به اعتبار و شهرت و فرسایش اعتماد مشتریان شوند. از آنجا که این سیستم‌ها به بخش جدایی‌ناپذیر عملیات روزمره مؤسسات مالی تبدیل شده‌اند، تأثیر بالقوه اختلال در آنها به‌طور تصاعدی تا سطح تهدید نابودی برای مؤسسات افزایش یافته است. افزون بر این، به هم پیوستگی سیستم مالی جهانی به این معناست که اختلال در یک نهاد می‌تواند اثرات آبشاری داشته باشد و به‌طور بالقوه منجر به ریسک‌های سیستمی با پیامدهای اجتماعی- اقتصادی گسترده و متنوع شود.

این تغییر رویکرد با تمرکز جدیدی بر تضمین یکپارچگی و در دسترس بودن خدمات در تمام شرایط همسو است و بدین ترتیب ریسک اختلالات سیستمی در بخش مالی را کاهش می‌دهد. در زمینه قوانین و مقررات، تاب‌آوری عبارت است از توانایی

[۲۳] high-level goals
[۲۴] Duty of Care

پیش‌بینی، تحمل، بازیابی، و سازگاری با شرایط نامطلوب، فشارها، حملات، یا به خطر افتادگی سیستم‌هایی که از منابع سایبری[۲۵] استفاده می‌کنند یا توسط آنها پشتیبانی می‌شوند. چنین رویکرد جامعی به تاب‌آوری، می‌تواند طیف وسیعی از استراتژی‌ها از جمله دفاع سایبری و برنامه‌های واکنش به حوادث باج‌افزاری، استراتژی‌های بازیابی عملیات کسب‌وکاری، آزمایش بازیابی واقعی و مدیریت بحران پیشرفته را در بر بگیرد.

۴,۲. استراتژی دیجیتال اروپا

اتحادیه اروپا نیاز به ارتقای تاب‌آوری دیجیتال را به صراحت در چارچوب استراتژی دیجیتال گسترده خود به رسمیت می شناسد.[۲۶] قوانین و چارچوب‌های نظارتی جدیدی برای افزایش تاب‌آوری دیجیتال و هماهنگی در سراسر بخش مالی معرفی شده‌اند. هدف این اقدامات ایجاد یک محیط نظارتی قوی است که نه تنها امنیت سیستم‌های فناوری اطلاعات و ارتباطات را افزایش می‌دهد، بلکه تاب‌آوری عملکردهای حیاتی کسب‌وکار وابسته به آنها را نیز تقویت می‌کند. نمونه‌هایی از قوانین در چارچوب استراتژی دیجیتال اتحادیه اروپا عبارتند از:

- Digital Operational Resilience Act (DORA) — قانون تاب‌آوری عملیاتی دیجیتال
- Network and Information Security 2 (NIS2) Directive — دستورالعمل امنیت شبکه و اطلاعات ۲
- Critical Entities Resilience (CER) Directive — دستورالعمل تاب‌آوری نهادهای حیاتی
- Cyber Resilience Act (CRA) — قانون تاب‌آوری سایبری
- Cybersecurity Act — قانون امنیت سایبری
- Cyber Solidarity Act — قانون همبستگی سایبری

مقررات جدید، نهادهای حیاتی (شامل کل اکوسیستم آنها) را ملزم به ایجاد و حفظ استراتژی‌های جامع تاب‌آوری، از جمله آزمایش‌های منظم، مدیریت ریسک و پروتکل‌های حاکمیتی می‌کند. این مقررات، با انجام این کار، سازمان‌ها را قادر می‌سازد تا حتی در مواجهه با اختلالات قابل توجه، عملیات خود را ادامه داده و از ذی‌نفعان محافظت کنند.
تأکید بر تاب‌آوری اذعان به این واقعیت دارد که در عصر دیجیتال، سؤال این نیست که آیا اختلالات رخ خواهند داد، بلکه چه زمانی رخ خواهند داد. بنابراین، مؤسسات مالی باید آماده مدیریت و کاهش تأثیر چنین رویدادهایی باشند. ایجاد تاب‌آوری در سیستم‌های فناوری اطلاعات و ارتباطات و فرآیندهای تجاری، تداوم، ثبات و اعتماد به بازار مالی را تضمین می‌کند که همگی برای سلامت اقتصادی و اعتماد عمومی ضروری هستند.

۴,۳. تنظیم تاب‌آوری عملیاتی دیجیتال

با توجه به وابستگی‌های روزافزون به سیستم‌های فناوری اطلاعات و ارتباطات، اتحادیه اروپا، DORA را که نشان‌دهنده تغییر قابل توجهی در چارچوب نظارتی گسترده‌تر اتحادیه اروپا است، برای مقابله با ریسک‌های چندوجهی در بخش مالی معرفی کرد و امروزه بر اهمیت تاب‌آوری عملیاتی دیجیتال برای حفظ ثبات و یکپارچگی بازار مالی تأکید می‌کند.

DORA که رسماً با عنوان آیین‌نامه (EU) 2022/2554 شناخته می‌شود، قانونی است که برای اطمینان از این امر در نظر گرفته شده است که نهادهای مالی در اتحادیه اروپا می‌توانند در برابر انواع اختلالات و تهدیدهای مرتبط با فناوری اطلاعات و ارتباطات مقاومت کنند، به آنها پاسخ دهند و از آنها بهبود یابند. این قانون الزامات موجود در حوزه فناوری اطلاعات و ارتباطات را تثبیت و تقویت می‌کند و یک چارچوب واحد برای تاب‌آوری عملیاتی دیجیتال در سراسر بخش مالی اروپا ایجاد می‌کند.

[۲۵] https://csrc.nist.gov/glossary/term/cyber_resiliency
[۲۶] https://eufordigital.eu/discover-eu/eu-digital-strategy/

علیرغم تلاش‌های نظارتی قبلی که هم در سطوح ملی و هم در سطح اتحادیه اروپا انجام شده است، شکاف‌ها و ناهماهنگی‌های قابل توجهی در پرداختن به ریسک‌های فناوری اطلاعات و ارتباطات همچنان حاکم بود. هیئت ریسک سیستمی اروپا در گزارش سال ۲۰۲۰[۲۷] خود، بر آسیب‌پذیری سیستمی ناشی از سطح بالای ارتباط و وابستگی متقابل در سیستم‌های فناوری اطلاعات و ارتباطات بخش مالی تأکید کرد. این آسیب‌پذیری‌ها، نیازمند رویکردی جامع‌تر و هماهنگ‌تر به مدیریت ریسک فناوری اطلاعات و ارتباطات بود، که دقیقاً همان چیزی است که DORA به دنبال ارائه آن می‌باشد و هدفش ارائه آن است.

۴,۳,۱.اهدافی که DORA به دنبال تحقق آن است.

DORA الزامات متعددی را برای کمک به سازمان‌ها در ایجاد و حفظ تاب‌آوری عملیاتی دیجیتال مشخص می‌کند. این الزامات حول پنج محور متمرکز هستند:

1. ICT risk management — مدیریت ریسک فناوری اطلاعات و ارتباطات
2. Incident management, classification, and reporting — مدیریت، طبقه‌بندی و گزارش‌دهی حوادث
3. Digital operational resilience testing — آزمایش تاب‌آوری عملیاتی دیجیتال
4. Managing of ICT third-party risks — مدیریت ریسک‌های پیمانکاران فناوری اطلاعات و ارتباطات
5. Information-sharing arrangements — ملاحظات اشتراک‌گذاری اطلاعات

۴,۳,۲. نحوه تحقق اهداف توسط DORA

قانون DORA برای دستیابی به اهداف خود، چندین الزام کلیدی را که به عنوان مقررات سطح ۱ شناخته می‌شوند، تعیین می‌کند. این الزامات که در خود قانون شرح داده شده‌اند، در چارچوب پنج رکن اساسی DORA مورد بحث قرار گرفته‌اند.

۱) مدیریت ریسک فناوری اطلاعات و ارتباطات – فصل ۲ قانون DORA (مواد ۵ تا ۱۶):

مدیریت ریسک فناوری اطلاعات و ارتباطات مستلزم آن است که نهادهای مالی چارچوب‌های جامعی را برای شناسایی، محافظت، تشخیص، پاسخ و بازیابی از ریسک‌های مرتبط با فناوری اطلاعات و ارتباطات ایجاد کنند. این رکن نخست، بر حاکمیت شفاف[۲۸]، ارزیابی‌های منظم ریسک، اقدامات حفاظتی، سیستم‌های تشخیص، برنامه‌های واکنش به حوادث و بهبود مستمر مبتنی بر تجارب گذشته را الزامی می‌سازد.

۲) گزارش حوادث مرتبط با فناوری اطلاعات و ارتباطات – فصل ۳ قانون DORA (مواد ۱۷ تا ۲۳):

گزارش‌دهی حوادث مرتبط با فناوری اطلاعات و ارتباطات، فرآیند گزارش‌دهی حوادث مهم فاوا را استانداردسازی می‌کند. این رکن مستلزم تدوین معیارهایی برای طبقه‌بندی حوادث، ایجاد رویه‌هایی برای گزارش آنها به مقامات در بازه‌های زمانی مشخص و ترویج اشتراک‌گذاری اطلاعات برای افزایش تاب‌آوری جمعی است.

۳) آزمایش تاب‌آوری عملیاتی دیجیتال – فصل ۴ قانون DORA (مواد ۲۴ تا ۲۷):

آزمایش تاب‌آوری عملیاتی دیجیتال، آزمایش منظم سیستم‌های فناوری اطلاعات و ارتباطات را برای ارزیابی استحکام آنها الزامی می‌کند. این رکن شامل برنامه‌های آزمایش منظم، آزمایش نفوذ تهدید محور (در صورت لزوم) برای شبیه‌سازی حملات دنیای واقعی و استفاده از نتایج آزمایش برای بهبود تاب‌آوری سیستم است.

---

[۲۷] European Systemic Risk Board, Annual Report 2020, https://www.esrb.europa.eu/pub/pdf/ar/2021/esrb.ar2020~f20842b253.en.pdf

[۲۸] clear governance

۴) مدیریت ریسک شخص ثالث فناوری اطلاعات و ارتباطات – فصل ۵ قانون DORA (مواد ۲۸ تا ۴۴):

مدیریت ریسک شخص ثالث فناوری اطلاعات و ارتباطات به ریسک‌های مرتبط با برون‌سپاری خدمات فاوا می‌پردازد. این رکن مشخص می‌کند که نهادهای مالی باید قبل از مشارکت با پیمانکاران، بررسی‌های دقیق[۲۹] را انجام داده و اطمینان حاصل کنند که توافق‌نامه‌های قراردادی شامل مفاد انعطاف‌پذیری و امنیتی هستند، به‌طور مداوم بر عملکرد شخص ثالث نظارت کنند و ریسک‌های ناشی از اتکای بیش از حد به تعداد محدودی از پیمانکاران را مدیریت نمایند.

۵) اشتراک‌گذاری اطلاعات - فصل ۶ قانون DORA (ماده ۴۵):

اشتراک‌گذاری اطلاعات به تبادل اطلاعات تهدید و به‌روشها بین نهادهای مالی و مقامات اشاره دارد. این رکن، مشارکت در شبکه‌های مشارکتی برای تبادل اطلاعات و هماهنگی واکنش‌ها در طول حوادث را برای بهبود تاب‌آوری کلی ترویج می‌دهد.

در مجموع، قانون DORA شامل ۶۴ ماده است که ۴۱ ماده آن در این پنج رکن قرار می‌گیرد. ۲۳ ماده دیگر صراحتاً به وظایف نهادهای مالی نمی‌پردازند. آنها بیشتر بر اطلاعات زمینه‌ای (دامنه کاربرد، مقامات صلاحیت‌دار، جرائم و مجازات‌ها، اختیارات تفویضی، مقررات انتقالی و نهایی، و اصلاحیه‌ها) تمرکز دارند.

۴,۳,۳. نقش استانداردهای فنی نظارتی (RTS)[۳۰] و استانداردهای فنی پیاده‌سازی (ITS)[۳۱]

متن اصلی DORA با جزئیات فنی مهمی در مجموعه‌ای از قوانین ثانویه، که به عنوان مقررات سطح ۲ شناخته می‌شوند، تکمیل شده است. سه مراجع نظارتی اروپایی[۳۲] به‌طور مشترک برای تهیه پیش‌نویس این استانداردها منصوب شدند. این مراجع شامل سازمان بانکداری اروپا[۳۳]، سازمان بیمه و بازنشستگی شغلی اروپا[۳۴] و سازمان اوراق بهادار و بازارهای اروپا[۳۵] هستند.

این استانداردهای فنی شامل دو نوع هستند:

- استانداردهای فنی نظارتی، که در مجموع هفت سند هستند.
- استانداردهای فنی اجرایی، که شامل دو سند هستند.

توسعه RTS و ITS در قالب دو مجموعه سند انجام شد. مجموعه اول در ۱۷ ژانویه ۲۰۲۴ به کمیسیون اروپا (EC) ارائه شد. سه سند RTS در این مجموعه اول در ۲۵ ژوئن ۲۰۲۴ در مجله رسمی اتحادیه اروپا منتشر شدند که نشان دهنده تصویب رسمی آنها است.

مجموعه اول شامل اسناد زیر است:

- RTS در مورد چارچوب مدیریت ریسک فناوری اطلاعات و ارتباطات شامل مدیریت ریسک ساده‌شده فناوری اطلاعات و ارتباطات
- چارچوب مواد ۲۸ الی ۴۱ (بخشی از رکن اول DORA)
- RTS در مورد معیارهای طبقه‌بندی حوادث مرتبط با فناوری اطلاعات و ارتباطات (رکن دوم)
- ITS برای ایجاد الگوهایی برای ثبت اطلاعات (رکن چهارم)

---

[۲۹] due diligence
[۳۰] Regulatory technical standards (RTS)
[۳۱] Implementation technical standards (ITS)
[۳۲] European supervisory authorities (ESA)
[۳۳] European Banking Authority (EBA)
[۳۴] European Insurance and Occupational Pensions Authority (EIOPA)
[۳۵] European Securities and Markets Authority (ESMA).

- RTS برای تعیین سیاست‌نامه مربوط به خدمات فناوری اطلاعات و ارتباطات انجام شده توسط ارائه‌دهندگان شخص ثالث فناوری اطلاعات و ارتباطات (رکن چهارم)

مجموعه دوم که در دو بخش، در تاریخ‌های ۱۷ و ۲۶ جولای ۲۰۲۴ به کمیسیون اروپا ارائه شد، شامل اسناد زیر است:

- RTS در مورد محتوا، جدول زمانی و قالب‌های گزارش حادثه (بخشی از رکن دوم DORA)
- ITS در مورد محتوا، جدول زمانی و قالب‌های گزارش حادثه (رکن دوم)
- RTS در مورد واگذاری وظایف حیاتی یا مهم به پیمانکاران فرعی (رکن چهارم)
- RTS در مورد هماهنگ‌سازی نظارت (رکن چهارم)
- RTS در مورد آزمون نفوذ تهدید محور TLPT (رکن سوم)

در حال حاضر تمام اسناد سطح ۲ نهایی شده‌اند. برای دسترسی به آخرین نسخه‌های RTS و ITS، لطفاً به انتشارات ثانویه ما مراجعه کنید: https://www.norea.nl/dora/statusupdate-wetgeving-dora

۴,۳,۴. رابطه DORA با NIS2

NIS2 و DORA که هر دو چارچوب‌های قانونی کلیدی اتحادیه اروپا هستند، که نه تنها در هدف خود برای افزایش امنیت سایبری و تاب‌آوری عملیاتی مشترک هستند، بلکه به یکدیگر نیز ارجاع می‌دهند. DORA در مقایسه با NIS2 از وضعیت ویژه‌ای برخوردار است، بدین معنا که DORA به‌عنوان مجموعه‌ای از قواعد تخصصی به حساب می‌آید که بر اهداف عام‌تر NIS2 تقدم دارد.

برخی از تفاوت‌های کلیدی بین این دو چارچوب عبارتند از:

- NIS2 دامنه بسیار وسیع‌تری از بخش‌ها را هدف قرار می‌دهد؛ در حالی که DORA به‌طور خاص بخش مالی را هدف قرار می‌دهد.
- NIS2 الزامات عمومی امنیت سایبری را ارائه می‌دهد؛ اما DORA الزامات دقیقی را برای بخش مالی ارائه می‌دهد.
- NIS2 دستورالعملی است که باید در قوانین ملی گنجانده شود (در هلند، به عنوان Cyberbeveiligingswet [۳۶]تصویب شده است)؛ در حالی که DORA یک آیین‌نامه اتحادیه اروپا است و بنابراین قابلیت اجرای فوری[۳۷] برای همه کشورهای عضو اتحادیه اروپا را دارد.

اگرچه NIS2 موضوع اصلی این مستند نیست، اما شایسته ذکر می‌باشد. ما معتقدیم که چارچوب کنترلی DORA می‌تواند برای سازمان‌هایی که در محدوده NIS2 قرار می‌گیرند نیز مفید باشد. از آنجا که هنوز کنترل‌های دقیقی برای NIS2 وجود ندارد، سازمان‌ها همچنان در مورد اینکه برای دستیابی به انطباق با NIS2 چه کاری باید انجام داده و چه چیزی را اجرا کنند، با عدم قطعیت مواجه هستند.

شایان ذکر است که NIS2 در ماده ۲۱,۱ خود رویکردی همه‌جانبه در برابر خطرات اتخاذ کرده است. در این زمینه، رویکرد همه‌جانبه به این معنا است که سازمان‌ها باید وضعیت امنیتی کلی و ثبات عملیاتی خود را از طریق اتخاذ یک استراتژی گسترده و فراگیر برای مدیریت ریسک و تاب‌آوری ارتقا دهند. این امر باید تضمین کند که آنها برای هرگونه منبع بالقوه اختلال (همه خطرات)، چه به شکل حملات سایبری، بلایای طبیعی، نقص فنی یا سایر رویدادهای پیش‌بینی نشده، آماده هستند. در مجموع،

[۳۶] قانون امنیت سایبری

[۳۷] immediate applicability

با توجه به اینکه الزامات DORA سختگیرانه‌تر از NIS2 است، به سازمان‌هایی که تحت تأثیر مقررات NIS2 قرار دارند، توصیه می شود پیاده‌سازی چارچوب کنترلی DORA را مد نظر قرار دهند.

۵. رویکرد DORA

۵,۱. مبتنی بر اصول[۳۸]

قانون DORA مظهر تغییر در تفکر نظارتی است و فراتر از انطباق صرف، به سمت رویکردی مبتنی بر اصول برای تاب‌آوری دیجیتال حرکت می‌کند. برای بهره‌برداری کامل از ارزش DORA، به سازمان‌ها توصیه می‌کنیم به عنوان یک اصل راهنمودی از آن برای بهبود ثبات و امنیت عملیاتی، متناسب با مشخصات ریسک خاص فرآیندهای حیاتی کسب‌وکار و سیستم‌های پشتیبانی فناوری اطلاعات و ارتباطات خود استفاده کنند. این دیدگاه تضمین می‌کند که پیاده‌سازی قانون به یک تمرین ساده انطباق تقلیل نیافته، بلکه به عنوان چارچوبی راهبردی برای تاب‌آوری مستمر یکپارچه می‌شود.

ماده ۴ قانون DORA اصل تناسب[۳۹] را شرح می‌دهد و دو روش برای اعمال آن مشخص می‌کند.

۱. اصول تناسب در مفاد خاص مربوط به مدیریت ریسک فناوری اطلاعات و ارتباطات (فصل ۲ DORA) گنجانده شده است، که به موجب آن به شرکت‌های کوچک[۴۰] اجازه داده می‌شود الزامات ساده‌شده را اعمال کنند.
۲. پیاده‌سازی و اعمال الزامات DORA می‌تواند به‌طور متناسب بر اساس اندازه و مشخصات کلی ریسک موسسه مالی و همچنین ماهیت، مقیاس و پیچیدگی خدمات، فعالیت‌ها و عملیات (از طریق مقررات مبتنی بر اصول) باشد.

مقررات مبتنی بر اصول[۴۱]، بر سازگاری مبتنی بر ریسک تأکید دارد که به مؤسسات مالی اجازه می‌دهد تا استراتژی‌های مدیریت ریسک و تاب‌آوری خود را با زمینه‌های عملیاتی منحصر به فرد خود تطبیق دهند. برخلاف مقررات تجویزی[۴۲] که اقدامات خاصی را دیکته می‌کنند، مقررات مبتنی بر اصول، نهادها را تشویق می‌سازد تا اقداماتی را اتخاذ نموده و کنترل‌هایی را اجرا کنند که متناسب با خطراتی است که با آن مواجه هستند. این رویکرد، تنوع مؤسسات مالی و سطوح مختلف پیچیدگی در محیط‌های فناوری اطلاعات و ارتباطات آنها را به رسمیت می‌شناسد.

با اتخاذ یک رویکرد مبتنی بر اصول، موسسات مالی می‌توانند از طرز فکرِ "تیک زدنِ گزینه‌ها"[۴۳] در مورد انطباق با قوانین، فراتر رفته و در عوض، مدیریت ریسک معنادار را داخلی سازی کنند. این امر مستلزم درک عمیق از مشخصات ریسک مؤسسه، شناسایی کارکردهای حیاتی یا مهم و ارزیابی سیستم‌های فناوری اطلاعات و ارتباطات است که ضمن اینکه اندازه یک موسسه را نیز در نظر می‌گیرند، زیربنای این کارکردها هم هستند.

تناسب اقدامات با مشخصات ریسک

رویکرد مبتنی بر اصول DORA بر این ایده استوار است که اقدامات و کنترل‌ها باید متناسب با مشخصات ریسک فرآیندهای تجاری و سیستم‌های فناوری اطلاعات و ارتباطات باشند. این بدان معناست که مؤسسات باید ارزیابی‌های کاملی از ریسک انجام دهند تا حیاتی‌ترین دارایی‌ها و فرآیندهای خود را شناسایی و اولویت‌بندی کنند. سپس سطح مکانیسم‌های حفاظت، تشخیص، پاسخ و بازیابی باید با تأثیر بالقوه ریسک‌ها بر این دارایی‌ها همسو شود.

---

[۳۸] Principles-based
[۳۹] proportionality principle
[۴۰] microenterprises
[۴۱] Principles-based regulation
[۴۲] prescriptive regulations
[۴۳] checking-the-boxes mindset

برای مثال، یک سیستم پردازش عملیات پرداخت که روزانه حجم زیادی از تراکنش‌ها را مدیریت می‌کند، در مقایسه با یک سیستم اداری داخلی کم‌اهمیت‌تر، به کنترل‌های سختگیرانه‌تر و اقدامات تاب‌آوری بیشتری نیاز دارد. این رویکرد هدفمند تضمین می‌کند که منابع به‌طور کارآمد تخصیص داده می‌شوند، مهم‌ترین ریسک‌ها مشخص هستند و در نتیجه امکان کاهش مؤثر مهم‌ترین ریسک‌ها فراهم می‌شود.

پویایی و بهبود مستمر

رویکرد مبتنی بر اصول، بر ماهیت پویای مدیریت ریسک و تاب‌آوری تأکید دارد. مؤسسات مالی باید به‌طور مداوم محیط‌های ریسک خود را رصد و ارزیابی مجدد کنند و کنترل‌ها و اقدامات خود را با ظهور تهدیدها و آسیب‌پذیری‌های جدید تطبیق دهند. برای حفظ تاب‌آوری در چشم‌انداز دیجیتالِ دائماً در حال تحول، برخورداری از یک فرآیند مداوم بهبود حائز اهمیت است.
DORA مؤسسات را تشویق می‌کند تا فرهنگ یادگیری و سازگاری مداوم را پرورش دهند. مؤسسات مالی با آزمایش منظم اقدامات تاب‌آوری، انجام تحلیل‌های سناریو و یادگیری از حوادث گذشته، می‌توانند آمادگی و قابلیت‌های پاسخگویی خود را افزایش دهند. این رویکرد فعالانه و پیشگیرانه نه تنها انتظارات نظارتی DORA را برآورده می‌کند، بلکه وضعیت امنیتی کلی مؤسسه را نیز تقویت می‌کند.

ادغام تاب‌آوری در استراتژی کسب‌وکار

در نظر گرفتن DORA به عنوان یک چارچوب مبتنی بر اصول، مستلزم ادغام تاب‌آوری عملیاتی دیجیتال در یک استراتژی کسب‌وکاری گسترده‌تر است. تاب‌آوری نباید یک اقدام ثانویه یا یک عملکرد جداگانه برای انطباق باشد، بلکه باید بخش جدایی‌ناپذیری از برنامه‌ریزی استراتژیک و فرآیندهای تصمیم‌گیری باشد. این ادغام تضمین می‌کند که ملاحظات تاب‌آوری در هر جنبه‌ای از کارکردهای موسسه، از توسعه محصول گرفته تا خدمات مشتری، گنجانده شده است.
بدنه مدیریتی نقش حیاتی در این ادغام ایفا می‌کند. این افراد باید از اهمیت تاب‌آوری حمایت کرده، منابع مناسب را اختصاص دهند و اطمینان حاصل کنند که اهداف تاب‌آوری با اهداف استراتژیک موسسه همسو هستند. تعهد از بالا به پایین برای ایجاد یک فرهنگ سازمانی تاب‌آور که امنیت و ثبات عملیاتی را در اولویت قرار می‌دهد، ضروری است.

حرکت فراتر از انطباق

در نهایت، باید به DORA به عنوان کاتالیزوری برای تغییر رویکرد موسسات مالی به تاب‌آوری عملیاتی دیجیتال نگریست. با پذیرش فلسفه مبتنی بر اصول آن، موسسات می‌توانند فراتر از تمرکز محدود بر انطباق با مقررات حرکت کرده و یک رویکرد استراتژیک جامع برای مدیریت ریسک اتخاذ کنند. این تغییر نه تنها انطباق را افزایش می‌دهد، بلکه باعث تعالی عملیاتی، نوآوری و اعتماد مشتری نیز می‌شود.

۵,۲. فرصت‌ها

در حالی که الزامات نظارتی اغلب به عنوان امری طاقت‌فرسا تلقی می‌شوند، قانون DORA به مؤسسات مالی فرصت قابل توجهی برای افزایش تاب‌آوری عملیاتی دیجیتال خود ارائه می‌دهد. این قانون به جای اینکه صرفاً یک الزام انطباق باشد، یک چارچوب استراتژیک ارائه می‌دهد که می‌تواند پیشرفت‌هایی غیر از مدیریت ریسک و ثبات عملیاتی فناوری اطلاعات و ارتباطات را به دنبال داشته باشد. همچنین می‌تواند اعتماد مشتری و رقابت‌پذیری کلی را در سراسر حوزه مالی افزایش دهد.

اعتماد مشتری

برای صنعت مالی که در عصر دیجیتال امروز فعالیت می‌کند، اعتماد و اطمینان از اهمیت بالایی برخوردار است. با رعایت الزامات سختگیرانه‌ی تاب‌آوری DORA، مؤسسات مالی می‌توانند تعهد خود را به حفاظت از دارایی‌های مشتریان و تضمین خدمات بدون وقفه نشان دهند. این تعهد به تاب‌آوری و امنیت، اعتماد بین مشتریان، شرکا و ذینفعان را ممکن می‌سازد. در نتیجه، مؤسسات مالی می‌توانند اعتبار خود را افزایش دهند، روابط قوی‌تری با مشتریان برقرار کنند و یک پایگاه مشتری وفادار ایجاد کنند که برای تعهد مؤسسه به تاب‌آوری دیجیتال ارزش قائل است.

مزیت‌های رقابتی

انطباق با DORA مستلزم پذیرش فناوری‌های پیشرفته و راه‌حل‌های نوآورانه برای مدیریت مؤثر ریسک‌های فاوا است. مؤسسات مالی که این الزامات را به عنوان فرصتی برای تحول دیجیتال می‌پذیرند، می‌توانند برتری رقابتی به دست آورند. با بهره‌گیری از ابزارهای پیشرفته امنیت سایبری، سیستم‌های مدیریت ریسک خودکار و روش‌های پیچیده آزمایش تاب‌آوری، مؤسسات استانداردهای نظارتی را رعایت می‌کنند و در عین حال خود را به عنوان پیشگامان تاب‌آوری دیجیتال معرفی می‌کنند. یک رویکرد فعالانه می‌تواند مشتریانی را جذب کند که امنیت و قابلیت اطمینان را در اولویت قرار می‌دهند و در نتیجه رشد کسب‌وکار و تمایز بازار را به همراه دارد.

قابلیت بازیابی[۴۴]

DORA با الزام به سازوکارهای بازیابی مستحکم[۴۵] و آزمایش‌های دقیق[۴۶] به منظور تضمین در دسترس بودن مستمر خدمات، فرصتی حیاتی را برای سازمان‌ها فراهم می‌کند تا قابلیت بازیابی دیجیتال خود را ارتقا دهند. با رعایت الزامات DORA، مؤسسات مالی می‌توانند به سرعت کارکردهای حیاتی را بازیابی[۴۷] کنند، زمان از کارافتادگی[۴۸] را به حداقل برسانند و از یکپارچگی داده‌ها[۴۹] در حین حوادث سایبری یا خرابی سیستم محافظت کنند. این امر نه تنها انطباق با مقررات را تضمین می‌کند، بلکه انعطاف‌پذیری عملیاتی را به یک مزیت استراتژیک تبدیل می‌کند.

۵.۳. چالش‌ها

اجرای DORA چالش‌های متعددی را برای مؤسسات مالی ایجاد می‌کند. در حالی که رویکرد مبتنی بر اصول DORA انعطاف‌پذیری و سازگاری را ارائه می‌دهد، تبدیل الزامات سطح بالا[۵۰]ی آن به اقدامات عملی[۵۱] می‌تواند پیچیده باشد. این امر می‌تواند هدایت و اجرای مؤثر را برای مدیریت دشوار کند.

تفسیر چند وجهی[۵۲]

یکی از چالش‌های اصلی DORA، الزام آن به تفسیر در حوزه‌های مختلف است. کارشناسان حقوقی ممکن است بر متن دقیق مقررات تمرکز نموده و بر رعایت و اجتناب از جریمه‌ها تأکید داشته باشند. متخصصان فناوری اطلاعات ممکن است جنبه‌های فنی، مانند امنیت سیستم و مکانیسم‌های واکنش به حوادث را در اولویت قرار دهند. مدیران کسب‌وکار احتمالاً نگران حفظ کارایی عملیاتی و همسوسازی اقدامات تاب‌آوری با اهداف استراتژیک گسترده‌تر هستند. ایجاد تعادل بین این دیدگاه‌ها برای تشکیل یک استراتژی منسجم و عملی می‌تواند چالش‌هایی را برای بسیاری از مؤسسات ایجاد کند.

---

۴۴ Recoverability
۴۵ robust recovery mechanisms
۴۶ diligent testing
۴۷ restore
۴۸ downtime
۴۹ data integrity
۵۰ broad requirements
۵۱ actionable measures
۵۲ Multifaceted interpretation

تبدیل اصول به اقدامات عملی

ماهیت مبتنی بر اصول DORA، در عین حال که انعطاف‌پذیری ارائه می‌دهد، می‌تواند یک شمشیر دولبه نیز باشد. فقدان رهنمودهای دستوری[۵۳] به این معنی است که موسسات مالی باید اقدامات خود را بر اساس پروفایل‌های ریسک منحصر به فرد خود تدوین کنند. با این حال، این امر مستلزم درک عمیق از الزامات نظارتی و ریسک‌های عملیاتی خاص فرا روی موسسه است. برای مدیریت، تبدیل این اصول کلی به اقدامات مشخص و عملی می‌تواند دلهره‌آور باشد. این امر نه تنها شامل شناسایی و ارزیابی ریسک‌ها، بلکه دربرگیرنده تعیین کنترل‌های مناسب و استراتژی‌های تاب‌آوری نیز می‌باشد. این فرآیند نیازمند تخصص و منابع قابل توجهی است که می‌تواند مانعی برای بسیاری از موسسات، به ویژه موسسات کوچک‌تر با ظرفیت محدود باشد.

نقش و مشارکت مدیریت

مدیریت نقش حیاتی در پیشبرد اجرای DORA ایفا می‌کند. با این حال، تبدیل الزامات فنی و قانونی به اقدامات استراتژیک تجاری، وظیفه‌ای پیچیده است که نیاز به رهبری و مشارکت قوی دارد. مدیریت نه تنها باید چشم‌انداز نظارتی را درک کند، بلکه باید بتواند اهمیت تاب‌آوری و امنیت را برای همه ذینفعان بیان کند.

بنابراین، مشارکت دادن مدیریت ارشد و اطمینان از تعهد آنها به تاب‌آوری عملیاتی دیجیتال بسیار مهم است. این امر شامل تأمین منابع لازم، تعیین اولویت‌های روشن و پرورش فرهنگی است که تلاش‌های تاب‌آوری را ارج می‌نهد و از آنها حمایت می‌کند. بدون رهبری و مشارکت قوی، اجرای DORA می‌تواند از هم گسیخته و در نهایت بی‌اثر شود.

توسعه یک چارچوب یکپارچه

با توجه به تفاسیر متنوع و نیاز به همکاری میان بخشی، ایجاد یک چارچوب واحد برای انطباق با DORA ضروری اما چالش برانگیز است. یک رویکرد پراکنده، که در آن بخش‌های مختلف به صورت جداگانه کار می‌کنند، می‌تواند منجر به ناهماهنگی و شکاف در اقدامات تاب‌آوری شود.

مؤسسات مالی به یک چارچوب جامع نیاز دارند که دیدگاه‌های حقوقی، فناوری اطلاعات و مدیریت کسب‌وکار را در یک استراتژی منسجم ادغام کند. این چارچوب باید ارتباطات شفاف، تفسیر منسجم از الزامات نظارتی و اقدام هماهنگ در تمام سطوح سازمان را تسهیل کند. دقیقاً به همین دلیل است که ما چارچوب کنترلی DORA را توسعه دادیم تا بر این چالش‌ها غلبه کنیم. این راهکار برای پر کردن شکاف بین اصول سطح بالای قانون و اقدامات عملی و قابل اجرا مورد نیاز برای انطباق و انعطاف‌پذیری طراحی شده است. این راهکار، کنترل‌های روشنی را برای کمک به مؤسسات مالی در جهت‌یابی پیچیدگی‌های DORA ارائه می‌دهد و تضمین می‌کند که آنها می‌توانند ضمن افزایش انعطاف‌پذیری عملیاتی دیجیتال خود، به انطباق دست یابند.

۶. DORA در چارچوب کنترلی

۶,۱. هدف مورد نظر

مؤسسات مالی با پیچیدگی‌های قانون تاب‌آوری عملیاتی دیجیتال دست و پنجه نرم می‌کنند که منجر به چالش‌هایی در اجرای کنترل‌های مؤثر می‌شود. از طریق گفتگوهایی که با متخصصان صنعت و تحقیقات گسترده بازار خود انجام دادیم، یک موضوع تکراری پدیدار شد: نیاز به یک چارچوب عملی که الزامات پیچیده DORA را ساده کند. برای این منظور، هدف اصلی چارچوب کنترلی DORA، تبدیل پیچیدگی‌های قانونی این قانون، به همراه ۱۰ RTS و ITS آن (به بخش ۴,۳,۳ مراجعه کنید)، به راهبردهای روشن و عملی برای مؤسسات مالی است.

در نهایت، این چارچوب در پی آن است که DORA را در دسترس و قابل اجرا قرار دهد و تضمین کند که مؤسسات مالی می‌توانند با اطمینان خاطر در چشم‌انداز نظارتی حرکت کنند و در عین حال عملیات خود را در برابر تهدیدات دیجیتال تقویت کنند. در

[۵۳] prescriptive guidelines

ساخت این چارچوب، ما به الزامات واقعی قانون پایبند ماندیم و از ایجاد هرگونه الزامات اضافی خودداری کردیم تا اطمینان حاصل شود که چارچوب صرفاً بر الزامات موجود در خود قانون تمرکز دارد.

۶,۲. نحوه پیاده‌سازی DORA در چهار مرحله

پیاده‌سازی DORA را می‌توان با موفقیت از طریق رویکرد ۴ مرحله‌ای زیر انجام داد که می‌تواند در پروژه‌های DORA در مؤسسات ادغام شود:

۱. هنگام اجرای DORA، اولین قدم ارزیابی کامل عملکردهای حیاتی و/ یا مهم سازمان است (ماده ۸,۱). این امر مستلزم بررسی جامع تمام فرآیندهای کلیدی و شناسایی زیرساخت فناوری اطلاعات و ارتباطات است که از عملیات این فرآیندها، از جمله اشخاص ثالث، پشتیبانی می‌کند و برای آنها ضروری است.
۲. مرحله بعدی انجام ارزیابی ریسک بر روی این زیرساخت فناوری اطلاعات و ارتباطات است که به ایجاد یک پروفایل ریسک و اولویت‌بندی حوزه‌هایی که نیاز به توجه دارند، کمک می‌کند.
۳. پس از ارزیابی ریسک، گام بعدی استقرار چارچوب کنترلی DORA برای انجام تحلیل شکاف خواهد بود. چنین تحلیلی مشخص می‌کند که موسسه در حال حاضر در چه جایگاهی نسبت به الزامات DORA قرار دارد و حوزه‌هایی را که نیاز به بهبود دارند، برجسته می‌کند.
۴. بر اساس یافته‌های تحلیل شکاف، گام نهایی باید تدوین یک طرح یا نقشه راه باشد که بر راه‌حل‌ها و اقدامات کاهشی[۵۴] برای پرداختن به شکاف‌های شناسایی‌شده و علل ریشه‌ای و اطمینان از انطباق با DORA تمرکز داشته باشد.

همانطور که در DORA تأکید شده است، مهم است که پروژه‌های پیاده‌سازی DORA مستقیماً تحت مسئولیت و نظارت نهاد مدیریت اجرا شوند. بنابراین، ارتباط مستمر با مدیریت برای حفظ مسئولیت‌پذیری و مشارکت آنها در سراسر فرآیند ضروری است. همانطور که در مرحله ۱ ذکر شد، مدیریت روابط با اشخاص ثالث حیاتی نیز به همان اندازه مهم است، به ویژه از آنجایی که مؤسسات مالی به‌طور فزاینده‌ای به خدمات فناوری اطلاعات برون‌سپاری شده متکی هستند؛ زنجیره قراردادی[۵۵] برای انطباق با DORA حیاتی می‌شود و اطمینان از اینکه همه روابط شخص ثالث با تاب‌آوری عملیاتی و تعهدات نظارتی مؤسسه همسو هستند، ضروری است.

۶,۳. توسعه چارچوب کنترلی

در تدوین چارچوب کنترلی DORA، تمرکز ما صراحتاً بر الزامات این قانون برای مؤسسات مالی بود. بنابراین، هرگونه الزام اختیاری یا الزاماتی که به نظارت، سرپرستی یا اطلاعات پیشینه اشاره داشتند را حذف نمودیم.

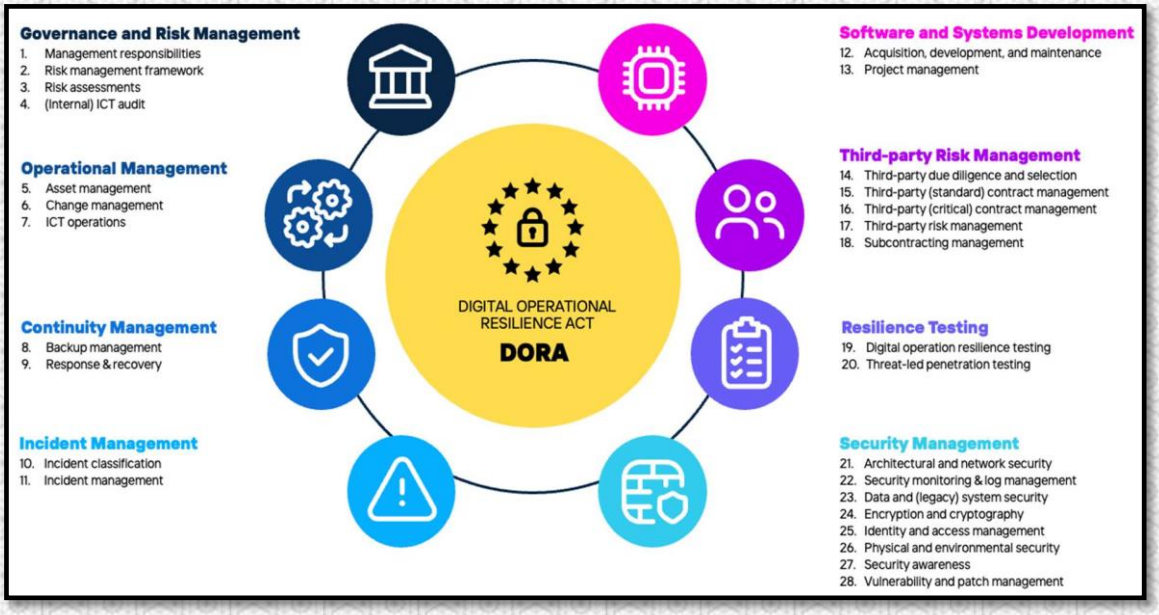
ساخت این چارچوب با تجزیه و تحلیل کامل الزامات قانونی اولیه (سطح ۱) و ثانویه (سطح ۲) آغاز شد. اولین قدم ما این بود که زبان حقوقی پیچیده را به قالبی قابل فهم‌تر برای همه ذینفعان تبدیل کنیم. پس از اینکه الزامات به عبارات ساده‌تر تبدیل شدند، از یک فرآیند ترکیب و تطبیق[۵۶] برای شناسایی موضوعات و الزامات همپوشانی استفاده کردیم. این امر به ما امکان داد تا الزامات تکی را در کنترل‌های عملی که می‌توانند به‌طور منطقی در حوزه‌های قابل تشخیص گروه‌بندی شوند، ادغام کنیم و کارایی بهبود یافته‌ای را هنگام انجام ارزیابی و پیاده‌سازی شکاف ارائه دهیم. هر کنترل با مفاد خاص DORA که از آنها مشتق شده بود، ارجاع متقابل[۵۷] داده شد که هم شفافیت و هم قابلیت ردیابی[۵۸] را افزایش می‌داد.

---

[۵۴] mitigating measures
[۵۵] chain of contracting
[۵۶] mix-and-match process
[۵۷] Cross-referenced
[۵۸] Traceability

فرآیند ما منجر به چارچوبی متشکل از ۸ دامنه کنترلی، ۲۸ زیر دامنه و ۹۵ کنترل واحد و مجزا[۵۹] شد. برای تجسم آن، به شکل زیر مراجعه کنید. در طول توسعه چارچوب، مدیران ریسک فناوری اطلاعات، مدیران ارشد امنیت اطلاعات و حسابرسان، یک فرآیند بررسی کامل را برای اطمینان از کیفیت چارچوب انجام دادند. همچنین، ما یک کاربرگ دقیق[۶۰] برای مستندسازی فرآیند ترجمه ایجاد کردیم که یک مسیر حسابرسی واضحی[۶۱] برای چگونگی تکامل چارچوب از متون قانونی DORA به کنترل‌های عملی فراهم می‌کند.

برای پشتیبانی بیشتر از پیاده‌سازی، مدل بلوغ برگرفته از "به‌روش امنیت اطلاعات" بانک مرکزی هلند[۶۲]، به همراه داشبوردی که کاربران را قادر می‌سازد پیاده‌سازی را تجسم کرده و در مورد پیشرفت آن اطلاع‌رسانی کنند، در چارچوب ادغام شده است.



شکل شماره ۴- چارچوب کنترلی DORA

۶,۴. ویژگی‌های کلیدی

چارچوب کنترلی DORA دارای چندین ویژگی طراحی کلیدی است که به منظور مقابله با پیچیدگی‌های این قانون و در عین حال ارائه راه‌حل‌های عملی و قابل اجرا تنظیم شده‌اند:

تفسیر حقوقی ساده شده: یکی از قابل توجه‌ترین ویژگی‌های این چارچوب، ترجمه اصطلاحات حقوقی پیچیده DORA به زبانی قابل فهم‌تر است.

کنترل‌های عملی تلفیقی[۶۳]: این چارچوب، الزامات خاص DORA را در مجموعه‌ای از کنترل‌های منسجم و قابل اجرا ادغام می‌کند. هر کنترل با مفاد خاص DORA ارجاع متقابل دارد که شفافیت را افزایش داده و قابلیت ردیابی را تسهیل می‌کند.

[۵۹] Individual controls
[۶۰] Detailed worksheet
[۶۱] Clear audit trail
[۶۲] Dutch Central Bank (DNB)
[۶۳] Consolidated actionable controls

ادغام مدل بلوغ DNB: برای کمک به مؤسسات در پیگیری پیشرفت خود، این چارچوب، مدل بلوغ DNB را از "به‌روش DNB برای امنیت اطلاعات[۶۴]" در بر می‌گیرد.

داشبورد پیشرفت بصری[۶۵]: این چارچوب شامل یک داشبورد برای ارائه نمایش بصری از پیشرفت پیاده‌سازی است. این ویژگی، روشی واضح و شهودی را برای مؤسسات فراهم می‌کند تا پیشرفت خود را پیگیری کرده و پیشرفت را به ذینفعان، از جمله مدیریت و نهادهای نظارتی، اطلاع دهند.

نقشه برداری از کنترل‌های DNB: این چارچوب شامل نگاشت کنترل‌ها در به‌روش DNB برای امنیت اطلاعات به کنترل‌های DORA است که به نیاز به گذار از استانداردهای موجود به چارچوب نظارتی جدید می‌پردازد. این ویژگی به ویژه برای مؤسساتی که به کنترل‌های DNB عادت دارند ارزشمند است؛ اگرچه با توجه به تصمیم DNB برای حذف تدریجی کنترل‌های خود به نفع DORA بسیار دارای اهمیت است.[۶۶] این نگاشت به مؤسسات کمک می‌کند تا رویه‌های خود را با الزامات DORA همسو کنند و در عین حال تداوم تلاش‌های انطباقی خود را حفظ کنند.

۶.۵. دیدگاه مهندسی

دیدگاه مهندسی مورد استفاده برای ساخت چارچوب کنترلی DORA بر تشریح و واکاوی پیچیدگی‌های قانون و استفاده از نظرات متخصصان برای حل چالش‌های ناشی از آن متمرکز بود. DORA مبتنی بر اصولی است که انعطاف‌پذیری را ارائه می‌دهد، اما برای امکان استفاده مؤثر از آن اصول، به تفسیر نیز نیاز دارد. ما معتقدیم که این دیدگاه مهندسی برای اجرای موفقیت‌آمیز DORA در مؤسسات مالی بسیار مهم است، زیرا بر اهمیت درک پیچیدگی‌های اساسی و علل ریشه‌ای ضمن اتخاذ یک رویکرد حل مسئله ساختاریافته و سیستماتیک تأکید دارد.

برای بهبود بیشتر اجرای صحیح کنترل‌های DORA در مؤسسات، به آنها توصیه می‌کنیم ستونی را برای مستندسازی گزینه‌های خاص اجرای کنترل خود اضافه کنند. این موارد باید بر اساس زمینه، تناسب و مشخصات ریسک مؤسسه انجام شود. برای انجام این کار از دیدگاه مهندسی، استفاده از روش 5W/1H را توصیه می‌کنیم. این روش شامل پرسیدن ۶ سوال حیاتی برای تجزیه و تحلیل صحیح مشکل و شناسایی راه‌حل است:

- **WHAT (چه چیزی)**: چه کنترل‌هایی مورد نیاز است؟ چه دارایی‌ها یا فرآیندهایی نیاز به حفاظت دارند؟ عواقب احتمالی و پیامدهای بالقوه عدم انجام کار چیست؟
- **WHO (چه کسی)**: چه کسی مسئول اجرا و نگهداری کنترل‌ها است؟ چه کسانی درگیر یا تحت تأثیر قرار می‌گیرند (کاربران، مشتریان یا اشخاص ثالث)؟
- **WHERE (کجا)**: کنترل‌ها کجا (مکان یا دارایی) اجرا خواهند شد؟ داده‌ها و منابع حساس کجا باید به‌طور ایمن ذخیره شوند؟

---

[۶۴] DNB Good Practice for Information Security

[۶۵] Visual progress dashboard

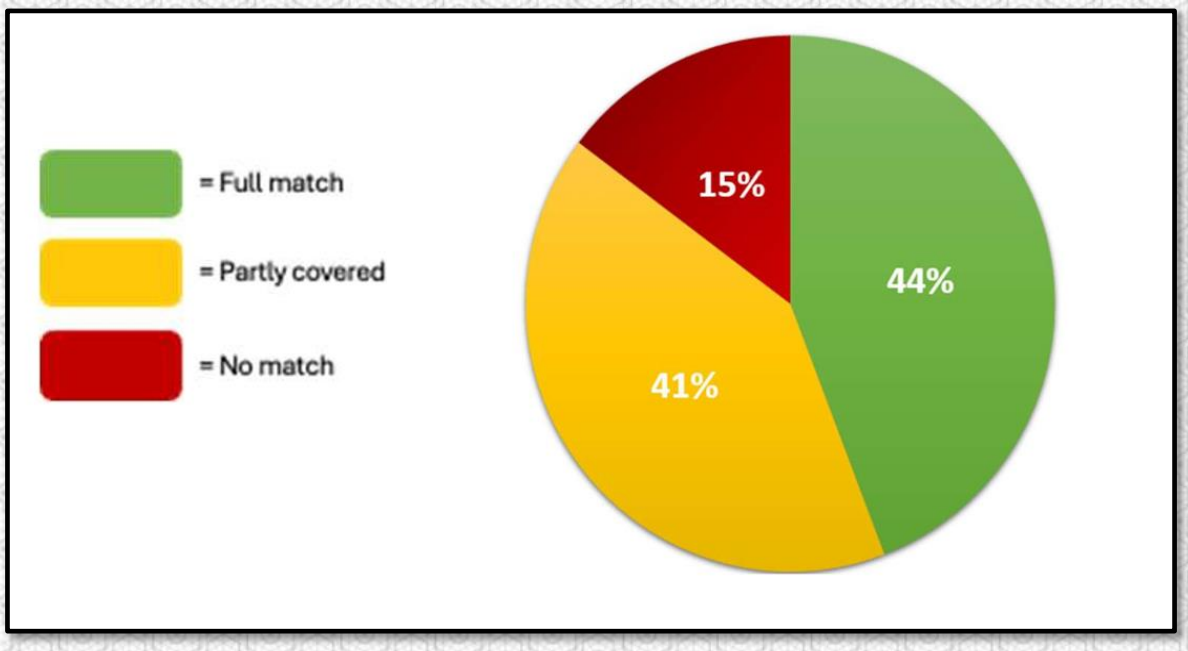
[۶۶] https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2024/dora-17-januari-2025-nadert-sneller-dan-u-denkt/

- **WHEN (چه زمانی)**: چه زمانی باید کنترل‌ها اجرا شوند؟ چه زمانی به‌روزرسانی‌ها و بررسی‌های کنترل‌ها انجام خواهد شد؟ چه زمانی آموزش و آگاهی‌رسانی به کاربران انجام خواهد شد؟
- **WHY (چرا)**: چرا این کنترل‌ها ضروری هستند؟ چرا این کنترل‌های خاص انتخاب شدند؟ چرا اقدامات موجود شکست خوردند؟
- **HOW (چگونه)**: چگونه کنترل‌ها پیاده‌سازی و اجرا خواهند شد؟ چگونه اثربخشی کنترل‌ها سنجیده می‌شود؟ چگونه مشکلات یا نقض‌ها مدیریت خواهد شد؟

۶,۶. نگاشت به‌روش DNB برای امنیت اطلاعات

در هلند، بسیاری از موسسات مالی عادت دارند برای پیاده‌سازی و گزارش امنیت سایبری، بر اساس "به‌روش DNB برای امنیت اطلاعات"[۶۷] از بانک مرکزی هلند استفاده کنند. بنابراین، چارچوب کنترلی DORA با کنترل‌های موجود در "به‌روش DNB برای امنیت اطلاعات ۲۰۲۳" تطبیق داده شده است. این تطبیق نشان می‌دهد که ۴۴٪ از کنترل‌های DORA قبلاً در کنترل‌های DNB لحاظ شده‌اند، در حالی که ۴۱٪ تا حدی تطبیق داده شده‌اند و ۱۵٪ کاملاً جدید هستند. برای مشاهده، به شکل ۵ مراجعه کنید.

لازم به ذکر است که این چارچوب از DNB اکنون با DORA جایگزین شده است و دیگر مورد استفاده قرار نخواهد گرفت. به عنوان جایگزین، نسخه ۳,۲ چارچوب کنترلی DORA شامل نگاشتی به دو پرسشنامه DNB DORA است: موسسات با درجه اهمیت متفاوت (مانند بانک‌ها) و SBA-Cyberweerbaarheid[۶۸] (شرکت‌های بازنشستگی و بیمه).



شکل شماره ۵- نتیجه نگاشت بین DORA در چارچوب کنترلی و به‌روش DNB برای امنیت اطلاعات ۲۰۲۳

[۶۷] https://www.dnb.nl/media/vskni24i/good-practice-ib-2023.pdf

[۶۸] https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2025/q4/vragenlijst-sba-cyberweerbaarheid-voor-de-pensioen-en-verzekeringssector-gepubliceerd/

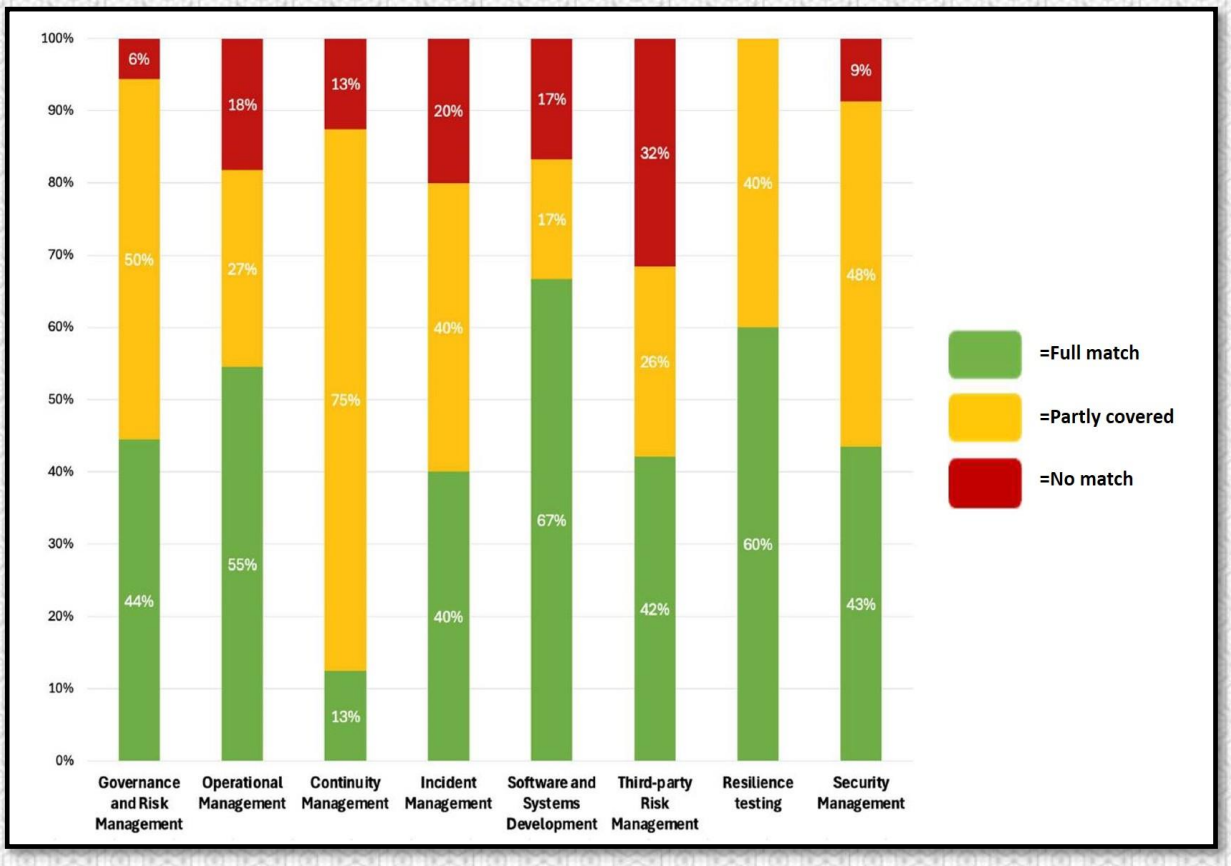
کنترل‌های DORA که عمدتاً توسط کنترل‌های DNB پوشش داده می‌شوند (بیش از ۵۰٪ همپوشانی) در حوزه‌های زیر قرار می‌گیرند:

۱) توسعه نرم افزار و سیستم
۲) مدیریت عملیاتی
۳) آزمایش تاب‌آوری

بزرگترین شکاف‌ها در تطابق بین کنترل‌های DORA و کنترل‌های DNB در حوزه‌های زیر قرار دارند:

۱) مدیریت تداوم
۲) مدیریت امنیت
۳) مدیریت ریسک شخص ثالث
۴) مدیریت حوادث

برای تجسم چگونگی همپوشانی هر هشت حوزه، لطفاً به شکل زیر مراجعه کنید.



شکل شماره ۶- نگاشت به‌روش DNB برای امنیت اطلاعات ۲۰۲۳ به DORA در چارچوب کنترلی به ازای هر دامنه

۶,۷. چک‌لیست کنترلی DORA

۶,۷,۱.فهرست نسخ و راهنمای انتشار

شماره نسخه	تاریخچه تغییرات نسخ	تغییرات
V1.0	2023-11-17	Initial version
V2.0	2024-08-30	Second version (with final RTS/ITS)
V3.0	2024-10-31	Final version (after DORA taskforce review and NOREA review)
V3.1	2025-05-14	Multiple changes to 16 controls. See tab "Detailed change log" for all changes performed.
V3.2	2025-11-25	Addition of Proportionality (column I) Addition of the DNB DORA questions (columns J & K) Small changes to 10 controls Changes to several RTS tabs to reflect final RTS text.

توضیحات تکمیلی و فهرست تغییرات دقیق در فایل اکسل اشاره شده موجود است.

مجوز DORA در چارچوب کنترلی و داشبورد

چارچوب کنترلی DORA و داشبورد NOREA تحت مجوز Creative Commons BY 4.0 منتشر می‌شود. اطلاعات بیشتر:
https://creativecommons.org/licenses/by/4.0

شما مجاز هستید که:

اشتراک‌گذاری - مواد را در هر رسانه یا قالبی کپی و بازتوزیع کنید؛

تطبیق - مواد را بازترکیب، تغییر داده و برای هر هدفی، حتی تجاری، توسعه دهید.

مجوزدهنده نمی‌تواند این آزادی‌ها را باطل کند تا زمانی که شما شرایط مجوز را رعایت کنید.

تحت شرایط زیر:

ارجاع - شما باید اعتبار مناسب بدهید، لینک مجوز را ارائه کنید و و در صورت ایجاد تغییرات، آن را اعلام کنید.

می‌توانید این کار را به هر روش معقولی انجام دهید، اما به هیچ شکلی نباید طوری به نظر برسد که دارنده مجوز از شما یا استفاده‌تان حمایت می‌کند.

سلب مسئولیت

چارچوب DORA در کنترل NOREA یک ابزار عملی است که با هدف حمایت از سازمان‌ها در مسیر دستیابی به انطباق با قانون تاب‌آوری عملیاتی دیجیتال (DORA) طراحی شده است. در حالی که این چارچوب راهنمایی‌های ارزشمندی ارائه می‌دهد، لازم به ذکر است که الزامات قانونی مندرج در خود قانون DORA همچنان الزامی و اصلی هستند.

بازخورد و سوالات

بازخورد و سوالات را می‌توان به آدرس زیر ارسال کرد: norea@norea.nl

مواد تکمیلی

تمام اسناد مربوط به DORA را می‌توانید از اینجا دانلود کنید: https://www.norea.nl/dora

۶،۷،۲ دامنه ها، زیر دامنه ها و مراجع

دامنه	شناسه	زیردامنه و تعداد کنترل	منابع DORA (L1 و L2)
GRM. Governance and Risk Management	1	GRM.1 Management responsibilities (5)	DORA: 5.1, 5.2, 5.3, 5.4, 6.8, 13.4 RTS TPPM: 3.1, 3.5, 4, 8.4
	2	GRM.2 Risk management framework (6)	DORA: 6.1, 6.2, 6.3, 6.4, 6.5, 6.7, 6.9, 6.10, 8.1, 9.1, 9.4, 11.1, 11.3, 11.6, 12.1, 12.2, 12.3, 14.2, 24.1, 28.2,28.3 RTS RM: 1.1, 2.1, 2.2, 3.1, 8.1, 8.2 RTS TPPM: 3.1, 3.2, 3.3, 3.4, 3.6, 3.7, 4.1, 7.1, 7.2
	3	GRM.3 Risk assessments (3)	DORA: 8.2, 8.3, 8.4, 8.7, 13.1
	4	GRM.4 (Internal) ICT audit (4)	DORA: 6.6, 11.3, 13.7, 28.6 RTS TPPM: 3.8, 8.1, 8.2, 8.3
OM. Operational Management	5	OM.1 Asset management (3)	DORA: 7, 8.1, 8.5, 8.6 RTS RM: 4.1, 4.2, 5.1, 5.2
	6	OM.2 Change management (4)	RTS RM: 8.1, 8.2, 17.1, 17.2
	7	OM.3 ICT operations (4)	RTS RM: 8.1, 8.2, 9.1, 9.2, 12.2
CM. Continuity Management	8	CM.1 Backup management (2)	DORA: 12.1, 12.2, 12.3, 12.6, 12.7
	9	CM.2 Response & recovery (6)	DORA: 11.1, 11.2, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 12.5, 14.1 RTS RM: 24.1, 24.2, 24.3, 24.4, 25.1, 25.2, 25.3, 25.4, 25.5, 25.6, 26.1, 26.2, 26.3, 26.4
IM. Incident Management	10	IM.1 Incident classification (2)	DORA: 18.1, 18.2, 45.1, 45.2, 45.3 RTS IM: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	11	IM.2 Incident management (3)	DORA: 13.2, 14.3, 17.1, 17.2, 17.3, 19.1, 19.2, 19.3, 19.4, 19.5 RTS RM: 22.1, 23.1, 23.5 RTS/ITS MIR: 1.1, 2.1, 3.1, 4.1, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1
SSD. Software and Systems Development	12	SSD.1 Acquisition, development, and maintenance (4)	RTS RM: 16.1, 16.2, 16.3, 16.4, 16.5
	13	SSD.2 Project management (2)	RTS RM: 15.1, 15.2, 15.3, 15.4, 15.5
TPRM. Third-party Risk Management	14	TPRM.1 Third-party due diligence and selection (2)	RTS TPPM: 3.5, 3.9, 5.2, 6.1, 6.2, 6.3
	15	TPRM.2 Third-party (standard) contract management (5)	DORA: 28.7, 30.1, 30.2 RTS TPPM: 3.9
	16	TPRM.3 Third-party (critical) contract management (3)	DORA: 26.4, 30.3, 30.4 RTS TPPM: 9.1, 9.2 RTS SCM: 4.1, 4.2, 6.1
	17	TPRM.4 Third-party risk management (6)	DORA: 8.5, 11.4, 28.1, 28.3, 28.4, 28.5, 28.6, 28.8, 29.1, 29.2 RTS TPPM: 3.8, 4.1, 10.1 RTS ROI
	18	TPRM.5 Subcontracting management (3)	RTS SCM: 1, 2, 3.1, 3.2, 3.3, 4, 5.1, 5.2
RT. Resilience Testing	19	RT.1 Digital operation resilience testing (3)	DORA: 24.1, 24.2, 24.3, 24.4, 24.5, 24.6, 25.1
	20	RT.3 Threat-led penetration testing (2)	DORA: 26.1, 26.2, 26.3, 26.5, 26.6, 26.7, 26.8, 27.1, 27.2, 27.3 RTS TLPT: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,12, 13
SM. Security Management	21	SM.1 Architectural and network security (3)	DORA: 9.4 (b), 12.4 RTS RM: 13.1, 13.2
	22	SM.2 Security monitoring & log management (3)	DORA: 10.1, 10.2, 10.3, 10.4 RTS RM: 9.1, 9.2, 12.1, 12.2, 23.2,23.3, 23.4
	23	SM.3 Data and (legacy) system security (5)	DORA: 9.2, 9.3 RTS RM: 11.2, 20.1

دامنه	شناسه	زیردامنه و تعداد کنترل	منابع DORA (L1 و L2)
	24	SM.4 Encryption and cryptography (2)	RTS RM: 6.1, 6.2, 6.3, 6.4, 6.5, 7.1, 7.2, 7.3, 7.4, 7.5
	25	SM.5 Identity and access management (4)	RTS RM: 20.1, 20.2, 21.1
	26	SM.5 Identity and access management (4)	RTS RM: 18.1, 18.2, 21.1
	27	SM.7 Security awareness (2)	DORA: 5.2, 13.6 RTS RM: 19.1
	28	SM.8 Vulnerability and patch management (3)	DORA: 25.2 RTS RM: 10.1, 10.2, 10.3, 10.4

۶,۷,۳. چک‌لیست کنترلی DORA

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
GRM. Governance and Risk Management			
GRM1 Management responsibilities **مسئولیت‌های مدیریت**	1.1	Governance of ICT risk (حاکمیت ریسک فاوا)	**ارکان مدیریتی** باید مسئولیت نهایی **مدیریت اثربخش تمامی ریسک‌های فاوای** موسسه مالی را بر عهده داشته باشد. بر این اساس، ارکان مدیریتی به‌صورت دوره‌ای *(برای مثال، سالانه)* موارد زیر را تضمین می‌کند: • سیاست‌نامه‌های مرتبط با **دسترس‌پذیری، اصالت، یکپارچگی** و **محرمانگی** داده‌ها ، از جمله سیاست‌نامه مربوط به **پیمانکاران فاوا** ، را تدوین کند *(کنترل ۲,۱ را مشاهده کنید).* • نقش‌ها، مسئولیت‌ها و ملاحظات حاکمیتی مربوط به **مدیریت ریسک** تمامی واحدهای مرتبط با فاوا *(از جمله موارد مرتبط با راهبران و همچنین مسائل مربوط به پیمانکاران فاوا)*، از جمله **پایش مستمر** آن‌ها را تعریف کند. • سیاست‌نامه مربوط به پیمانکاران فاوا را بازبینی کند و نسبت به قراردادهای پیمانکاران، خدمات ارائه‌شده، تغییرات بااهمیت برنامه‌ریزی‌شده مربوط به پیمانکاران، آگاه باشد و همچنین تأثیر این تغییرات بر **خدمات حیاتی و مهم** موسسه را *(از جمله نتایج ارزیابی ریسک)* درک کند.
	1.2	Knowledge of the Management Body (دانش و آگاهی ارکان مدیریتی)	**ارکان مدیریتی** باید اطمینان حاصل کند که دانش و مهارت‌های خود را به‌روز نگه می‌دارد تا بتواند **ریسک‌ها** و **عملیات فاوا** را درک و ارزیابی کند *(برای مثال، از طریق آموزش‌های دوره‌ای).*
	1.3	Digital Operational Resilience Strategy (راهبرد تاب‌آوری عملیاتی دیجیتال)	**ارکان مدیریتی** باید راهبرد **تاب‌آوری عملیاتی دیجیتال** را تعیین و تصویب کرده و در صورت نیاز، آن را به‌صورت دوره‌ای به‌روزرسانی کند. راهبرد تاب‌آوری عملیاتی دیجیتال باید: • مشخص کند که **چارچوب مدیریت ریسک** چگونه پیاده‌سازی خواهد شد. • هم‌راستایی میان **چارچوب مدیریت ریسک** و **راهبرد و اهداف کسب‌وکار** را تشریح کند. • **سطح تحمل ریسک فاوا** *(اشتهای ریسک)* و **سطح تحمل اثر اختلالات فاوا** را تعیین کند. • شامل **اهداف امنیتی شفاف**، از جمله **شاخص‌های کلیدی عملکرد (KPIs)** و **معیارهای ریسک** باشد. • **معماری مرجع فاوا** و هرگونه تغییرات مورد نیاز برای دستیابی به اهداف مشخص کسب‌وکار را تشریح کند. • سازوکارهای موجود برای **شناسایی رخدادهای مرتبط با فاوا** را تبیین کند.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			• شامل شواهدی برای اثبات و ضعیت فعلی **تاب‌آوری عملیاتی دیجیتال** با شد *(برای مثال، بر ا ساس تعداد رخدادهای عمده مرتبط با فاوا و اثربخشی اقدامات پیشگیرانه).* • نحوه اجرای **آزمون‌های تاب‌آوری عملیاتی دیجیتال** را مشخص کند *(کنترل‌های ۱۹ و ۲۰ را مشاهده کنید).* • **راهبرد ارتباطات** در صورت وقوع رخدادها را تبیین کند (۱۱,۳ *را مشاهده کنید).* **ارکان مدیریتی سازمان (هیأت مدیره)** می‌بایست بودجه لازم به منظور تأمین منابع موردنیاز جهت رفع نیازهای تاب‌آوری عملیاتی دیجیتال مو س سه را تخ صیص داده و مورد بازنگری قرار دهد. همچنین باید اطمینان حا صل کند که سازوکار **پایش اثربخ شی پیاده سازی تاب‌آوری عملیاتی دیجیتال** پیاده‌سازی شده است.
	1.4	Business Continuity Oversight (نظارت بر تداوم کسب‌وکار)	**ارکان مدیریتی** باید **سیا ست‌نامه تداوم کسب‌وکار فاوا** و **برنامه‌های پا سخ و بازیابی فاوا** را به‌صورت دوره‌ای *(برای مثال، سالانه* بازبینی و تصویب کند.)
	1.5	Audit Plan Approval and Review (تصویب و بازبینی برنامه حسابرسی)	**ارکان مدیریتی** می‌بایست به‌صورت دوره‌ای (برای مثال، سالانه) **برنامه‌های حسابرسی داخلی فاوا، ممیزی‌های فاوا و تغییرات اساسی در حسابرسی‌ها** را بازبینی و تصویب می‌کند.
GRM.2 Risk management framework **چارچوب مدیریت ریسک**	2.1	Protection Measures (اقدامات حفاظتی)	**پیاده سازی سیا ست‌نامه‌ها و رویه‌ها برای حفاظت از تمامی اطلاعات، دارایی‌های فاوا و اجزای فیزیکی و زیر ساخت‌های مرتبط فاوا ضروری است.** حداقل سیاست‌نامه‌های زیر باید تدوین و نگهداری شوند: • سیاست‌نامه امنیتی؛ • سیاست‌نامه منابع انسانی؛ • سیاست‌نامه کنترل‌های رمزگذاری و رمزنگاری؛ • سیاست‌نامه مدیریت هویت و دسترسی(IAM)؛ • سیاست‌نامه مدیریت تغییرات؛ • سیاست‌نامه امنیت شبکه؛ • سیاست‌نامه‌ها و رویه‌های عملیاتی فاوا؛ • سیاست‌نامه ارتباطات (در شرایط بحران)؛ • سیاست‌نامه مدیریت آسیب‌پذیری و وصله‌های امنیتی؛ • سیاست‌نامه پشتیبان‌گیری؛ • سیاست‌نامه مدیریت پروژه؛

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			• سیاست‌نامه امنیت فیزیکی و محیطی؛ • سیاست‌نامه تداوم کسب‌وکار همراه با برنامه‌های پاسخ و بازیابی (شامل برنامه‌های آزمون)، مطابق کنترل ۱،۴؛ • سیاست‌نامه مدیریت پیمانکاران فاوا، مطابق کنترل ۱،۱؛ • مدیریت و عملیات دارایی‌های فاوا (شامل تضمین امنیت شبکه، حفاظت در برابر نفوذ و سوءاستفاده از داده‌ها، و تعریف نحوه بهره‌برداری، پایش، کنترل و بازیابی دارایی‌های فاوا، از جمله مستندسازی عملیات فاوا). این موارد باید توسط ارکان مدیریتی تصویب شوند.
	2.2	Critical and Important Functions (کارکردهای حیاتی و مهم)	**شناسایی، طبقه‌بندی و مستندسازی مناسب تمامی عملیات و خدمات حیاتی و مهم الزامی است. این فرآیند شامل تعیین مواردی است که برای ثبات عملیاتی و تداوم فعالیت واحد ضروری‌اند. این طبقه‌بندی باید در صورت نیاز و حداقل سالی یک‌بار، از نظر کفایت مورد بازنگری قرار گیرد.**
	2.3	Clear Segregation of Duties (SoD) (تفکیک واضح وظایف)	**تفکیک وظایف (SoD) در ارتباط با فعالیت‌های کارکردی مدیریت ریسک باید بر اساس مدل سه خط دفاعی یا مدل داخلی مدیریت و کنترل ریسک برقرار شود.**
	2.4	ICT Risk management framework (چارچوب ریسک فناوری اطلاعات و ارتباطات)	**چارچوبی جامع**، مستحکم و مستندسازی‌شده از **مدیریت ریسک فاوا** استقرار یابد که پوشش‌دهنده تمامی ریسک‌های فاوا بوده و زمینه حفظ و ارتقای تاب‌آوری عملیاتی دیجیتال را فراهم آورد. مسئولیت راهبری، نظارت و مدیریت ریسک‌های فاوا نیز باید به‌طور مناسب به یک واحد کنترلی مستقل تخصیص یابد. چارچوب مدیریت ریسک فاوا باید مستندسازی شده و حداقل سالانه بازبینی شود، یا در مورد **سازمان‌های کوچک (microenterprises)** به‌صورت دوره‌ای بازبینی گردد؛ با این تفاوت که در صورت وقوع **رخدادهای عمده مرتبط با حوزه فاوا** یا دریافت **بازخوردهای مرتبط با مراجع نظارتی**، بازبینی‌های فوری انجام می‌شود. بهبود مستمر باید از طریق ادغام **درس‌آموخته‌های عملیاتی** از اجرا، پایش و حسابرسی‌ها تضمین گردد. گزارش بازبینی باید مطابق الزامات فصل ۵ (ماده ۲۷) از **RTS RM** تهیه شده و در صورت درخواست، برای ارائه به مرجع ذی‌صلاح در دسترس قرار گیرد. استانداردهای جدید و تحولات مرتبط با فناوری در حوزه **امنیت اطلاعات، امنیت سایبری و تاب‌آوری** باید به صورت مستمر ارزیابی شوند و پیشنهادهایی برای تقویت اقدامات کنترلی امنیت اطلاعات و امنیت سایبری سازمان ارائه گردد. این چارچوب باید به‌طور صریح به **ریسک‌های باقیمانده فاوا** که پس از اجرای اقدامات مدیریت ریسک باقی می‌مانند، پرداخته و شامل موارد زیر باشد: • شناسایی و مستندسازی تمامی ریسک‌های باقیمانده فاوا؛ • تخصیص نقش‌ها و مسئولیت‌های روشن برای پذیرش ریسک‌های باقیمانده فاوا (ایجاد Raci Chart برای ریسک‌های باقی‌مانده فاوا)، به‌ویژه آن‌هایی که از سطح تحمل ریسک تعیین‌شده سازمان فراتر می‌روند؛ • نگهداری یک فهرست به‌روز از ریسک‌های باقیمانده پذیرفته‌شده فاوا، همراه با دلایل پذیرش آن‌ها؛ • انجام بازبینی حداقل سالانه ریسک‌های باقیمانده پذیرفته‌شده حوزه فاوا.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
	2.5	Annual Framework Review and Audit Process (بازبینی سالانه چارچوب و فرآیند حسابرسی)	**اثربخشی چارچوب مدیریت ریسک بر اساس میزان مواجهه با ریسک در طول زمان نسبت به کارکردهای حیاتی یا مهم کسب‌وکار تحت پایش قرار گیرد.** **فرآیند بازبینی و ارزیابی حسابرسی بایستی** شامل حداقل بازبینی سالانه چارچوب بوده و همچنین در صورت وقوع رخدادهای عمده فاوا، صدور دستور از سوی نهاد ناظر، یا یافته‌های مهم حسابرسی، به‌صورت موردی فعال گردد. وظایف مربوط به **راستی‌آزمایی انطباق با الزامات مدیریت ریسک فاوا** می‌تواند به واحدهای درون‌سازمانی یا پیمانکاران برون‌سپاری شود. در صورت برون‌سپاری، **موسسه مالی همچنان به‌طور کامل مسئول تأیید انطباق با الزامات مدیریت ریسک فاوا باقی می‌ماند.**
	2.6	Third-Party (Multivendor) Risk Management Program (برنامه مدیریت ریسک طرف‌های ثالث (چندفروشنده‌ای))	**برنامه جامع مدیریت ریسک پیمانکاران (اشخاص ثالث) باید وجود داشته باشد که شامل موارد زیر است:** • وجود اطلاعات مربوط به همکاری با پیمانکاران، به‌ویژه پیمانکارانی که **خدمات حیاتی یا مهم موسسه** را پشتیبانی می‌کنند *(همچنین کنترل ۱۷،۳ را مشاهده کنید).* • استقرار **سیاست‌نامه مدیریت پیمانکاران فاوا**، شامل معیارهای تعیین **حیاتی بودن خدمات پیمانکاران** و همچنین **مسئولیت‌های داخلی برای مدیریت پیمانکاران.** • حصول اطمینان از اینکه **مدیریت ارشد** این سیاست‌نامه را بازبینی کرده و یک عضو (نقش) را برای **پایش روابط با پیمانکاران و اطمینان از رعایت الزامات قراردادی** را تعیین می‌کند. • راهبرد چند تامین کننده‌ای جامع (در صورت مرتبط بودن) که وابستگی‌های کلیدی به پیمانکاران فاوا را نشان داده و دلایل و ملاحظات مؤثر در انتخاب و ترکیب تأمین‌کنندگان پیمانکاران فاوا (Procurement Mix) را تشریح نماید.
GRM.3 Risk assessments **ارزیابی‌های ریسک**	3.1	Risk assessment (ارزیابی ریسک)	**شناسایی تمامی منابع ریسک فاوا باید به صورت مستمر انجام شود، از جمله طرح مواجهه ریسک به/ و از سایر واحدها یا نهادها. اطلاعات مربوط به تهدیدهای سایبری و آسیب‌پذیری‌های فاوا مرتبط با کارکردهای کسب‌وکار و دارایی‌ها باید جمع‌آوری، ارزیابی و حداقل به‌صورت سالانه بازبینی شود. همچنین باید اثر (بالقوه) این تهدیدها و آسیب‌پذیری‌ها بر دارایی‌ها مورد ارزیابی قرار گیرد.**
	3.2	Major change risk assessment (ارزیابی ریسک تغییرات عمده)	**در صورت بروز هرگونه تغییر عمده در شبکه، زیر ساخت فاوا، فرآیندها یا رویه‌های مؤثر بر خدمات و دارایی‌های کسب‌وکار، انجام ارزیابی ریسک الزامی است.**
	3.3	Legacy Systems risk assessment (ارزیابی ریسک سیستم‌های به ارث رسیده (قدیمی))	**ارزیابی‌های ریسک اختصاصی برای تمامی سیستم‌ها، برنامه‌ها یا زیر ساخت‌های قدیمی فاوا حداقل سالانه انجام شود. همچنین ارزیابی‌ها باید پیش از اتصال و پس از اتصال سیستم‌ها، برنامه‌ها یا سامانه‌های قدیمی فاوا انجام شوند.**
GRM.4 (Internal) ICT audit	4.1	Audit approach and frequency	**واحد حسابرسی داخلی باید حسابرسی‌هایی را در حوزه‌های زیر انجام دهد:**

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
حسابرسی (داخلی) فاوا		(رویکرد و تناوب حسابرسی)	• چارچوب مدیریت ریسک، سیاست‌نامه‌ها، فرآیندها و رویه‌های مرتبط؛ • برنامه‌های پاسخ و بازیابی فاوا؛ • پیمانکاران فاوا. تناوب و تمرکز حسابرسی باید بر اساس **پروفایل ریسک فاوای موسسه** تنظیم شود.
	4.2	Auditor requirements (الزامات حسابرس)	**اطمینان حاصل شود که کارکنان حسابرسی داخلی دارای دانش، مهارت و تخصص کافی در حوزه ریسک فاوا برای انجام حسابرسی‌ها هستند. همچنین استقلال واحد حسابرسی باید تضمین گردد.**
	4.3	Audit findings (یافته‌های حسابرسی)	**فرآیندی به‌منظور پیگیری یافته‌های حسابرسی اجرا شود که شامل روالی جهت تأیید به‌موقع و اختتام یافته‌های حیاتی باشد. همچنین فرآیند یادگیری و بهبود مستمر بر اساس نتایج ارزیابی ریسک، آزمون‌های تاب‌آوری، حوادث (سایبری) و آزمون‌های برنامه‌های تداوم کسب‌وکار می‌بایست ایجاد گردد. نتایج این فرآیند باید به ارکان مدیریتی گزارش شده و به‌عنوان ورودی برای "گزارش سالانه بازبینی چارچوب مدیریت ریسک فاوا" مطابق فصل ۵ (ماده ۲۷) از RTS RM، مورد استفاده قرار گیرد.**
	4.4	Reliance Third-Party Assurance and Certifications (اتکاء به تضمین‌ها و گواهی‌های اشخاص ثالث)	در صورت لزوم، می‌توان از **اسناد، گزارش‌های حسابرسی اشخاص ثالث یا حسابرسی داخلی ارائه شده توسط پیمانکاران فاوا**، یا **گزارش‌های حسابرسی خود موسسه** استفاده کرد تا پایبندی به الزامات قراردادی مرتبط با **دسترسی به اطلاعات، بازرسی، حسابرسی و آزمون‌های فاوا** در ارتباط با پیمانکاران تأیید شود. اتکاء به **گواهی‌ها و گزارش‌های حسابرسی پیمانکاران حوزه فاوا** تنها در صورتی مجاز است که شرایط مشخص زیر برقرار باشد: • طرح حسابرسی با **توافقات و الزامات قراردادی** هم‌راستا باشد؛ • دامنه حسابرسی جامع بوده و **دارایی‌های شناسایی‌شده و کنترل‌های کلیدی** را پوشش دهد؛ • ارزیابی مستمر محتوای گواهی‌ها/ گزارش‌های انجام شده و صحت آن‌ها تأیید گردد؛ • در نسخه‌های بعدی گزارش حسابرسی، **دارایی‌ها و کنترل‌های کلیدی** همچنان پوشش داده شوند؛ • اطمینان از **توانمندی و صلاحیت نهاد صادرکننده گواهی یا موسسه حسابرسی** وجود داشته باشد؛ • حسابرسی‌ها مطابق با **استانداردهای حرفه‌ای شناخته‌شده** انجام شوند؛ • حق درخواست **گسترش دامنه حسابرسی** در قرارداد لحاظ شده باشد؛ • حق انجام **حسابرسی‌های اختیاری (discretionary)** برای واحد محفوظ باشد.
OM. Operational Management			
OM.1 Asset management **مدیریت دارایی‌ها**	5.1	Resilient Systems (سامانه‌های تاب‌آور)	**بهره‌برداری و نگهداری از سامانه‌ها، پروتکل‌ها و ابزارهای فاوا به‌روز بوده و دارای ویژگی‌های زیر باشند:** • متناسب با **مقیاس عملیات فاوا**؛ • **قابل اتکا (Reliable)**؛

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			• مجهز به ظرفیت کافی برای پردازش دقیق داده‌ها و مدیریت زمان اوج سفارشات، پیام‌ها یا تراکنش‌ها، حسب نیاز؛ • از منظر فناوری، به گونه‌ای تاب‌آور باشد که بتواند نیازهای پردازشی اضافی ناشی از شرایط تنش‌زا یا سایر شرایط نامساعد (کسب‌وکار) را مدیریت کند.
	5.2	Inventory Management (مدیریت موجودی)	**فهرستی از دارایی (موجودی)های فاوا نگهداری شود، چرخه عمر آن‌ها پایش گردد و به‌صورت دوره‌ای و همچنین در هر تغییر عمده در شبکه، زیرساخت فناوری اطلاعات و فرآیندها و رویه‌های پشتیبانی واحدهای کسب‌وکاری به‌روزرسانی شود.** برای هر دارایی فاوا، سوابق زیر نگهداری گردد: • شناسه یکتا؛ • محل استقرار (فیزیکی یا منطقی)؛ • طبقه‌بندی دارایی؛ • هویت مالک دارایی؛ • اطلاعات لازم برای ارزیابی ریسک اختصاصی سیستم‌های قدیمی (Legacy Systems)؛ • امور یا خدمات کسب‌وکار پشتیبانی‌شده؛ • الزامات تداوم کسب‌وکار (مانند RTO، RPO)؛ • میزان مواجهه با شبکه‌های خارجی از جمله اینترنت؛ • ارتباطات و وابستگی‌ها بین دارایی‌ها و کارکردهای کسب‌وکار استفاده‌کننده از هر دارایی؛ • تاریخ پایان خدمات پشتیبانی عادی، تمدیدشده و سفارشی پیمانکاران فاوا، پس از آن‌که دارایی دیگر توسط تأمین‌کننده یا ارائه‌دهنده خدمات فاوا پشتیبانی نمی‌شود. در حالت ایده‌آل، **مدیریت دارایی به‌صورت خودکار و پیوسته** انجام می‌شود.
	5.3	Asset Classification and Documentation (طبقه بندی و مستندسازی دارایی‌ها)	**شناسایی، طبقه‌بندی و مستندسازی تمامی عملیات کسب‌وکاری پشتیبانی‌شده توسط فاوا، از جمله دارایی‌های پشتیبان آن‌ها، و تشریح نقش‌ها و وابستگی‌های این دارایی‌ها در ارتباط با ریسک فاوا الزامی است. همچنین باید تمامی واحدهای کسب‌وکاری وابسته به فاوا که از پیمانکاران فاوا استفاده می‌کنند شناسایی و مستندسازی شوند و خدمات ارائه‌شده توسط این پیمانکاران که از واحدهای حیاتی یا مهم پشتیبانی می‌کنند مشخص گردند.** **برای دارایی‌های حیاتی فاوا** بر مبنای ارزیابی سطح اهمیت و حیاتی بودن آن‌ها، **نگاشت (mapping) دارایی‌ها تهیه و نگهداری شود.که شامل موارد زیر باشد:** • **منابع شبکه؛** • **تجهیزات سخت‌افزاری؛** • **منابع مستقر در سایت‌های خارج از مرکز (اتاق‌های سرور و ...).**

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			این نگاشت باید همچنین شامل پیکربندی دارایی‌ها و ارتباطات و وابستگی‌های آن‌ها با سایر دارایی‌ها باشد. **ارزیابی اهمیت (Criticality Assessment)** باید بر اساس **معیارهای شفاف صورت** پذیرد تا ریسک فاوای مرتبط با امور کسب‌وکاری، با در نظر گرفتن تأثیر احتمالی از دست رفتن **محرمانگی، یکپارچگی و دسترس‌پذیری**، ارزیابی گردد. کفایت این طبقه‌بندی و مستند سازی باید حداقل به صورت سالانه بازبینی شود تا اطمینان حاصل گردد که الزامات مربوط به نگهداری سوابق دقیق و به‌روز دارایی‌ها رعایت می‌شود.
OM.2 Change management **مدیریت تغییرات**	6.1	Change Procedures (رویه تغییرات)	**اطمینان حاصل شود که تمامی تغییرات در اجزای حوزه‌های نرم‌افزاری، سخت‌افزاری، میان‌افزاری (Firmware) و سامانه‌ها، همراه با پارامترهای امنیتی، به‌طور مناسب تعریف و دامنه‌بندی (Scoped) می‌شوند.** جزئیات تغییر شامل **هدف و دامنه تغییر، زمان‌بندی اجرا، و نتایج مورد انتظار** باید مستندسازی و اطلاع‌رسانی شود. نقش‌ها و مسئولیت‌های مشخصی (RACI Chart) تعریف گردد تا اطمینان حاصل شود که تغییرات به‌صورت کنترل‌شده **تعریف، برنامه‌ریزی، پیاده‌سازی، آزمون و نهایی‌سازی** می‌شوند. همچنین باید **رویه‌های تضمین کیفیت (Quality Assurance)** مؤثر برقرار گردد. سازوکارهایی باید پیاده سازی شود تا **استقلال بین واحدها یا افرادی که تغییرات را تأیید می‌کنند و افرادی که مسئول درخواست و اجرای تغییرات هستند** حفظ شود.
	6.2	Security Requirements (الزامات امنیتی)	**شناسایی تأثیر بالقوه هر تغییر بر اقدامات امنیتی موجود و ارزیابی این موضوع که آیا برای اجرای آن تغییر، اقدامات امنیتی اضافی موردنیاز است یا خیر، الزامی است. همچنین باید اطمینان حاصل شود که تمامی الزامات امنیتی برای تغییرات اعمال شده رعایت شده‌اند.** رویه‌های **بازگشت به حالت قبلی (Fallback)** باید تعریف شده و مسئولیت‌ها برای **لغو تغییرات یا بازیابی در صورت عدم اجرای موفق تغییرات** به‌طور مشخص تعیین شوند.
	6.3	Emergency Change Management (مدیریت تغییرات اضطراری)	رویه‌هایی برای مستندسازی، ارزیابی، ارزیابی مجدد و تصویب اجرای تغییرات اضطراری، شامل راهکارهای موقت و وصله‌های ترمیمی، تعریف شود.
	6.4	OTAP / DTAP Implementation (پیاده‌سازی OTAP / DTAP)	**اطمینان حاصل شود که محیط‌های عملیاتی از محیط‌های توسعه، آزمون و سایر محیط‌های غیرعملیاتی به صورت مجزا هستند و این تفکیک شامل تمامی اجزای هر محیط می‌باشد. این الزامات همچنین شامل ممنوعیت یا محدودیت و کنترل استفاده از محیط عملیاتی برای فعالیت‌های توسعه و آزمون است.** همچنین باید اطمینان حاصل شود که مواردی که در آن **آزمون در محیط عملیاتی انجام می‌شود** به‌طور شفاف شناسایی و توجیه شده و برای **مدت‌زمان محدود** بوده و توسط **واحد ذی‌صلاح مربوطه** تأیید شده باشد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
OM.3 ICT operations **عملیات فاوا**	7.1	ICT Monitoring (پایش فناوری اطلاعات و ارتباطات)	**رویه‌های مدیریت ظرفیت و کارایی باید تدوین، مستندسازی و پیاده‌سازی شوند تا نیازهای ظرفیتی سامانه‌های فاوا شناسایی گردد و همچنین رویه‌های بهینه سازی منابع و پایش به‌کار گرفته شود تا د سترس‌پذیری داده‌ها و سامانه‌های فاوا و کارایی آن‌ها حفظ و بهبود یابد و از بروز کمبود ظرفیت فاوا جلوگیری شود.**
	7.2	Clock Synchronization Standardization (استانداردسازی همگام‌سازی ساعت)	**حصول اطمینان از همگام‌سازی ساعت تمامی سامانه‌های فاوا با یک منبع زمانی مرجع و قابل‌اعتماد یکتا، الزامی است.**
	7.3	System Management and Security (مدیریت و امنیت سامانه‌ها)	**ارائه مستندات راهنمای راهبری و کاربری سامانه‌ها، که شامل نصب امن، نگهداری، پیکربندی و حذف/ امحاء دارایی‌های فاوا با شد الزامی است. این موضوع بایستی شامل مدیریت دارایی‌ها، به صورت خودکار و دستی، و همچنین شناسایی و کنترل سیستم‌های قدیمی گردد.**
	7.4	Error Handling and Recovery (مدیریت خطا و بازیابی)	**راهنمایی‌هایی برای مدیریت خطاها باید تدوین شود که شامل اطلاعات پشتیبانی و گام‌های ارجاع، و همچنین اطلاعات تماس پشتیبانی در صورت بروز مشکلات عملیاتی یا فنی غیرمنتظره باشد.** رویه‌های مربوط به **راه‌اندازی مجدد سامانه‌های فاوا، بازگشت (Rollback) و بازیابی** باید در صورت وقوع اختلال در سامانه‌های فاوا تعریف شوند. همچنین باید اطمینان حاصل شود که **اطلاعات تماس در شرایطی که سامانه‌ها در دسترس نیستند نیز قابل دسترسی باشد.**
CM. Continuity Management			
CM.1 Backup management **مدیریت پشتیبانگیری**	8.1	Backup Policy (سیاست‌نامه پشتیبان‌گیری)	**تدوین سیاست‌نامه‌های پشتیبان‌گیری با هدف تضمین حداقل زمان توقف (Downtime)، محدودسازی اختلال و کاهش از دست‌رفتگی داده‌ها الزامی بوده و می‌بایست با رویه‌های بازیابی و بازگردانی نیز منطبق باشد.** دامنه داده‌های مشمول پشتیبان‌گیری و حداقل تناوب انجام پشتیبان‌گیری باید بر اساس **میزان حیاتی بودن یا سطح محرمانگی داده‌ها** تعیین شود. همچنین باید **زمان بازیابی هدف (RTO) و نقطه بازیابی هدف (RPO)** بر ا ساس سطح اهمیت داده‌ها و تأثیر آن بر کارایی کسب‌وکار تعیین گردد تا اطمینان حاصل شود که سطوح خدمات در سناریوهای بحرانی نیز قابل تحقق هستند.
	8.2	Restore Procedures (رویه‌های بازیابی)	**اطمینان حاصل گردد که فعال‌سازی سامانه‌های پشتیبان، امنیت، دسترس‌پذیری، اصالت، یکپارچگی و محرمانگی داده‌های سامانه های فاوا را به خطر نیندازد. این امر می‌تواند از طریق اجرای آزمون‌های دوره‌ای بازگردانی (Restore Test) مبتنی بر رویه‌های پشتیبان‌گیری، بازگردانی و بازیابی تحقق یابد.** همچنین باید اطمینان حاصل شود که در هنگام بازیابی داده‌های پشتیبان با استفاده از سامانه‌های خودکار، از سامانه‌هایی استفاده شود که از نظر **فیزیکی و منطقی از سامانه مبدأ تفکیک شده‌اند** تا از حفاظت مناسب اطمینان حاصل گردد. علاوه بر این، در رابطه با سامانه‌های پشتیبان بایستی تدابیری اندیشیده شود تا از هرگونه **دسترسی غیرمجاز یا خرابی سامانه‌ها و سرویس‌های فاوا جلوگیری شده و سامانه‌ها و**

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			سرویس‌ها به‌طور امن محافظت شوند و همچنین امکان بازیابی به‌موقع را فراهم سازد. مؤسسات باید تأیید کنند که در فرآیند بازیابی پشتیبان‌ها، **بالاترین سطح یکپارچگی داده‌ها حفظ می‌شود.** به‌طور خاص برای سامانه‌های **واسط [مانند اتاق تسویه پایاپای و غیره] (Central Counterparties)** برنامه‌های بازیابی باید امکان **بازیابی تمامی تراکنش‌ها در زمان وقوع اختلال** را فراهم کنند تا این سیستم‌ها بتوانند با اطمینان به فعالیت خود ادامه داده و عملیات تسویه را در تاریخ برنامه‌ریزی‌شده تکمیل کند. برای **ارائه‌دهندگان خدمات مرتبط با فعالیت‌های گزارش‌گری و گزارش‌دهی (DRSP)، باید علاوه بر موارد فوق، منابع کافی را حفظ کرده و تسهیلات پشتیبان‌گیری و بازگردانی** را در اختیار داشته باشند تا بتوانند خدمات خود را در تمام زمان‌ها ارائه داده و حفظ کنند. برای تعریف DRSP به لینک زیر مراجعه شود: *https://www.esma.europa.eu/esmasactivities/markets-and-infrastructure/datareporting-services-providers*
CM.2 Response & recovery **پاسخ و بازیابی**	9.1	Business Continuity Policy (سیاست‌نامه تداوم کسب‌وکار)	**سیاست‌نامه تداوم کسب‌وکار فاوا که امکان استمرار عملیات مربوط به فعالیت‌های حیاتی یا مهم را فراهم کند، تدوین شود؛ که پاسخ سریع به رخدادها را تضمین نماید، از سرگیری فعالیت‌ها را تسهیل کند، استقرار اقدامات مقابله و مهار (Containment) را ممکن سازد، و همچنین فعال‌سازی و غیرفعال‌سازی رویه‌های پاسخ و بازیابی را پوشش دهد. این سیاست‌نامه باید شامل برآورد اثر، خسارت و زیان‌ها بوده و ارتباطات شفاف با ذی‌نفعان مرتبط را فراهم سازد.** سیاست‌نامه تداوم کسب‌وکار باید به‌صورت منظم بازبینی شده و اصلاحات لازم برای افزایش اثربخشی در آن اعمال گردد. برای کسب اطلاعات بیشتر از الزامات خاص مرتبط با **واسط‌ها (Central Counterparties)، مکان‌های (یا پلتفرم‌های) معاملاتی (Trading Venues) و سپرده‌گذاری مرکزی اوراق بهادار (Central Securities Depositories)**، به مواد ۲۴,۲ تا ۲۴,۴ از RTS RM مراجعه کنید.
	9.2	Crisis Management (مدیریت بحران)	**نسبت به تشکیل یک تیم مدیریت بحران که مسئول نظارت و هماهنگی اقدامات در طول بحران یا اختلال عمده باشد، اقدام گردد. برنامه‌های پاسخ و بازیابی باید به‌صورت منظم بازبینی شده و اصلاحات لازم برای افزایش اثربخشی در آن‌ها اعمال گردد.**
	9.3	Record Keeping (نگهداری سوابق)	**سوابق تفصیلی از فعالیت‌های انجام‌شده پیش از، حین و پس از اختلالات و نتایج آن‌ها، باید نگهداری شود. همچنین باید برآوردی از هزینه‌ها و خسارات تجمیعی سالانه ناشی از اختلالات عمده ثبت و حفظ گردد. این اطلاعات باید در صورت درخواست مرجع ناظر، به آن ارائه شود.**
	9.4	Business Impact analysis (تحلیل تاثیر کسب‌وکار)	**تحلیل جامعی از تأثیر کسب‌وکار (BIA_Business Impact Analysis) در مواجهه با اختلالات شدید کسب‌وکار می‌بایست صورت‌پذیرد. این تحلیل باید با استفاده از معیارهای کمی و کیفی، داده‌های داخلی و خارجی و در صورت لزوم تحلیل سناریوها انجام گیرد.** **BIA** باید **اهمیت (Criticality)** کارکردهای کسب‌وکار شناسایی شده و شناسایی، توصیف و ترسیم شده، فرآیندهای پشتیبان، وابستگی به پیمانکاران و دارایی‌های اطلاعاتی، و همچنین وابستگی‌های متقابل آن‌ها را در نظر بگیرد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			واحدهای مالی باید اطمینان حاصل کنند که دارایی‌ها و خدمات فاوا به‌گونه‌ای طراحی و استفاده می‌شوند که به‌طور کامل با نتایج BIA هم‌راستا باشند؛ به‌ویژه در خصوص تضمین مناسب **افزونگی (Redundancy)** تمامی اجزای حیاتی.
	9.5	Response and Recovery (پاسخ و بازیابی)	**باید برنامه‌های جامع پاسخ و بازیابی شامل گزینه‌های بازیابی کوتاه‌مدت و بلندمدت تدوین شود. این برنامه‌ها باید به‌طور کامل سناریوهای احتمالی را شناسایی کنند (بر اساس اطلاعات به‌روز از تهدیدها و درس‌آموخته‌های ناشی از اختلالات قبلی کسب‌وکار) و به‌طور مقتضی سناریوهای زیر را در نظر بگیرند: حملات سایبری، تعویض سامانه از حالت اصلی به پشتیبان (Switchover)، افت کیفیت ارائه کارکردهای حیاتی، خرابی محل استقرار، اختلال در دارایی‌های فاوا یا زیرساخت‌های ارتباطی، عدم دسترسی کارکنان، بلایای طبیعی و اثرات تغییرات اقلیمی، بحران‌های همه‌گیر (مانند شیوع بیماری به‌صورت فراگیر)، حملات فیزیکی، تهدیدهای داخلی (Insider Threats)، بی‌ثباتی سیاسی یا اجتماعی و قطعی برق.** علاوه بر این، این برنامه‌ها باید گزینه‌های جایگزین را نیز در مواردی که اقدامات بازیابی اصلی به دلایل هزینه، ریسک، لجستیک یا شرایط پیش‌بینی‌نشده در کوتاه‌مدت غیرقابل اجرا هستند، در خود لحاظ کنند. همچنین باید احتمال **نقص یا اختلال در ارائه‌دهندگان خدمات کلیدی شخص ثالث فاوا** نیز در این برنامه‌ها پیش‌بینی شود.
	9.6	Testing and Assessment (آزمون و ارزیابی)	**برنامه‌های تداوم کسب‌وکار، پاسخ و بازیابی فاوا باید به صورت منظم، به‌ویژه با همکاری پیمانکاران که از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند، مورد آزمون قرار گیرند. این آزمون‌ها باید تأثیر (ریسک) بر کسب‌وکار (BIA) و ارزیابی ریسک فاوای مؤسسه مالی را در نظر گرفته و حداقل به‌صورت سالانه و همچنین در هر زمان که تغییرات قابل‌توجهی در سامانه‌های پشتیبان کارکردهای حیاتی یا مهم رخ می‌دهد، انجام شوند.** آزمون‌ها باید مبتنی بر سناریوهای واقع‌بینانه باشند و سناریوهایی مانند حملات سایبری، ورشکستگی یا از کار افتادن ارائه‌دهنده شخص ثالث، بازیابی از پشتیبان (Backup Restore) و جابه‌جایی بین سایت‌های اصلی و جایگزین (Switchover) را در برگیرند. این آزمون‌ها باید بررسی کنند که حداقل کارکردهای حیاتی یا مهم بتوانند به‌طور منا سب و برای مدت زمان کافی اجرا شوند و همچنین امکان بازگردانی عملکرد عادی فرآیندهای کسب‌وکار وجود داشته باشد. آزمون مربوط به برنامه‌های ارتباطی در زمان وقوع بحران نیز باید انجام شود تا اطمینان حاصل گردد که راهبردهای ارتباطی در شرایط بحران یا اختلال عمده اثربخش هستند. نتایج آزمون‌ها باید مستند گردیده و هرگونه نقص شناسایی‌شده به هیئت مدیره گزارش شود. برای الزامات خاص مربوط به **واسطه‌ها (Central Counterparties)** و **سپرده‌گذاری مرکزی اوراق بهادار (Securities Depositories)** به مواد ۲۴,۲ تا ۲۴,۳ از RTS RM مراجعه شود.
IM. Incident Management			
IM.1 Incident classification **طبقه‌بندی رخداد**	10.1	Incident Classification Criteria	**رخدادهای مرتبط با فناوری اطلاعات و ارتباطات باید بر اساس میزان اثر آن‌ها و با استفاده از معیارهای زیر طبقه‌بندی شوند:** • تعداد مشتریان/کاربران یا طرف‌های مالی متأثر؛

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
		(معیارهای طبقه‌بندی رخدادها)	• تعداد تراکنش‌های تحت تأثیر؛ • آسیب به اعتبار و شهرت سازمان؛ • مدت‌زمان رخداد و از کار افتادن خدمات؛ • گستره جغرافیایی رخداد؛ • میزان تلفات داده‌ها در ارتباط با **سه مؤلفه محرمانگی، یکپارچگی و دسترس‌پذیری (CIA Triad)**؛ • میزان حیاتی بودن خدمات تحت تأثیر؛ • و اثر کلی اقتصادی رخداد. یک رخداد در صورتی **عمده (Major)** تلقی می‌شود که: ۱. هرگونه **دسترسی غیرمجاز و مخرب** به شبکه‌ها و سامانه‌های اطلاعاتی شناسایی شود که ممکن است منجر به از دست رفتن داده‌ها گردد؛ ۲. آستانه‌های مربوط به **دو معیار ا ضافی** برآورده شوند *(برای مقادیر آستانه به سند DORA RTS IM (Major Incidents) مراجعه شود)*. همچنین **رخدادهای تکرارشونده** نیز باید مدنظر قرار گیرند. رخدادهای تکرارشونده در صورتی عمده محسوب می‌شوند که: ۱. رخدادها حداقل **دو بار در بازه ۶ ماهه** رخ داده باشند؛ ۲. رخدادها دارای **علت ریشه‌ای در ظاهر یکسان** باشند؛ ۳. رخدادها در مجموع به‌عنوان **رخداد عمده** طبقه‌بندی شوند. برای جزئیات کامل، به قسمت DORA RTS IM (Major incidents) مراجعه شود. همچنین **کارگروه DORA (DORA Taskforce)** یک ابزار طبقه‌بندی رخداد DORA طراحی کرده است که می‌تواند مفید باشد. کارگروه ویژه DORA ابزاری برای طبقه‌بندی حوادث DORA طراحی کرده که می‌تواند مفید باشد، برای اطلاعات بیشتر به آدرس زیر مراجعه کنید: https://www.norea.nl/dora/dora-incidentclassificationtool
	10.2	Cyber Threat Classification Criteria and Information Exchange (معیارهای طبقه‌بندی تهدیدات سایبری و تبادل اطلاعات)	تهدیدات سایبری مهم باید طبقه‌بندی شوند. یک تهدید زمانی با اهمیت در نظر گرفته می‌شود که: ۱. احتمال وقوع بالایی داشته باشد، ۲. در صورت وقوع بتواند هر یک از معیارهایی را که یک رخداد را در دسته رخدادهای عمده قرار می‌دهند، برآورده سازد، و نیز بتواند کارکردهای حیاتی یا مهم نهاد مالی را تحت تأثیر قرار دهد یا قرار داده باشد، یا بتواند سایر نهادهای مالی، ارائه‌دهندگان شخص ثالث، مشتریان یا طرف‌های مالی را تحت تأثیر قرار دهد. ۳. بتواند بر عملیات حیاتی یا مهم نهاد مالی تأثیر بگذارد یا می‌توانست تأثیر بگذارد، یا بر سایر نهادهای مالی، ارائه‌دهندگان ثالث، مشتریان یا همتایان مالی اثرگذار باشد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			اطلاعات و تحلیل تهدیدات سایبری به‌منظور افزایش تاب‌آوری عملیاتی دیجیتال، با سایر نهادهای مالی به اشتراک گذاشته شود. در این حالت، می‌بایست اطمینان حاصل شود که به اشتراک‌گذاری شامل اطلاعاتی مانند شاخص‌های نفوذ، تاکتیک‌ها، تکنیک‌ها، رویه‌ها، هشدارها و ابزارهای پیکربندی باشد. اشتراک باید جوامع مورد اعتماد صورت گیرد و تابع توافقات اشتراک‌گذاری اطلاعاتی باشد به‌طوری که محرمانگی تجاری و داده‌های شخصی را حفظ کرده و قوانین رقابت را رعایت کند. این توافق‌ها باید شرایط مشارکت را به‌طور شفاف تعریف کنند، نقش احتمالی مقامات عمومی و ارائه‌دهندگان خدمات فاوا ثالث را مشخص کنند، و جنبه‌های عملیاتی از جمله استفاده از سکوهای امن فاوا را تعیین کنند. مؤسسات مالی موظف‌اند هنگام پیوستن یا خروج از چنین توافقاتی، مراجع ناظر ذی‌صلاح را مطلع سازند. برای تمامی جزئیات به برگه (Major incidents) DORA RTS IM مراجعه شود.
IM.2 Incident management **مدیریت رخداد**	11.1	Incident Management Process (فرآیند مدیریت رخداد)	**یک فرآیند مدیریت رخداد باید پیاده سازی شود تا امکان شناسایی، مدیریت و گزارش‌دهی رخدادهای مرتبط با فاوا فراهم گردد. این فرآیند شامل رویه‌های پاسخ به رخداد برای کاهش اثرات و تضمین بازگردانی به‌موقع خدمات نیز می‌باشد.** برای سناریوهای مختلف رخداد، **نقش‌ها و مسئولیت‌های مشخص** باید تعیین شوند. همچنین باید **فهرستی از اطلاعات تماس** درون‌سازمانی و ذی‌نفعان خارجی که به‌طور مستقیم در امنیت عملیات فاوا دخیل هستند، تهیه شود؛ از جمله در حوزه‌های زیر: • شناسایی و پایش تهدیدات سایبری؛ • شناسایی فعالیت‌های غیرعادی؛ • مدیریت آسیب‌پذیری‌ها. **همچنین باید شاخص‌های هشدار زودهنگام** برای رخدادهای بالقوه و **محرک‌های وقوع رخداد (Incident Triggers)** در صورت وقوع شرایط زیر تعریف شوند: • فعالیت‌های مخرب؛ • از دست رفتن داده‌ها؛ • شناسایی اثرات نامطلوب بر تراکنش‌ها و عملیات مؤسسه مالی؛ • عدم دسترس‌پذیری سامانه‌ها و شبکه‌ها؛ • مشکلات گزارش‌شده توسط کاربران نهاد مالی؛ • اعلان‌های رخداد از سوی پیمانکار، در مواردی که رخداد در سامانه‌ها یا شبکه‌های آن ارائه‌دهنده شناسایی شده و ممکن است بر نهاد مالی تأثیر بگذارد. **علل ریشه‌ای رخدادها** باید شناسایی، مستند و رسیدگی شوند. همچنین پس از وقوع **اختلالات عمده مرتبط با فاوا**، باید **بازبینی پس از رخداد** انجام شود. در این بازبینی، باید **علل رخداد، سرعت و کیفیت پاسخ به رخداد ارزیابی شود و میزان مؤثر بودن فرآیندهای ارجاع به سطوح بالاتر (تشدید) و ارتباطات مرتبط با حادثه (هماهنگی‌های انجام‌شده در زمان وقوع حادثه) مورد بررسی قرار گیرد.**

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
	11.2	Incident Tracking (ردیابی رخداد)	**باید رویه‌هایی برای شناسایی، پیگیری، ثبت، دسته‌بندی و طبقه‌بندی حوادث فاوا بر اساس اولویت، شدت و حیاتی بودن خدمات تحت تاثیر تدوین شوند.** سوابق تمامی **رخدادهای مرتبط با فاوا** و **تهدیدات سایبری بااهمیت** باید نگهداری شود. همچنین باید یک **فرآیند پایش** برای ردیابی رخدادها و تهدیدات سایبری پیاده‌سازی گردد.
	11.3	Incident Communication and Reporting (ارتباطات و گزارش‌دهی رخداد)	**ایجاد برنامه‌های ارتباطی برای اطلاع‌رسانی به ذی‌نفعان داخلی (کارکنان، مدیریت ارشد) و خارجی (مشتریان، طرف‌های مالی) در خصوص رخدادها الزامی است.** حداقل باید یک یا چند نفر در سازمان تعیین شوند که مسئول اجرای **راهبرد ارتباطی رخدادهای مرتبط با فناوری اطلاعات و ارتباطات** بوده و همچنین وظیفه **ارتباطات عمومی و رسانه‌ای** در این خصوص را بر عهده داشته باشند. به‌محض اطلاع از رخدادی که بر مشتریان تأثیر می‌گذارد، باید **اطلاع‌رسانی سریع به مشتریان آسیب‌دیده** انجام شود. این اطلاع‌رسانی باید شامل **ارائه جزئیات رخداد** و همچنین **تشریح اقدامات کاهش اثر انجام‌شده و برنامه‌ریزی‌شده** باشد. رخدادهای عمده باید در سه مرحله به مرجع ناظر گزارش شوند: ۱. **اعلان اولیه** به‌محض شناسایی رخداد (حداکثر ظرف ۴ ساعت از زمان طبقه‌بندی رخداد به‌عنوان رخداد عمده، و حداکثر تا ۲۴ ساعت از زمان شناسایی رخداد)؛ ۲. **گزارش میانی** درباره وضعیت رخداد (حداکثر ظرف ۷۲ ساعت پس از ارسال اعلان اولیه، حتی اگر وضعیت یا نحوه رسیدگی به حادثه تغییر نکرده باشد یا فعالیت‌های عادی بازیابی شده باشند)؛ ۳. **گزارش نهایی** شامل تحلیل علت ریشه‌ای و اقدامات پیگیری (حداکثر تا یک ماه پس از آخرین گزارش میانی به‌روزرسانی شده). وظایف گزارش‌دهی می‌تواند به ارائه‌دهنده خدمات شخص ثالث واگذار شود؛ با این حال در صورت چنین برون سپاری، **مؤسسه مالی همچنان مسئولیت کامل تحقق الزامات گزارش حادثه را بر عهده دارد.** همچنین باید **اطلاع‌رسانی درباره تهدیدات سایبری بااهمیت** به مرجع ناظر انجام شود. گزارش‌های رخداد و اعلان‌های مربوط به تهدیدات سایبری باید مطابق با دستورالعمل‌های محتوایی تعریف‌شده در **استانداردهای فنی و اجرایی مربوطه (RTS/ITS)** تهیه شوند.
SSD. Software and Systems Development			
SSD.1 Acquisition, development, and maintenance **تامین، توسعه و نگهداری**	12.1	Policy Framework (چارچوب سیاست‌نامه‌ها)	**سیاست‌نامه تأمین، توسعه و نگهداری سامانه‌های فناوری اطلاعات و ارتباطات باید تدوین و نگهداری شود. در سراسر چرخه حیات تأمین، توسعه و نگهداری، باید رویه‌ها و متدولوژی‌های امنیتی پیاده‌سازی گردد.** همچنین باید **الزامات کارکردی و غیرکارکردی سامانه‌های فاوا**، از جمله الزامات امنیتی، تعریف شوند. مطابق با **سازوکارهای حاکمیتی داخلی**، این الزامات باید به تأیید **کارکردهای کسب‌وکار مرتبط** و **مالکین دارایی‌ها** برسد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
	12.2	Environment Risk Mitigation Measures (اقدامات کاهش ریسک محیطی)	می‌بایست اقداماتی انجام شود که خطر تغییرات غیرعمدی یا دستکاری عمدی اطلاعات در طول توسعه، نگهداری و راه‌اندازی سیستم در محیط تولید کاهش پیدا کند. همچنین، باید از یکپارچگی و محرمانگی داده‌ها در محیط‌های غیرعملیاتی مثل محیط آزمایش یا محیط توسعه محافظت شود. در این محیط‌ها فقط نمونه داده‌های واقعی مجاز به ذخیره شدن هستند به‌طوری که نام و نشانی از صاحب واقعی داده در آنها نباشد، یا به جای مشخصات واقعی، یک کد ساختگی به آنها اختصاص داده شده باشد، یا اینکه داده‌ها کاملاً تصادفی و ساختگی باشند. داده‌های واقعی و دست نخورده که این سه ویژگی را ندارند، فقط برای آزمایش‌های خاص، آن هم برای مدت زمان کوتاهی مجاز به ذخیره سازی هستند. در این موارد حتماً باید تأیید واحد مربوطه دریافت شود. علاوه بر این، مؤسسات مالی بزرگ موظف هستند این نوع آزمایش‌ها را به واحد مدیریت ریسک فاوا گزارش کنند.
	12.3	Systems Testing Procedures (رویه‌های آزمون سیستم‌ها)	**رویه‌هایی برای آزمون و تأیید تمامی سامانه‌های فاوا قبل از بهره‌برداری و پس از نگهداری باید تدوین و اجرا شود. سطح آزمون باید بر اساس اهمیت کارکردهای کسب‌وکار و دارایی‌های فاوا تعیین گردد.** همچنین رویه‌های آزمون باید به‌گونه‌ای طراحی و پیاده‌سازی شوند که اطمینان حاصل شود سامانه‌های جدید فاوا به درستی قادر به انجام وظایف مورد نظر هستند، از جمله ارزیابی کیفیت نرم‌افزارهای توسعه‌یافته داخلی. آزمون امنیتی بسته‌های نرم‌افزاری باید حداکثر تا مرحله یکپارچه‌سازی (Integration Phase) انجام شود.
	12.4	Source Code Reviews (بازبینی‌های مربوط به کد منبع)	**بازبینی کد منبع باید به منظور تأمین، توسعه و نگهداری سامانه‌های فناوری اطلاعات و ارتباطات انجام شود و شامل آزمون‌های ایستا (Static) و پویا (Dynamic) باشد. همچنین آزمون‌های امنیتی برای سامانه‌های لبه اینترنت نیز الزامی است.** آسیب‌پذیری‌ها و ناهنجاری‌های موجود در کد منبع باید شناسایی و رفع شوند و برای کاهش آن‌ها برنامه‌های مشخصی تدوین گردد. اقدامات کاهش ریسک باید به‌طور مستمر پایش شوند. کنترل‌هایی باید پیاده‌سازی شود تا **یکپارچگی کد منبع**، چه در داخل سازمان توسعه یافته باشد، و چه توسط پیمانکاران، حفظ گردد. همچنین باید کد منبع و نرم‌افزارهای دارای لایسنس اختصاصی ارائه شده توسط پیمانکاران یا پروژه‌های متن‌باز از نظر آسیب‌پذیری‌ها تحلیل و آزمون شوند.
SSD.2 Project Management **مدیریت پروژه**	13.1	ICT Project Management Practices (رویه‌های مدیریت پروژه‌های فناوری اطلاعات و ارتباطات)	مدیریت مؤثر پروژه‌های فاوا مرتبط با تأمین، نگهداری و در صورت لزوم توسعه سامانه‌های فاوا باید از طریق یک **سیاستنامه مدیریت پروژه** تضمین شود. طرح پروژه فاوا باید شامل موارد زیر باشد: • اهداف روشن پروژه؛ • ساختار حاکمیت پروژه؛ • نقش‌ها و مسئولیت‌های تعریف‌شده؛ • بازه زمانی تعریف شده و مراحل اجرایی مشخص؛ • نقاط عطف کلیدی پروژه؛ • الزامات مدیریت تغییر.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			الزامات مربوط به اعضای تیم پروژه باید مشخص شود، به‌گونه‌ای که شامل کارکنانی از بخشی که مالک کسب‌وکار پروژه هستند باشد. اعضای تیم باید از دانش کافی برای تضمین اجرای امن و موفق پروژه برخوردار باشند. همچنین باید الزامات گزارش‌دهی تعیین گردد، از جمله گزارش‌های دوره‌ای درباره راه‌اندازی و پیشـــرفت پروژه‌هایی که بر کارکردهای حیاتی یا مهم تأثیر دارند، همراه با ریسک‌های مرتبط با آن‌ها. با در نظر گرفتن اهمیت و اندازه پروژه‌های فاوا و ارزیابی ریسک پروژه، گزارش‌دهی باید به صورت دوره‌ای و در صورت لزوم به صورت رویدادمحور انجام شود.
	13.2	Project Risk Management (مدیریت ریسک پروژه)	ارزیابی ریسک در پروژه‌های فاوا باید انجام شود. همچنین این ارزیابی باید بر روی تمامی الزامات مدیریت پروژه، از جمله الزامات امنیتی، صورت پذیرد. یک فرآیند تأیید برای استقرار در محیط عملیاتی باید ایجاد شود.
TPRM. Third-party Risk Management			
TPRM.1 Third-party due diligence and selection **بررسی‌های پیش‌ازقرارداد و انتخاب ارائه‌دهندگان شخص ثالث**	14.1	Suitability Criteria (معیارهای سنجش تناسب)	اطمینان حاصل شود که پیمانکار دارای **اعتبار تجاری مناسب**، **توانمندی‌ها و تخصص کافی**، **و منابع مالی، انسانی و فنی لازم** است و همچنین از **استانداردهای مناسب امنیت اطلاعات** برخوردار می‌باشد. علاوه بر این، ارائه‌دهنده باید دارای **ساختار سازمانی مناسب** (شامل مدیریت ریسک و کنترل‌های داخلی) بوده و در صورت لزوم، **در یک نهاد نظارتی ثبت رسمی گردیده و مجوزهای حقوقی مورد نیاز** را برای ارائه خدمات فاوا که از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند، به‌صورت قابل اتکا و حرفه‌ای در اختیار داشته باشد.
	14.2	Selection Criteria (معیارهای انتخاب)	در فرآیند انتخاب و ارزیابی ارائه‌دهنده خدمات، موارد زیر باید مورد توجه قرار گیرد: حسابرسی‌های انجام‌شده توسط مؤسسه مالی یا به نمایندگی از آن، گواهی‌نامه‌های اشخاص ثالث، گزارش‌های حسابرسی مستقل، گزارش‌های واحد حسابرسی داخلی، و اطلاعات عمومی در دسترس قرار گرفته. همچنین باید انطباق با اصول **اخلاقی**، **اجتماعی**، **انسانی و زیست‌محیطی (پایداری)**، از جمله شرایط کاری مناسب و ممنوعیت کار کودکان مورد تأیید قرار گیرد. باید بررسی شود که آیا ارائه‌دهنده خدمات در **کشور ثالث** فعالیت می‌کند یا خیر و ارزیابی شود که آیا این موضوع موجب افزایش ریسک‌های عملیاتی، اعتباری یا تحریمی می‌گردد یا خیر. رضایت ارائه‌دهنده خدمات برای انجام مؤثر حسابرسی‌ها باید اخذ شود؛ این حسابرسی‌ها می‌توانند به‌صورت حضوری یا توسط طرف‌های تعیین‌شده، شامل حسابرسان نهاد مالی، حسابرسان خارجی (اشخاص ثالث) و همچنین مقامات ناظر ذی‌صلاح انجام شوند. در نهایت باید بررسی شود که آیا ارائه‌دهنده خدمات قصد دارد از **پیمانکاران فرعی فاوا** برای بخش‌های قابل‌توجهی از خدمات خود استفاده کند یا خیر.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
TPRM.2 Third-party (standard) contract management **مدیریت قراردادهای (استاندارد) اشخاص ثالث**	15.1	Termination Rights and Conditions (حقوق و شرایط فسخ)	حقوق صریح برای خاتمه قرارداد باید تعریف شود، از جمله در مواردی مانند نقض‌های عمده قوانین، مقررات یا مفاد قرارداد، تغییرات اساسی در ریسک‌های مرتبط با شخص ثالث، ضعف‌های اثبات‌شده در فناوری اطلاعات و ارتباطات و محدودیت‌های ناشی از نظارت‌های رگولاتوری. همچنین باید تمهیداتی پیش‌بینی شود تا در صورت خاتمه قرارداد، ورشکستگی، رویه ساماندهی و انحلال کنترل شده یا توقف فعالیت پیمانکار، امکان **دسترسی، بازیابی و بازگردانی داده‌ها در قالبی قابل دسترس و استاندارد** تضمین گردد.
	15.2	Service Level Management (مدیریت سطح خدمات)	مفاد شرح خدمات باید به‌طور روشن و قابل اندازه‌گیری تعریف شود و استانداردهای عملکرد و کیفیت مورد انتظار را مشخص کند. ارائه‌دهنده خدمات موظف است توضیح کاملی از تمام کارکردها و خدمات فناوری اطلاعات خود، از جمله مواردی که به پیمانکار فرعی واگذار می شود، ارائه دهد. همچنین سازوکاری برقرار شود که حفاظت از داده‌ها در سطح مناسب و مطابق با قوانین نظارتی تضمین گردد.
	15.3	Service Locations and Data Processing (مکان‌های ارائه خدمت و پردازش داده‌ها)	محل‌های ارائه خدمات و سایت‌های پردازش داده باید به‌طور مشخص تعیین شوند. همچنین باید الزام شود که هرگونه تغییر برنامه‌ریزی شده در این محل‌ها به‌موقع اطلاع‌رسانی گردد.
	15.4	Cooperation in Incident Response (همکاری در پاسخ به رخدادها)	ارائه‌دهنده خدمات فناوری اطلاعات و ارتباطات شخص ثالث باید ملزم شود که در صورت وقوع رخدادی مرتبط با خدمات ارائه‌شده، به‌طور کامل با مرجع ناظر همکاری کرده و کمک‌های لازم را ارائه دهد.
	15.5	Participation in Security Awareness Programs (مشارکت در برنامه‌های آگاهی‌رسانی امنیتی)	شرایط مشارکت ارائه‌دهنده خدمات در برنامه‌ها و آگاه‌سازی در خصوص موضوعات امنیتی و تاب‌آوری باید مشخص شود.
TPRM.3 Third-party (critical) contract management **مدیریت قراردادهای (حیاتی) اشخاص ثالث**	16.1	(Critical) Service Level Management مدیریت سطح خدمات (حیاتی)	اطمینان حاصل شود که قرارداد با پیمانکاران فاوا که خدمات حیاتی یا مهم ارائه می‌دهند، شامل **توصیف‌های جامع سطح خدمات** باشد؛ از جمله به‌روزرسانی‌ها و گزارش‌دهی دقیق (کمی و کیفی). انطباق ارائه‌دهنده خدمات با استانداردهای عملکرد و کیفیت باید از طریق بررسی گزارش‌های مربوط به فعالیت‌ها و خدمات، گزارش رخدادها، اقدامات امنیتی و تداوم کسب‌وکار و نتایج آزمون‌ها ارزیابی شود. ارزیابی عملکرد باید با استفاده از **شاخص‌های کلیدی عملکرد(KPI)**، **شاخص‌های کلیدی کنترل(KCI)**، حسابرسی‌ها، خوداظهاری‌ها و بررسی‌های مستقل سنجیده شود. اطلاعات مرتبط با فعالیت‌ها و خدمات باید از ارائه‌دهنده دریافت شده و **اطلاع‌رسانی به‌موقع درباره رخدادها و پاسخ به آن‌ها** تضمین گردد. همچنین باید بررسی‌های مستقل و حسابرسی‌های انطباق با الزامات قانونی، مقرراتی و سیاست‌نامه‌ها انجام شود. برای اطلاع رسانی هرگونه تغییر بنیادی که ممکن است بر نهاد مالی یا سطوح خدمات توافق‌شده تأثیر بگذارد، می‌بایست بازه‌های زمانی مشخصی تعیین گردد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			برای جزئیات کامل، به بخش‌های **DORA RTS TPPM** و **DORA RTS SCM** مراجعه شود.
	16.2	Contractual Clauses (بندهای قراردادی)	حقوق پایش مداوم عملکرد، از جمله حق دسترسی، بازرسی و حسابرسی بدون هیچ محدودیتی، می‌بایست برای مؤسسه مالی در نظر گرفته شود؛ که شامل سطوح جایگزین تضمین، همکاری با بازرسی‌های نهاد ناظر، و افشای کامل دامنه، رویه‌ها و تعداد دفعات حسابرسی می‌شود. همچنین باید یک **دوره انتقال اجباری** در زمان خاتمه قرارداد پیش‌بینی شـــود تا ارائه‌دهنده خدمات بتواند در طول مهاجرت، ارائه خدمات را ادامه دهد و به مؤسسه مالی فرصت دهد تا بر اساس پیچیدگی خدمات، به ارائه‌دهنده دیگر یا راهکارهای داخلی منتقل شود. اجرای و آزمون **برنامه‌های تداوم کسب‌وکار** و استقرار یک **سیستم مدیریت امنیت** توسط ارائه‌دهنده خدمات الزامی است. در زمان مذاکره هنگام عقد قراردادها، از **بندهای استاندارد** که توسط مقامات عمومی برای خدمات مشخص تدوین شده‌اند، استفاده شود. همچنین باید مشارکت ارائه‌دهنده خدمات در **برنامه آزمون‌های پیشرفته (TLPT)** مؤسسه مالی، در صورت لزوم، الزامی گردد. در مواردی که مشـــارکت ارائه‌دهنده فاوا در TLPT ممکن اســـت بر خدمات یا محرمانگی داده‌های مشـــتریان خارج از دامنه DORA تأثیر منفی بگذارد، می‌توان به‌صورت مکتوب توافق کرد که **TLPT تجمیعی**[۶۹] (به صورت گروهی و مشترک با سایر مؤسسات) انجام شود. برای جزئیات کامل، به بخش‌های **DORA RTS TPPM** و **DORA RTS SCM** مراجعه شود.
	16.3	Third-party Critical Subcontracting Management (مدیریت پیمانکاران حیاتی طرف ثالث)	در قراردادهای مربوط به پیمانکاران فاوا، باید خدمات فاوای حیاتی و مهم به‌طور مشـــخص تفکیک شـــده و شـــرایط مربوط به **پیمانکاران** تعیین گردد. پایش م ستمر خدمات برون سپاری شده که از کارکردهای حیاتی پ شتیبانی می‌کنند الزامی ا ست تا اطمینان حا صل شود که الزامات قراردادی رعایت می‌شوند. همچنین باید مسئولیت‌های مربوط به **پایش و گزارش‌دهی پیمانکار به مؤسسه مالی**، از جمله ارزیابی ریسک‌های مرتبط با **محل استقرار پیمانکاران فرعی و مالکیت داده‌ها** به‌صورت دقیق مشخص شود. برنامه‌های **پاسخ به رخداد** و **تداوم کسب‌وکار** برای پیمانکاران فرعی باید الزامی باشد و همچنین رعایت **سطوح خدمات تعیین‌شده و استانداردهای امنیتی** تضمین گردد. مؤسسه مالی باید حق خاتمه قرارداد را در موارد **برون‌سپاری غیرمجاز** یا **عدم تحقق سطوح خدمات توافق‌شده** حفظ کند. تغییرات مرتبط با توافقات قراردادی باید در اسرع وقت اعمال شده و **برنامه زمانی اجرای آن‌ها مستندسازی شود.** برای جزئیات کامل، به بخش‌های **DORA RTS TPPM** و **DORA RTS SCM** مراجعه شود.
TPRM.4 Third-party risk management	17.1	Third-party risk management (مدیریت ریسک اشخاص ثالث)	ریسک‌های مرتبط با اشخاص ثالث باید متناسب با ماهیت وابستگی، ریسک‌های مرتبط با خدمات، و تأثیر آن‌ها بر تداوم و دسترس‌پذیری مؤسسه مالی در صورت وقوع اختلال مدیریت شوند. در حال حاضر ریسک‌های ناشی از پیمانکاران IT سازمان، در مقوله‌های زیر مدیریت می‌شوند:

[۶۹] Pooled TLPT

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
مدیریت ریسک اشخاص ثالث			• ریسک‌های ناشی از ماهیت شخص ثالث و میزان وابستگی پیمانکاران به سازمان • ریسک‌های مرتبط با خدمات ارائه‌شده از سوی پیمانکاران • ریسک‌های ناشی از میزان تأثیر اختلال احتمالی بر تداوم کسب‌وکاری • ریسک‌های مرتبط با موقعیت مکانی پیمانکاران • ریسک‌های مرتبط با محل پردازش و ذخیره‌سازی داده‌ها • ماهیت داده‌های به اشتراک گذاشته شده با پیمانکاران همچنین باید **آزمون پاسخ و بازیابی خدمات پشتیبان عملیات حیاتی که توسط اشخاص ثالث ارائه می‌شوند** انجام شود.
	17.2	Pre-Contract Risk Assessment (ارزیابی ریسک پیش از قرارداد)	ارزیابی ریسک می‌بایست پیش از انعقاد قرارداد با پیمانکاران انجام شود. این ارزیابی باید مشخص کند که: • آیا پیمانکار عملیات حیاتی یا مهم را پوشش می‌دهد؟ • آیا پیمانکار به راحتی قابل جایگزینی است؟ • آیا ریسک‌های پیمانکاران فرعی پوشش داده شده‌اند؟ • آیا ریسک‌های برون‌سپاری خدمات به یک کشور ثالث پوشش داده شده‌اند؟ • آیا ریسک‌های ورشکستگی در سمت ارائه‌دهنده خدمات پوشش داده شده‌اند؟ • آیا شرایط نظارتی برای انعقاد قرارداد رعایت شده است؟ • آیا تمامی ریسک‌های قراردادی شناسایی و ارزیابی شده‌اند؟ (به عنوان مثال، برای پوشش ریسک‌های فناوری اطلاعات) • آیا ارائه‌دهنده خدمات مناسب است اما در عین حال ریسک تعارض منافع وجود دارد؟ همچنین باید منابع ارائه‌دهنده خدمات برای اطمینان از انطباق سازمان با تمامی الزامات قانونی و مقرراتی مورد ارزیابی شود.
	17.3	Register of Information (ثبت اطلاعات)	اطمینان حاصل شود که در سازمان، اطلاعات قراردادها با پیمانکاران به‌صورت جامع و با تمایز قراردادهای حیاتی – غیر حیاتی و حاوی فیلدها و بخش‌های اجباری که توسط مقررات داخلی و بالادستی تعیین شده، ثبت، نگهداری و بروزرسانی می‌شود. این ثبت باید با تمامی **فیلدهای الزامی تعریف‌شده در ITS مربوط به ثبت اطلاعات** هم‌راستا باشد.
	17.4	Contractual Requisites (الزامات قراردادی)	قرارداد صرفاً باید با ارائه‌دهندگانی منعقد شود که دارای استانداردهای مناسب امنیت اطلاعات (مانند ISO 27001، SOC، PCI-DSS و غیره) بوده و همچنین متناسب با سطح اهمیت خدمات ارائه‌شده باشند. همچنین باید تناوب حسابرسی ارائه‌دهندگان خدمات تعیین شود و اطمینان حاصل گردد که حسابرسان دارای **مهارت‌ها و دانش لازم برای ارزیابی خدمات پیچیده** هستند.
	17.5	Exit strategies (راهبردهای خروج)	راهبردها و برنامه‌های خروج باید با در نظر گرفتن ریسک‌های مرتبط با ارائه‌دهندگان خدمات شخص ثالث، از جمله احتمال شکست ارائه‌دهنده، کاهش کیفیت خدمات، اختلال در کسب‌وکار و خاتمه توافقات قراردادی، تدوین و به‌صورت دوره‌ای آزمون شوند. برنامه خروج باید واقع‌بینانه، قابل اجرا و مبتنی بر سناریوهای محتمل و فرضیات معقول باشد و دارای **برنامه زمان‌بندی اجرای مشخص** بوده که با شرایط خروج و خاتمه مندرج در قراردادهای مربوط هم‌راستا باشد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			همچنین باید اطمینان حاصل شود که فرآیند خروج و انتقال بار کاری به ارائه‌دهنده دیگر به‌صورت **سلسله‌وار و بدون ایجاد اختلال در کسب‌وکار، نقض انطباق یا کاهش کیفیت خدمات** انجام شود. کارگروه DORA یک **الگوی برنامه خروج** طراحی کرده است که می‌تواند مورد استفاده قرار گیرد: https://www.norea.nl/dora/dora-template-exit-plan
	17.6	Annual Reporting of New Arrangements (گزارش‌دهی سالانه درباره ترتیبات جدید)	قراردادهای جدید مربوط به ارائه‌دهندگان خدمات باید به مرجع ناظر گزارش شوند، به‌ویژه مواردی که از عملیات حیاتی یا مهم پشتیبانی می‌کنند. این گزارش‌دهی باید به‌صورت سالانه انجام شود و در مورد خدمات حیاتی، اطلاع‌رسانی باید به‌صورت فوری صورت گیرد.
TPRM.5 Subcontracting management **مدیریت پیمانکاران فرعی**	18.1	Third-Party Subcontractor Due Diligence (بررسی‌های پیش از قرارداد پیمانکاران فرعی اشخاص ثالث)	در خصوص پیمانکاران فرعی که از عملیات حیاتی یا مهم پشتیبانی می‌کنند: • باید رویه‌های بررسی صلاحیت (Due Diligence) برای ارزیابی شیوه‌های برون‌سپاری ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات شخص ثالث پیاده‌سازی شود. • تمامی پیمانکاران فرعی ارائه‌دهنده خدمات فناوری اطلاعات و ارتباطات (فاوا) که از کارکردهای حیاتی یا بخش‌های قابل‌توجه آن پشتیبانی می‌کنند باید شناسایی شده و به مؤسسه مالی اطلاع داده شوند. • باید اطمینان حاصل شود که توافقات قراردادی با پیمانکاران فرعی امکان رعایت تعهدات مؤسسه مالی را فراهم می‌سازد. • در قرارداد با ارائه‌دهنده فاوا باید تضمین شود که پیمانکار فرعی همان سطح دسترسی و بازرسی قراردادی را که به ارائه‌دهنده اصلی اعطا شده است، فراهم می‌کند. • ساختار سازمانی، منابع و استانداردهای امنیت اطلاعات ارائه‌دهنده ثالث، از جمله سازوکارهای پاسخ به رخداد و مدیریت ریسک مرتبط با پیمانکار فرعی باید ارزیابی شود. • ساختار سازمانی، منابع و استانداردهای امنیت اطلاعات خود مؤسسه مالی نیز، از جمله سازوکارهای پاسخ به رخداد و مدیریت ریسک در ارتباط با ارائه‌دهنده فاوا و پیمانکاران فرعی باید ارزیابی شود. • اثر احتمالی شکست (ورشکستگی) پیمانکار فرعی بر تاب‌آوری عملیاتی دیجیتال و سلامت مالی باید بررسی شود. • محل استقرار پیمانکاران فرعی بالقوه باید ارزیابی گردد. • ریسک تمرکز فاوا در سطح واحد باید مطابق الزامات مربوطه بررسی شود. • هرگونه مانع در خصوص حقوق حسابرسی و دسترسی برای مراجع ذی‌صلاح و مؤسسه مالی باید برطرف گردد. برای جزئیات کامل، به بخش DORA RTS SCM مراجعه شود.
	18.2	Subcontracting Risk Management (مدیریت ریسک پیمانکاران فرعی)	در خصوص پیمانکاران فرعی که از عملیات حیاتی یا مهم پشتیبانی می‌کنند: • باید یک فرآیند مدیریت ریسک برای نظارت مؤثر بر فعالیت‌های برون‌سپاری به پیمانکاران فرعی ایجاد شود. • کل زنجیره برون سپاری فاوا باید پایش شود، شرایط آن مستند سازی گردد و انطباق با تعهدات قراردادی و همچنین الزام نگهداری و به‌روزرسانی ثبت اطلاعات (Register of Information) تضمین شود.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			• اسناد قراردادی باید بررسی شوند تا انطباق با شرایط تعیین‌شده در سراسر زنجیره برون‌سپاری راستی‌آزمایی گردد. • اطلاع‌رسانی قبلی در خصوص تغییرات مهم در ترتیبات برون‌سپاری الزامی است تا امکان ارزیابی و کاهش ریسک فراهم شود. • در قراردادهای پیمانکاران که برای انجام خدمات مهم و حیاتی فناوری اطلاعات منعقد گردیده، بندی با مضمون تأیید یا درخواست تغییر فعالیت‌های برون‌سپاری (برون‌سپاری بخشی از قرارداد به پیمانکار فرعی) درج گردیده است. • اقدامات پیشگیرانه برای رسیدگی به ریسک‌های شناسایی‌شده و تقویت نظارت بر برون‌سپاری فرعی باید اجرا گردد. برای جزئیات کامل، به بخش **DORA RTS SCM** مراجعه شود.
	18.3	Subcontracting Monitoring (پایش پیمانکاران فرعی)	در خصوص پیمانکاری‌های فرعی که از یک وظیفه حیاتی یا مهم پشتیبانی می‌کنند: • یک فرآیند بهبود مستمر و پایش ایجاد شود تا شیوه‌های پیمانکاری فرعی بهبود یافته و ریسک‌های مرتبط کاهش یابد. • شرایط برون‌سپاری به پیمانکاران فرعی باید به‌طور منظم بر اساس تغییرات محیط کسب‌وکار و ارزیابی‌های ریسک بازبینی و به‌روزرسانی گردد. • ارزیابی‌های دوره‌ای از معیارهای پیمانکار فرعی انجام دهید، شامل تهدیدات فاوا، ریسک‌های تمرکز و عوامل ژئوپلیتیک. • اثربخشی کنترل‌های پیمانکاری فرعی از طریق حقوق قراردادی دسترسی و بازرسی پایش و ارزیابی شود. • هرگونه نقص یا ریسک‌های نوظهور به‌طور پیشگیرانه شناسایی و رفع شود تا حاکمیت و نظارت بر پیمانکاری فرعی تقویت گردد. برای تمامی جزئیات به زبانه DORA RTS SCM مراجعه کنید.
RT. Resilience testing			
RT.1 Digital operation resilience testing **آزمون تاب‌آوری عملیاتی دیجیتال**	19.1	Resilience Testing Program (برنامه آزمون تاب‌آوری)	یک برنامه آزمون تاب‌آوری عملیاتی دیجیتال مبتنی بر ریسک باید ایجاد شود که شامل شناسایی، طبقه‌بندی و رفع کامل نواقص آزمون بر اساس چشم‌انداز ریسک و میزان اهمیت دارایی‌ها و خدمات باشد. برای اجرای آزمون‌ها باید از طرف‌های مستقل داخلی یا خارجی استفاده شود و تفکیک وظایف به‌طور شفاف رعایت گردد. حداقل سالی یک‌بار باید تمامی سامانه‌ها و برنامه‌های کاربردی پشتیبان کارکردهای حیاتی یا مهم مورد آزمون قرار گیرند (برای آزمون‌های تاب‌آوری عملیاتی دیجیتال به کنترل‌های ۱۹ تا ۲۰ مراجعه شود).
	19.2	Diverse Testing Modalities (روش‌های متنوع آزمون)	باید مجموعه‌ای متنوع از آزمون‌ها به کار گرفته شود، از جمله: ارزیابی آسیب‌پذیری، تحلیل منابع متن‌باز، ارزیابی امنیت شبکه، تحلیل شکاف، بررسی‌های امنیت فیزیکی، پرسش‌نامه‌ها، استفاده از ابزارهای اسکن نرم‌افزاری، بازبینی کد منبع (در صورت کاربرد)، آزمون‌های مبتنی بر سناریو، آزمون سازگاری، آزمون کارایی، آزمون سرتاسری و در صورت لزوم آزمون نفوذ.
	19.3	Periodic TLPT Testing (آزمون دوره‌ای TLPT)	آزمون نفوذ تهدید محور (Threat-Led Penetration Testing - TLPT) باید هر سه سال یک‌بار و متناسب با پروفایل ریسک مؤسسه مالی انجام شود. اطمینان حاصل شود که TLPT تمامی کارکردهای حیاتی یا مهم را پوشش داده و بر روی سامانه‌های عملیاتی اجرا می‌شود. گزارشی شامل یافته‌های TLPT، برنامه‌های اصلاحی و مستندات نشان‌دهنده انطباق با این کنترل باید به مرجع ناظر ارائه گردد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			TLPT باید مطابق با چارچوب TLPT در DORA (مبتنی بر چارچوب- EU TIBER) و همان‌گونه که در RTS مربوطه تعریف شده است، انجام شود. این کنترل تنها برای مؤسسات مالی واجد شرایط TLPT قابل اعمال است. برای اطلاعات بیشتر درباره دامنه شمول، به RTS مربوط به TLPT مراجعه شود.
RT.3 Threat-led penetration testing **آزمون نفوذ تهدید محور**	20.1	Outsourced System testing (آزمون سیستم برون‌سپاری‌شده)	باید آزمون نفوذ تهدید محور (TLPT) به سامانه‌ها، فرآیندها و فناوری‌های حیاتی برون‌سپاری‌شده نیز تعمیم داده شود. مؤسسه مالی همچنان مسئولیت حصول اطمینان از انطباق با کنترل ها را بر عهده خواهد داشت. همچنین، باید با ارائه‌دهندگان خدمات همکاری شود تا کنترل‌های مدیریت ریسک استقرار یافته و ریسک‌های وارد بر داده‌ها، دارایی‌ها و کارکردهای حیاتی کاهش داده شود. این کنترل تنها برای مؤسسات مالی واجد شرایط TLPT قابل اعمال است. برای اطلاعات بیشتر درباره دامنه شمول، به RTS مربوط به TLPT مراجعه شود.
	20.2	Selection of TLPT Testers (انتخاب آزمون‌دهندگان TLPT)	برای اجرای آزمون نفوذ تهدید محور (TLPT) باید از آزمونگران داخلی یا خارجی استفاده شود؛ به‌گونه‌ای که در هر **چرخه سوم**[۷۰] **TLPT**، آزمونگران خارجی به‌کار گرفته شوند. آزمونگران داخلی باید دارای **تأییدیه نهاد ناظر** بوده، از منابع کافی برخوردار باشند و استفاده کنند. انتخاب آزمونگران TLPT باید بر اساس معیارهای زیر انجام شود: • اعتبار حرفه‌ای؛ • تخصص در اطلاعات تهدید، آزمون نفوذ و روش‌های تیم قرمز؛ • داشتن گواهی‌نامه‌های مرتبط؛ • برخورداری از تضمین مستقل؛ • و پوشش بیمه مسئولیت. همچنین قراردادهای منعقدشده با آزمونگران خارجی باید شامل الزامات مدیریت صحیح نتایج TLPT باشد، به‌گونه‌ای که هرگونه پردازش داده‌ها (شامل تولید، ذخیره‌سازی، تجمیع، پیش‌نویس، گزارش‌دهی، ارتباط یا امحای داده‌ها) هیچ‌گونه ریسک اضافی ایجاد نکند. باید استقلال تیم‌ها تضمین شود، به‌گونه‌ای که آزمونگران داخلی و خارجی به صورت مجزا فعالیت کنند، و همچنین وجود گواهی‌نامه‌ها، تضمین مستقل و بیمه مسئولیت بررسی و تأیید گردد. این کنترل فقط برای مؤسسات مالی واجد شرایط TLPT قابل اعمال است. برای جزئیات بیشتر به RTS مربوط به TLPT مراجعه شود.

[۷۰] به یک دوره قراردادی استاندارد (Contractual Period) اشاره دارد. مطابق الزامات حاکمیتی (Governance Requirements) و برای حفظ بی‌طرفی و اثربخشی ارزیابی، پس از حداکثر ۲ دوره تناوب (Two Consecutive Cycles)، در دوره (چرخه) سوم (Third Rotation Cycle) می‌بایست ارائه‌دهنده خدمات ارزیابی خارجی (External Assessment Provider) تغییر یابد. این چرخه‌مندسازی (Cyclical Rotation) یک سازوکار کنترلی برای تضمین استقلال و جلوگیری از تثبیت ارتباط طولانی مدت با یک پیمانکار واحد است.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
SM. Security Management			
SM.1 Architectural and network security **امنیت معماری و شبکه**	21.1	Network Design and Segmentation (طراحی و تفکیک شبکه)	زیرساخت شبکه باید به‌گونه‌ای طراحی شود که امکان **جداسازی یا قطع فوری بخش‌های آن** فراهم باشد تا از گسترش اختلال جلوگیری کند. باید تمهیداتی برای **ایزوله‌سازی موقت زیرشبکه‌ها و اجزای شبکه/دستگاه‌ها** در نظر گرفته شود. ظرفیت‌های **افزونگی** باید به منابع، قابلیت‌ها و عملکردهای کافی مجهز باشند (مانند طراحی شبکه‌های پشتیبان). سامانه‌ها و شبکه‌ها باید بر اساس **اهمیت عملیات، طبقه‌بندی و سطح ریسک کلی** از یکدیگر تفکیک شوند. همچنین باید یک **شبکه جداگانه برای مدیریت دارایی‌ها** نگهداری شود سازمان باید تصویری شفاف و مستند از معماری شبکه و جریان‌های تبادل داده ارائه کند؛ به‌گونه‌ای که مسیر حرکت اطلاعات و ارتباط میان سامانه‌ها در سطح شبکه (لایه ۳) و سطح کاربردی (لایه ۷) به‌سادگی قابل مشاهده و تحلیل باشد. بازبینی عملکرد و طراحی معماری شبکه باید به‌صورت **سالانه** انجام شود.
	21.2	Network Security (امنیت شبکه)	کنترل‌های لازم برای جلوگیری و کشف اتصالات غیرمجاز شبکه پیاده‌سازی شود. پیکربندی امن پایه برای همه اجزای شبکه، و بر اساس دستورالعمل‌های تولیدکننده، استانداردهای صنعتی و بهترین روش‌ها، برقرار و حفظ گردد. باید از **محرمانگی، یکپارچگی و دسترس‌پذیری** داده‌ها در حین انتقال در شبکه اطمینان حاصل شود. همچنین باید از **نشت داده جلوگیری و آن را شناسایی** کرده و انتقال داده با طرف‌های خارجی به‌صورت امن انجام شود. اقدامات لازم برای ایمن‌سازی ترافیک شبکه بین شبکه‌های داخلی و اینترنت/اتصالات خارجی باید اجرا شود. برای تمامی پروتکل‌های ارتباطی در شبکه‌های سازمانی، عمومی، داخلی، شخص ثالث و بی‌سیم، باید **رمزنگاری** بر اساس طبقه‌بندی داده و ارزیابی ریسک اعمال گردد. نقش‌ها و مسئولیت‌ها در خصوص تعریف، پیاده‌سازی، تأیید، تغییر و بازبینی قوانین فایروال و فیلترهای ارتباطی باید به‌صورت دوره‌ای بررسی شوند. سازمان‌ها باید بازبینی قوانین فایروال و فیلترهای ارتباطی را به‌صورت منظم و متناسب با طبقه‌بندی و سطح ریسک سیستم‌های فاوا انجام دهند. برای سامانه‌هایی که از عملیاتی حیاتی یا مهم پشتیبانی می‌کنند، باید حداقل هر **شش ماه یک‌بار** کفایت قوانین فایروال و فیلترهای ارتباطی بررسی و تأیید شود.
	21.3	Session Management (مدیریت نشست)	اقدامات مقتضی می‌بایست صورت پذیرد تا **نشست‌های سیستمی و دسترسی‌های راه‌دور** پس از یک بازه از پیش تعیین‌شده عدم فعالیت، محدود، قفل و در نهایت خاتمه یابند.
SM.2 Security monitoring & log management	22.1	Security Monitoring (SIEM) (پایش امنیتی)	باید سازوکارهایی برای شناسایی فعالیت‌های غیرعادی، از جمله کاهش کارایی شبکه، رخدادها (گزارش‌شده توسط ارائه‌دهندگان خدمات شخص ثالث در خدمات ارائه‌شده)، و شکست به‌دلیل اتکا به نقطه واحد (Single Point Of Failure) بالقوه و با اهمیت، ایجاد شود. این سازوکارها باید امکان **کنترل چندلایه** را فراهم کرده، آستانه‌های هشدار را تعریف کنند و پایش بر رویدادها و معیارهای مشخصی را انجام دهند که به‌صورت خودکار باعث **فعال‌سازی پاسخ به رخداد** شوند.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
پایش امنیت و مدیریت لاگ			ابزارهایی باید شناسایی و پیاده‌سازی شوند که بتوانند **هشدارهای مربوط به فعالیت‌ها و رفتارهای غیرعادی** تولید کنند، حداقل برای دارایی‌های فاوا و دارایی‌های اطلاعاتی که از عملیات حیاتی یا مهم پشتیبانی می‌کنند. منابع کافی باید به فعالیت‌های **شناسایی و پایش** به‌ویژه در حوزه مقابله با حملات سایبری اختصاص یابد.
	22.2	Event Identification for Logging (شناسایی رویداد برای ثبت لاگ)	رویه‌ها، پروتکل‌ها و ابزارهایی برای ثبت لاگ (Logging) مربوط به ناهنجاری‌ها باید ایجاد، مستند و پیاده‌سازی شوند. رویدادهایی که باید ثبت شوند باید شناسایی گردند و شامل موارد زیر باشند: • دسترسی منطقی (Logical Access) • دسترسی فیزیکی (Physical Access) • مدیریت هویت (Identity Management) • مدیریت ظرفیت (Capacity Management) • مدیریت تغییر (Change Management) • عملیات فناوری اطلاعات (ICT Operation) شامل فعالیت‌های سیستمی • فعالیت‌های ترافیک شبکه، شامل عملکرد شبکه سطح جزییات وقایع (لاگ‌ها) همسو با هدفی که وقایع برای آن ایجاد شده‌اند و به منظور امکان تشخیص مؤثر فعالیت‌های غیرعادی، تعیین شود. دوره‌های نگهداری لاگ‌ها باید مشخص شوند و در تعیین آن‌ها باید اهداف کسب‌وکار و امنیت، هدف از ثبت لاگ‌ها و ارزیابی ریسک‌ها در نظر گرفته شود. به منظور حصول اطمینان از صحت و جامعیت گزارش‌های کسب‌وکاریِ ارسال‌شده به مقام ناظر، عملیات واحدهای ذیربط در حوزه گزارش‌گری و فرآوری داده، مجهز به سامانه هوشمند ارسال گزارشات (مالی، تجاری و ...) به مراجع بالادستی باید دارای ویژگی‌های ذیل باشد: • اطمینان حاصل می‌کند تمام فیلدهای اطلاعاتی الزامی به‌صورت صحیح پر شده و فیلدهای اطلاعاتی الزامی خالی وجود نداشته باشد. • قابلیت ثبت و بررسی وقایع (لاگ) را دارا است و اگر لاگ فایل‌هایی که در گزارش مورد استفاده قرار می‌گیرند، دستکاری شده باشند آنها را تشخیص داده و پیش از برطرف‌سازی، اجازه ارسال آن را نمی‌دهد. • ایجاد، حذف و تغییر در گزارش توسط افراد فاقد صلاحیت را تشخیص داده و از آنها جلوگیری می‌کند.
	22.3	Secure Handling of Log Data (مدیریت امن داده‌های لاگ)	برای ایمن‌سازی و مدیریت داده‌های لاگ، و با در نظر گرفتن هدفی که لاگ‌ها برای آن ایجاد شده‌اند، باید تمهیداتی پیاده‌سازی گردد. باید سازوکارهایی برای **شناسایی خرابی در سیستم‌های ثبت لاگ** ایجاد گردد. ثبت فعالیت‌های غیرعادی باید در برابر **دستکاری (Tampering)** و **دسترسی غیرمجاز** محافظت شود؛ این حفاظت شامل حالت‌های زیر است: • در حالت ذخیره‌شده • در حالت استفاده، در موارد مرتبط • در حین انتقال

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
SM.3 Data and (legacy) system security **امنیت داده‌ها و سیستم‌های به ارث رسیده (قدیمی)**	23.1	ICT (Security) Systems, tools, and solutions (سامانه‌ها، ابزارها و راهکارهای فاوا (امنیتی))	راهکارها و ابزارهای امنیتی باید به‌گونه‌ای طراحی، تهیه و پیاده‌سازی شوند که **تاب‌آوری، تداوم و محرمانگی، یکپارچگی و دسترس‌پذیری** سامانه‌های فاوا، به‌ویژه برای سامانه‌هایی که از عملیات حیاتی یا مهم پشتیبانی می‌کنند، تضمین گردد.
	23.2	Data Protection Practices (روش‌های حفاظت داده‌ها)	می‌بایست پیکربندی امنی برای دارایی‌های فاوا ایجاد شود که مشتمل بر رویه‌ها و فنون رایج صنعتی بوده و هدف از آن کاهش میزان مواجهه با تهدیدات سایبری باشد. به گونه‌ای پیاده‌سازی شود که محرمانگی، صحت و دسترس‌پذیری تأمین شده، از اتلاف و نشت داده‌ها جلوگیری گردد و در برابر کدهای مخرب حفاظت ایجاد شود. داده‌ها باید در برابر ریسک‌های ناشی از مدیریت داده، از جمله مدیریت ضعیف، ریسک‌های پردازشی و خطای انسانی محافظت شوند. انتقال داده‌ها باید به صورت امن انجام شود و ریسک‌های مرتبط با **خرابی یا از دست رفتن داده، دسترسی غیرمجاز و نقص‌های فنی که ممکن است مانع فعالیت کسب‌وکار شوند** به حداقل برسد. کنترل‌های دسترسی باید بر اساس **طرح‌های طبقه‌بندی داده** اعمال شود. همچنین باید به‌صورت دوره‌ای از استقرار مؤثر این پیکربندی‌های پایه اطمینان حاصل گردد.
	23.3	Vendor Recommended Security Settings (تنظیمات امنیتی توصیه شده توسط فروشنده)	باید تنظیمات و اقدامات امنیتی توصیه‌شده توسط ارائه‌دهنده خدمات فاوا شخص ثالث که خدمتی ارائه می‌دهد، مورد توجه قرار گیرد. همچنین باید اقدامات فنی و سازمانی برای **کاهش ریسک‌های مرتبط با زیر ساختی که توسط ارائه‌دهنده فاوا شخص ثالث استفاده و مدیریت می‌شود** پیاده‌سازی گردد.
	23.4	Endpoint Devices (دستگاه‌های کاربری)	سازمان باید الزامات مربوط به استفاده از دستگاه‌های کاربری قابل‌حمل و غیرقابل‌حمل را برقرار و اعمال نماید. همچنین باید اطمینان حاصل شود که انتقال و ذخیره‌سازی داده‌ها صرفاً از طریق رسانه‌های ذخیره‌سازی، سامانه‌ها و دستگاه‌های کاربری مجاز انجام می‌شود و تنها نرم‌افزارهای مورد تأیید بر روی این دستگاه‌ها نصب و مورد استفاده قرار می‌گیرند. همچنین باید تضمین شود که فقط **نرم‌افزارهای مجاز** بر روی دستگاه‌های پایانه نصب می‌شوند. اقدامات امنیتی باید به‌گونه‌ای پیاده‌سازی شوند که **دورکاری و استفاده از دستگاه‌های شخصی** تأثیر منفی بر امنیت کلی مؤسسه نداشته باشد. این اقدامات شامل موارد زیر است: • استفاده از یک راهکار مدیریت متمرکز برای مدیریت و پاک‌سازی (Wipe) از راه دور دستگاه‌ها؛ • به‌کارگیری مکانیزم‌های امنیتی که قابل تغییر، حذف یا دور زدن نباشند؛ • استفاده از دستگاه‌های ذخیره‌سازی قابل‌حمل تنها در صورتی که ریسک باقیمانده فاوا در محدوده تحمل ریسک از پیش تعیین‌شده قرار داشته باشد. همچنین باید کنترل‌های امنیتی به گونه‌ای اعمال شود که تنها نصب نرم‌افزارهای مجاز بر روی سامانه‌ها و دستگاه‌های پایانه میسر باشد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
	23.5	Secure Data Deletion and Disposal (حذف و امحا امن داده)	باید فرآیندی برای حذف امن داده‌ها در داخل و خارج از محل سازمان ایجاد شود. همچنین باید فرآیندی برای امحا یا از رده خارج‌سازی امن دستگاه‌های ذخیره‌سازی داده در داخل و خارج از محل سازمان که حاوی اطلاعات محرمانه هستند، تدوین و اجرا گردد.
SM.4 Encryption and cryptography **رمزنگاری و رمزگذاری**	24.1	Data Encryption (رمزنگاری داده‌ها)	یک سیاست‌نامه برای رمزنگاری داده‌ها در حالت ذخیره، انتقال و در صورت امکان در حالت پردازش، با در نظر گرفتن طبقه‌بندی داده و ارزیابی ریسک باید تدوین شود. در مواردی که امکان رمزنگاری داده در حال پردازش وجود ندارد، باید رویه‌هایی تعیین گردد تا پردازش در محیطی جداگانه و محافظت‌شده انجام شود، یا اقدامات معادل دیگری به کار گرفته شود. همچنین باید قواعدی برای **رمزنگاری ارتباطات شبکه داخلی و ترافیک با طرف‌های خارجی** پیاده‌سازی شود که با طبقه‌بندی داده‌ها و ارزیابی ریسک هم‌راستا باشد.
	24.2	Cryptographic Key Management and Lifecycle (مدیریت چرخه حیات و کلیدهای رمزنگاری)	باید پروتکل‌هایی برای استفاده صحیح، حفاظت و مدیریت چرخه حیات کلیدهای رمزنگاری تدوین شود. همچنین لازم است معیارهایی برای انتخاب روش‌ها و فنون رمزنگاری تعریف گردد که شامل بهترین رویه‌ها و استانداردهای رایج صنعتی باشد. در صورت عدم امکان پیروی از این استانداردها، باید اقدامات مناسب جهت کاهش ریسک انجام شود. الزامات مدیریت و کنترل کلیدهای رمزنگاری باید در تمام مراحل چرخه حیات آن‌ها مشخص باشد، این مراحل عبارتند از: تولید، ذخیره‌سازی، پشتیبان‌گیری، بایگانی، بازیابی، انتقال، بازنشستگی، لغو اعتبار و امحاء. همچنین باید روش‌هایی برای بازیابی کلیدهای رمزنگاری در شرایطی مانند از دست رفتن، افشا یا آسیب‌دیدن آن‌ها تعیین گردد. تحولات حوزه **رمزنگاری** باید پایش شده و در صورت نیاز، فناوری رمزنگاری به‌روزرسانی یا تغییر داده شود. در صورتی که امکان تغییر یا به‌روزرسانی فناوری وجود نداشته باشد، باید اقدامات پایش و کاهش ریسک اجرا گردد. در نهایت، باید فهرستی جامع برای تمامی گواهی‌نامه‌ها و دستگاه‌های نگهداری گواهی‌نامه‌ها نگهداری شود.
SM.5 Identity and access management **مدیریت هویت و دسترسی**	25.1	Identity Management (مدیریت هویت)	به هر یک از کارکنان سازمان یا کارکنان پیمانکاران که به اطلاعات و دارایی‌های فاوای سازمان دسترسی دارند، باید یک شناسه منحصربه‌فرد اختصاص داده شود. سیاست‌نامه، رویه‌ها و فرآیندهای مدیریت چرخه عمر هویت‌ها باید پیاده‌سازی شوند و ایجاد، تغییر، بازبینی دوره‌ای دسترسی‌ها، غیرفعال سازی موقت و حذف حساب‌های کاربری را پوشش دهند. در صورت امکان، باید از **راهکارهای خودکار** استفاده شود.
	25.2	Privilege Access Management (مدیریت دسترسی ممتاز)	سطح دسترسی باید بر اساس اصول نیاز به دانستن، نیاز به استفاده و کمترین سطح دسترسی تعریف و الزامات مربوط به دسترسی از راه‌دور و دسترسی اضطراری در آن پیشبینی شود. با اعمال تفکیک وظایف صحیح در مدیریت دسترسی‌ها، از دسترسی‌های غیرموجه یا ترکیب‌های اختیاری که ممکن است کنترل‌ها را دور بزنند، جلوگیری شده است. با توجه به ممنوعیت استفاده از حساب‌های کاربری مشترک یا عمومی، تمام اقدامات صورت گرفته در سامانه‌ها به کاربر مشخصی قابل انتساب بوده و او نسبت به آن‌ها پاسخگو است. همچنین، کنترل‌ها و ابزارهایی برای محدودکردن دسترسی غیرمجاز پیاده‌سازی شده است.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
	25.3	Account Management (مدیریت حساب)	میبایست رویه‌هایی برای اعطا، تغییر و لغو مجوز دسترسی همراه با تعیین نقش‌ها و مسئولیت‌ها تدوین گردد. برای نگهداری **لاگ‌های دسترسی (Access Logs)** باید مدت زمان مشخصی تعریف گردد. دسترسی‌های ممتاز، اضطراری و مدیریتی باید بر اساس **نیاز به استفاده** یا به صورت موردی تخصیص داده شوند و در این زمینه از راهکارهای خودکار برای مدیریت دسترسی‌های ممتاز استفاده شود. مجوز دسترسی باید به‌محض پایان همکاری یا زمانی که دیگر نیازی به آن نباشد، به‌سرعت لغو گردد. بازبینی دوره‌ای سطح دسترسی باید انجام شود، به‌طوری‌که حداقل **سالانه برای سامانه‌های غیرحیاتی فاوا** و **هر شش ماه یک‌بار برای سامانه‌های حیاتی** صورت گیرد.
	25.4	Authentication Methods (روش‌های احراز هویت)	روش‌های احراز هویت باید متناسب با طبقه‌بندی و پروفایل ریسک دارایی‌های فاوا به‌کار گرفته شوند. روش‌های **احراز هویت قوی** به‌طور ویژه برای موارد زیر باید پیاده‌سازی گردد: • دسترسی از راه‌دور (Remote Access) • دسترسی‌های ممتاز (Privileged Access) • دسترسی به دارایی‌های حیاتی فاوا
SM.6 Physical and environmental security **امنیت فیزیکی و محیطی**	26.1	Physical and environmental security (امنیت فیزیکی و محیطی)	باید اقداماتی برای حفاظت از محیط (شامل محل‌های استقرار، مراکز داده و نواحی حساس تعیین‌شده) که دارایی‌های مهم در آن‌ها قرار دارند، در برابر حملات، حوادث و تهدیدها و مخاطرات محیطی اجرا شود. سطح حفاظت در برابر تهدیدات محیطی باید متناسب با اهمیت محل نگهداری دارایی و سطح بحرانی بودن عملیات باشد. دارایی‌ها باید چه در محل و چه در خارج از سازمان محافظت شوند و **محرمانگی، یکپارچگی و دسترس‌پذیری** آن‌ها تضمین گردد. این اقدامات باید بر اساس نتایج ارزیابی ریسک تعیین شوند. همچنین باید رویه‌هایی مانند **میز کار پاک** و اطمینان از عدم نمایش اطلاعات حساس روی نمایشگرها در مراکز پردازش و محل دسترسی به دارایی‌های حیاتی فاوا رعایت شود. افراد مجاز برای ورود به محل‌های حیاتی مؤسسه مالی باید شناسایی و ثبت شوند. سطح دسترسی فیزیکی به دارایی‌های حیاتی فاوا باید بر اساس اصول **نیاز به‌دانستن، کمترین سطح دسترسی** و نیازهای موردی مطابق با سیاست‌نامه مدیریت دسترسی اعطا شود. دسترسی فیزیکی به محل‌ها، مراکز داده و نواحی حساس باید پایش شود و با طبقه‌بندی دارایی‌ها و سطح اهمیت هر ناحیه هم‌راستا باشد. سطح دسترسی فیزیکی باید به‌صورت دوره‌ای بازبینی شده و دسترسی‌های غیرضروری به‌سرعت لغو شوند.
SM.7 Security awareness **آگاهسازی امنیتی**	27.1	Resilience Training Programs (برنامه‌های آموزش تاب‌آوری)	آگاه‌سازی امنیتی و تاب‌آوری عملیاتی دیجیتال باید به‌عنوان بخش جدایی‌ناپذیر برنامه‌های آموزش کارکنان پیاده‌سازی شود و تمامی کارکنان از جمله مدیریت ارشد را پوشش دهد. سطح و میزان آموزش باید متناسب با نقش‌ها و مسئولیت‌های کارکنان تنظیم گردد. محتوای آموزشی باید شامل موضوعاتی مانند امنیت شبکه، درس‌آموخته‌های برگرفته از رخدادهای گذشته، هوش تهدید، مقابله با نفوذ و حملات سایبری، و روش‌های حفاظت از داده‌ها از جمله رمزگذاری و رمزنگاری باشد.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			برنامه آموزش تاب‌آوری باید به صورت سالانه اجرا شود. کارکنان باید در زمینه الزامات امنیتی فاوا آموزش ببینند و با کانال‌های تعیین شده برای گزارش فعالیت‌های مشکوک یا غیرعادی آشنا باشند. با پایان همکاری، کارکنان موظف به بازگرداندن تمام دارایی‌های اطلاعاتی و فاوا می‌باشند.
	27.2	Inclusion of Third-Party Providers (مشارکت ارائه‌دهندگان شخص ثالث)	در صورت نیاز، ارائه‌دهندگان خدمات فاوا شخص ثالث باید در برنامه‌های آموزشی مرتبط گنجانده شوند. طرف‌های ثالث باید از الزامات امنیت فاوا مطلع شده و کانال‌های تعیین‌شده برای گزارش فعالیت‌های غیرعادی به ایشان اطلاع‌رسانی شود. ارائه‌دهندگان شخص ثالث در زمان پایان همکاری یا خاتمه قرارداد، موظف به بازگرداندن تمامی دارایی‌های فاوای متعلق به مؤسسه مالی می‌باشند.
SM.8 Vulnerability and patch management **مدیریت آسیب‌پذیری و وصله‌های ترمیمی**	28.1	Resource Management (مدیریت منابع)	منابع اطلاعاتی معتبر و مرتبط باید شناسایی و به‌روز نگه داشته شوند تا سازمان بتواند از آسیب‌پذیری‌های جدید و موجود آگاه باشد. استفاده از کتابخانه‌های نرم‌افزاری متن‌باز پیمانکار، باید پایش شود و نسخه‌ها و به‌روزرسانی‌های احتمالی آن‌ها ردیابی گردد (همچنین به بندهای ۲۸,۲–۲۸,۳ مراجعه شود).
	28.2	Vulnerability Management (مدیریت آسیب‌پذیری)	سیاست‌نامه، رویه‌ها و پروتکل‌های مدیریت آسیب‌پذیری‌ها به همراه ابزارهای مربوطه تدوین شود. اسکن و ارزیابی خودکار آسیب‌پذیری باید بر روی دارایی‌های فاوا انجام گیرد. برای دارایی‌هایی که از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند، اسکن‌ها و ارزیابی‌ها باید به‌صورت **هفتگی** انجام شود. آسیب‌پذیری‌های شناسایی‌شده باید ثبت، وضعیت رفع آن‌ها پایش و اصلاحات انجام‌شده تأیید شوند. در صورت لزوم، آسیب‌پذیری‌های شناسایی‌شده باید به صورت مسئولانه به مشتریان، طرف‌های ذی‌نفع و عموم اعلام شوند. ارائه‌دهندگان خدمات شخص ثالث باید ملزم شوند آسیب‌پذیری‌های مرتبط با خدمات خود را گزارش دهند. این گزارش شامل بررسی آسیب‌پذیری‌ها، تعیین علل ریشه‌ای و اجرای راه‌حل‌های مناسب توسط ارائه‌دهندگان خدمات است. بطور خاص، برای **سپرده‌گذاری مرکزی اوراق بهادار (CSD)** و **اتاق‌های پایاپای مرکزی (CCP)**، ارزیابی آسیب‌پذیری می‌بایست پیش از هرگونه استقرار/ استقرار مجدد برنامه‌ها و مؤلفه‌های زیرساختی جدید/ موجود و همچنین خدمات فناوری اطلاعاتی که پشتیبان کارکردهای حیاتی یا مهم می‌باشند، انجام پذیرد.
	28.3	Patch Management (مدیریت وصله‌های ترمیمی)	دستورالعمل، رویه‌ها و پروتکل‌های لازم شامل ابزارهای مورد نیاز برای فرآیند مدیریت وصله‌ها (نرم‌افزارهای به‌روزرسانی امنیتی) تدوین شود. و صله‌ها و به‌روز سانی‌های موجود برای دارایی‌های فاوا مانند نرم‌افزار و سخت‌افزار باید تا حد امکان با ا ستفاده از ابزارهای خودکار، شنا سایی و ارزیابی شوند. وصله‌ها باید برای رفع آسیب‌پذیری‌های شناسایی‌شده در بازه زمانی از پیش تعیین‌شده اعمال شوند. اولویت ن صب و صله‌ها و سایر اقدامات کاهش ری سک باید بر ا ساس اهمیت آ سیب‌پذیری و طبقه‌بندی و پروفایل ری سک دارایی‌های تحت تأثیر تعیین گردد. رویه‌های اضطراری برای اعمال وصله و به‌روزرسانی دارایی‌های فاوا باید تدوین گردد. وصله‌ها و به‌روزرسانی‌های دارایی‌های فاوا ابتدا باید مورد آزمون قرار گرفته و سپس نصب شوند.

زیر دامنه	شناسه	کنترل‌ها	توصیف کنترل
			برای نصب وصله‌ها و به‌روزرسانی‌ها باید مهلت اجرای مشخصی تعیین شود و در صورت عدم امکان رعایت سررسیدهای تعیین شده، سازوکاری تعریف گردد که در آن مشخص شود موضوع به چه کسانی در سطوح بالاتر گزارش شده و چه مراحلی طی خواهد شد سازوکاری تعریف گردد که در آن مشخص شود موضوع به چه کسانی در سطوح بالاتر گزارش شده و چه مراحلی طی خواهد شد(رویه تشدید[۷۱]) در مواردی که وصله‌ای موجود نبوده یا قابل نصب نباشد، باید اقدامات جایگزین کاهش ریسک در همان سررسیدهای تعیین شده، شناسایی و اجرا شود.

[۷۱] Escalation procedure

۷. تأثیر DORA بر حسابرسی داخلی

۷,۱. الزامات مستقیم DORA برای حسابرسی داخلی

DORA به منظور تقویت توانمندی بخش مالی برای مقابله با خطرات عملیاتی دیجیتال، فناوری اطلاعات و ارتباطات و امنیت سایبری طراحی شده و چندین الزام جدید را با هدف رعایت آنها به نهادهای مالی تحمیل می‌کند. این امر اثرات قابل توجهی بر عملکرد حسابرسی داخلی دارد؛ زیرا مانند آنچه که در ماده‌های ۵، ۶ و ۱۱ آمده است، به‌طور مستقیم انتظاراتی را نسبت به این کارکرد اعمال می‌کند.

ماده ۵- حاکمیت و سازماندهی

بدنه مدیریتی نهاد مالی باید تمامی مراتب مربوط به چارچوب مدیریت ریسک فناوری اطلاعات و ارتباطات را که در ماده ۶ آمده است، تعریف، تصویب، و بر آنها نظارت نموده و مسئول اجرای آن باشد. علاوه بر این، هیئت‌مدیره باید برنامه‌های حسابرسی داخلی فناوری اطلاعات و ارتباطات نهاد مالی، حسابرسی‌های فاوا و تغییرات اساسی آنها را تصویب کرده و به‌طور دوره‌ای مورد بازبینی قرار دهد.

ماده ۶- چارچوب مدیریت ریسک فناوری اطلاعات و ارتباطات

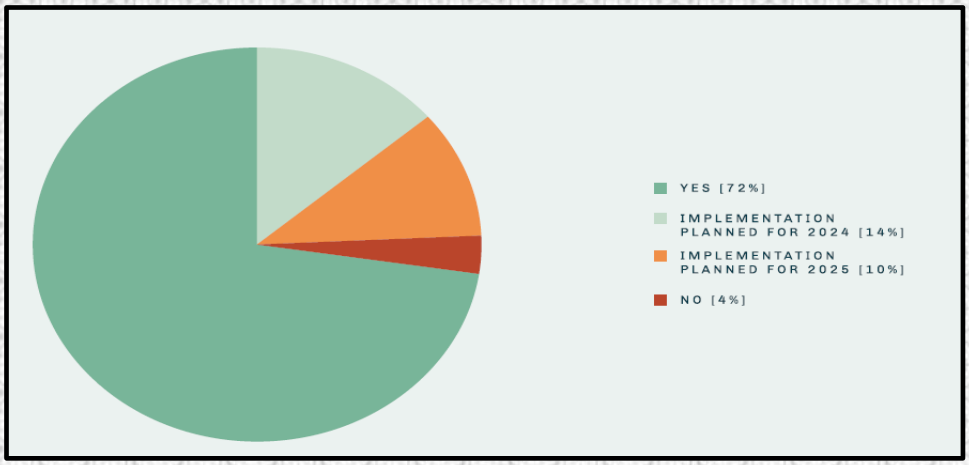
نهادهای مالی باید اطمینان حاصل کنند که تفکیک و استقلال مناسب میان کارکردهای مدیریت ریسک فناوری اطلاعات و ارتباطات، کنترل و حسابرسی داخلی، مطابق با مدل سه خط دفاعی یا یک مدل داخلی مدیریت ریسک و کنترل وجود داشته باشد. علاوه بر این، چارچوب مدیریت ریسک فناوری اطلاعات و ارتباطات نهادهای مالی به‌جز شرکت‌های کوچک، به‌طور منظم باید مطابق با برنامه حسابرسی نهاد مالی، تحت حسابرسی داخلی قرار گیرد. حسابرسان درگیر باید به‌طور مناسب از دانش، مهارت و تخصص کافی در زمینه ریسک فاوا، و استقلال برخوردار باشند. تمرکز و دفعات اجرای حسابرسی فناوری اطلاعات و ارتباطات باید با ریسک فاوا نهاد مالی متناسب باشد. بر اساس نتایج حاصل از بررسی حسابرسی داخلی، نهادهای مالی باید یک فرآیند رسمی پیگیری[۷۲] ایجاد کنند که شامل قوانین مربوط به تأیید و اصلاح به‌موقع یافته‌های بحرانی حسابرسی فناوری اطلاعات و ارتباطات باشد.

ماده ۱۱- پاسخ و بازیابی

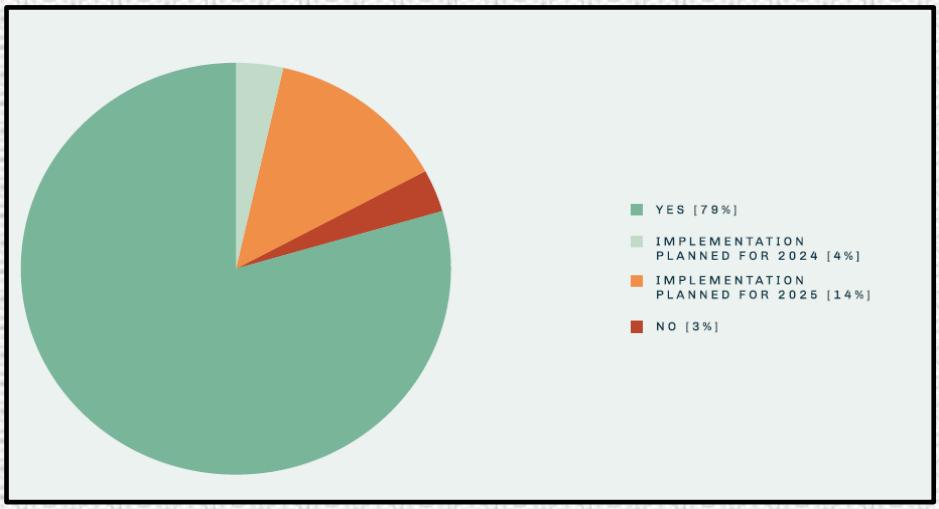
به عنوان بخشی از چارچوب مدیریت ریسک فاوا که در ماده ۶ آمده است، نهادهای مالی باید طرح‌های پاسخ و بازیابی مرتبط با فناوری اطلاعات و ارتباطات را پیاده‌سازی کنند. این طرح‌ها باید در مورد نهادهای مالی غیر از شرکت‌های کوچک، تحت بازبینی‌های مستقل حسابرسی داخلی قرار گیرد.

بر اساس نظرسنجی انجام‌شده در سه‌ماهه اول سال ۲۰۲۴ در صنعت مالی، مشخص شد که بدنه مدیریتی ٪۷۲ از شرکت‌ها در حال حاضر حسابرسی فاوا، برنامه‌های آن، و تغییرات اساسی آنها را تصویب نموده و به‌طور دوره‌ای مورد بازبینی قرار می‌دهند. تنها ٪۲۴ از پاسخ‌دهندگان همچنان در حال پیاده‌سازی این روند هستند؛ این درحالیست که ٪۴ از آنها هنوز برنامه‌ای برای پیاده‌سازی ندارند (شکل۷). این امر نشان می‌دهد که حسابرسی چارچوب مدیریت ریسک فاوا یا به‌طور منظم در حال انجام است و یا اینکه در آینده و بر اساس برنامه تصویب‌شده حسابرسی فاوا انجام خواهد شد. همچنین، این موضوع دربرگیرنده حسابرسی برنامه‌های پاسخ و بازیابی فاوا است. این مطالعه به خوبی نشان می‌دهد که فرآیند پیگیری اقدامات اصلاحی یافته‌های بحرانی حسابرسی فاوا به میزان بالایی (٪۷۹) برقرار شده است (شکل ۸).

[۷۲] formal follow-up process



شکل شماره ۷- درصد شرکت‌های بیمه با بدنه مدیریتی مورد تایید که در خصوص برنامه حسابرسی داخلی فاوا، حسابرسی فاوا، و تغییرات آنها بطور مستمر مورد بازبینی قرار گرفته‌اند.



شکل شماره ۸- شرکت‌های بیمه با فرآیند پیگیری استقرار یافته شامل قوانینی برای اصلاح و صحت‌سنجی یافته‌های فاوای بحرانی

۷,۲. سایر تأثیرات DORA بر حسابرسی داخلی

مقررات DORA بخش‌های مختلفی دارد که معرف بررسی‌های مستقل و اطمینان‌بخشی است. حتی اگر چنین بخش‌هایی به‌طور مستقیم به حسابرسی داخلی اشاره نداشته باشند، الزامات مرتبط باید توسط حسابرسی داخلی در اجرای ارزیابی ریسک حسابرسی و تعریف برنامه حسابرسی در نظر گرفته شوند. در اینجا به‌ویژه ماده‌های ۶، ۱۱، ۲۷، ۲۸ و ۳۰ از اهمیت خاصی برخوردارند. در حالی که برخی از قسمت‌های ماده‌های ۶ و ۱۱ الزامات مستقیمی را برای حسابرسی داخلی ایجاد می‌کنند، بخش‌های دیگر به بررسی‌ها و فعالیت‌های خطوط اول و دوم دفاعی که حسابرسی داخلی باید از آن‌ها مطلع باشد اشاره دارند. ماده‌های ۲۷، ۲۸ و ۳۰ به فعالیت‌هایی پرداخته‌اند که در صورت عدم تخصیص به منابع دیگر، می‌توانند توسط حسابرسی داخلی انجام شوند.

ماده ۶- چارچوب مدیریت ریسک فاوا

چارچوب مدیریت ریسک فاوا باید مستند گردیده و حداقل به‌طور سالیانه مورد بازبینی قرار گیرد؛ همچنین، در صورت بروز حوادث عمده مرتبط با فناوری اطلاعات و ارتباطات، و پس از دستورات نظارتی یا نتایج حاصل از آزمایش‌های مربوط به تاب‌آوری عملیاتی دیجیتال یا فرآیندهای حسابرسی، بازبینی شود. این چارچوب باید به‌طور مستمر و بر اساس تجاربی که از پیاده‌سازی و نظارت بر آن به دست آمده است، بهبود یابد. لازم به ذکر است، گزارش مربوط به بازبینی چارچوب مدیریت ریسک فاوا باید بنا به درخواست مقام ذی‌صلاحیت، ارائه شود.

ماده ۱۱- پاسخ و بازیابی

نهادهای مالی باید سیاست‌نامه تداوم کسب‌وکار فاوا و برنامه‌های پاسخ و بازیابی فاوا خود را به‌طور منظم بازبینی کنند و نتایج آزمون‌هایی را که سالیانه توسط خطوط دفاعی اول و دوم انجام می‌شوند و نیز توصیه‌هایی را که از بررسی‌های حسابرسی یا بازبینی‌های نظارتی به دست می‌آید، در نظر بگیرند.

ماده ۲۷- الزاماتی برای آزمایش‌کنندگان جهت انجام آزمون‌های نفوذ تهدید محور (TLPT)

در رابطه با مدیریت صحیح ریسک‌های مرتبط با آزمون نفوذهای تهدید محور، از جمله حفاظت مناسب از اطلاعات محرمانه نهاد مالی و جبران ریسک‌های تجاری نهاد مالی، باید یک اطمینان‌بخشی مستقل یا گزارش حسابرسی فراهم شود. در این ماده، قانون‌گذار تأکید می‌کند که آزمون‌های نفوذ تهدید محور، به‌ویژه باید بر ریسک‌های مرتبط با حفاظت از اطلاعات و اثرات منفی احتمالی بر عملیات تجاری تمرکز نمایند.

ماده ۲۸- اصول کلیدی برای مدیریت صحیح ریسک‌های فاوا مربوط به تأمین‌کنندگان خارجی

در اعمال حقوق دسترسی، بازرسی و حسابرسی تأمین‌کنندگان خدمات فاوا شخص ثالث، و بر اساس رویکرد مبتنی بر ریسک، نهادهای مالی باید با پیروی از استانداردهای حسابرسی پذیرفته‌شده، دفعات بازرسی، حسابرسی و همچنین زمینه‌های مورد حسابرسی را تعیین کنند. این امر باید به‌گونه‌ای صورت گیرد که با هر دستور نظارتی در خصوص استفاده و گنجاندن چنین استانداردهای حسابرسی مطابقت داشته باشد. در صورتی که توافقات قراردادی با تأمین‌کنندگان خدمات فاوا شخص ثالث در استفاده از خدمات فاوا شامل پیچیدگی‌های فنی بالایی باشد، نهاد مالی باید تأیید کند که حسابرسان داخلی یا خارجی، دارای مهارت و دانش کافی برای انجام مؤثر حسابرسی و ارزیابی‌های مربوطه هستند.

علاوه بر الزامات فوق، ماده ۳۰ به نکات کلیدی مفاد قراردادی تأمین‌کنندگان فناوری اطلاعات و ارتباطات اشاره دارد. با وجود آنکه تضمین توافقات قراردادی بر عهده حسابرسی داخلی نیست، حسابرسی داخلی باید در طول حسابرسی تأیید کند که مفاد مذکور در قراردادها وجود دارد.

ماده ۳۰- مفاد کلیدی قراردادی

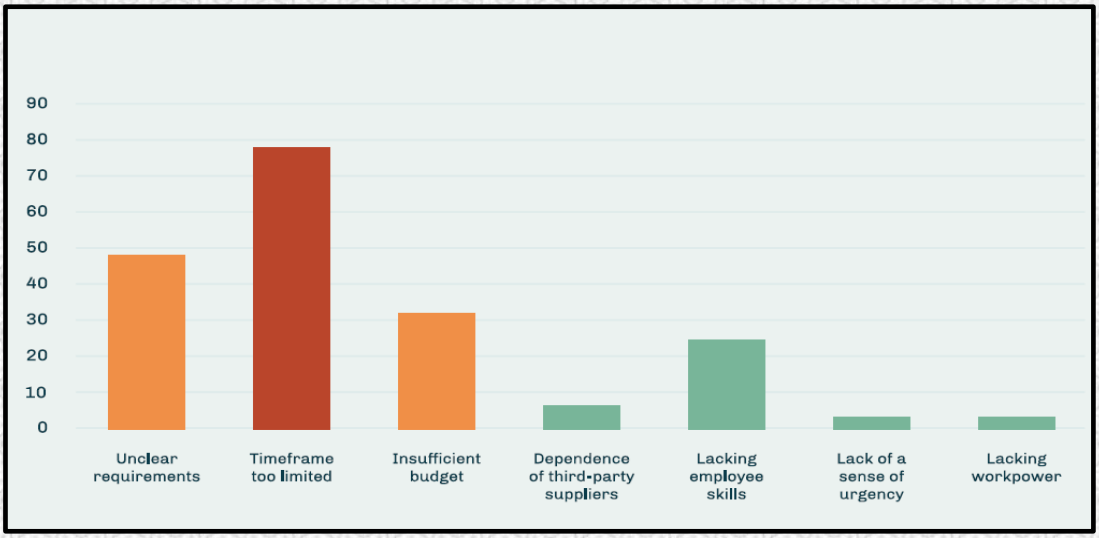
ترتیبات قراردادی در خصوص استفاده از خدمات فاوا باید شامل عناصر حق نظارت به‌طور مستمر، کارآیی تأمین‌کننده خدمات فناوری اطلاعات و ارتباطات شخص ثالث باشد که مستلزم موارد زیر است:

- حقوق نامحدود در خصوص دسترسی، بازرسی و حسابرسی توسط نهاد مالی یا شخص ثالث منصوب و مقام ذیصلاح، کپی برداری از مستندات مرتبط در محل در صورتی که این مستندات برای عملیات تأمین‌کننده خدمات فاوا شخص ثالث حیاتی بوده و با شرط آن که با سایر ملاحظات قراردادی یا سیاست‌نامه‌های اجرایی محدود یا منع نشده باشند؛
- حق توافق بر سطوح اطمینان جایگزین، آن هم در صورتی که حقوق سایر مشتریان تحت تأثیر قرار گرفته باشد؛
- تعهد تأمین‌کننده خدمات فاوای شخص ثالث به همکاری کامل در طول بازرسی و حسابرسی انجام‌شده توسط مقامات ذیصلاح، ناظر اصلی، نهاد مالی یا شخص ثالث منصوب‌شده؛
- تعهد تأمین‌کننده به ارائه جزئیات به نهاد مالی در خصوص دامنه، رویه‌های ملزم به پیروی و دفعات بازرسی و حسابرسی.

۷.۳. آموزش و ارتقای مهارت‌های حسابرسان داخلی

برای آموزش حسابرسان داخلی در خصوص DORA، رویکردی جامع و ساختاریافته لازم است تا اطمینان حاصل شود که آنها الزامات نظارتی را درک نموده و می‌توانند میزان انطباق را به‌طور مؤثری ارزیابی کنند. شرکت‌ها در پیاده‌سازی با چالش‌هایی در زمینه زمان، بودجه، مهارت و انتظارات روبه‌رو هستند. برای یک واحد حسابرسی داخلی، ضروری است الزامات را درک نموده و

مهارت‌های خود را ارتقا دهند. براساس نتایج مطالعه انجام‌شده، فقدان مهارت‌های کارکنان به عنوان چهارمین مشکل مهم در عدم انطباق با DORA شناخته شده است منعکس گردیده است (شکل ۹).



شکل شماره ۹- بزرگترین مسائل مورد انتظار در راستای جلوگیری از مطابقت موفقیت‌آمیز با DORA

دوره‌های آموزشی ممکن است شامل موضوعات کلیدی زیر باشد:

- **مقدمه‌ای بر DORA**: مروری بر DORA، اهداف، دامنه و الزامات اصلی آن.
- **مدیریت ریسک فناوری ارتباطات و اطلاعات**: درک ارزیابی ریسک فاوا، شناسایی و استراتژی‌های کاهش آن.
- **گزارش‌دهی و مدیریت حوادث**: رویه‌های گزارش‌دهی، مدیریت و تحلیل حوادث مرتبط با فاوا.
- **آزمایش تاب‌آوری عملیاتی**: روش‌های انجام آزمایش تاب‌آوری، از جمله تمرین‌های میزگرد، شبیه‌سازی و آزمایش‌های زنده.
- **مدیریت ریسک تأمین‌کنندگان خارجی**: ارزیابی و مدیریت ریسک‌های مرتبط با تأمین‌کنندگان خدمات فاوا شخص ثالث.
- **انطباق و گزارش‌دهی**: الزامات دقیق برای گزارش‌دهی انطباق، مستندسازی و ردیابی سوابق حسابرسی[۷۳].

و علاوه بر آن:

- **آموزش حین کار**: آموزش افراد تازه وارد با همکاری اعضای تیم با تجربه‌تر.
- **روش‌شناسی حسابرسی**: روش‌های حسابرسی برای ارزیابی انطباق با الزامات DORA باید توسعه یافته، و بر اساس بازخورد و یادگیری مستمر به‌طور مداوم بهبود یابد.

۸. برنامه دقیق حسابرسی برای DORA

این بخش شامل توصیه‌هایی برای واحدهای حسابرسی داخلی جهت برنامه‌ریزی حسابرسی‌ها، ملاحظات آزمون‌های حسابرسی DORA و برنامه پیشنهادی حسابرسی است. نظرات و دیدگاه‌های بیان‌شده در این فصل لزوماً بازتاب سیاست یا موضع رسمی هیچ سازمان یا مرجعی نمی‌باشند. اطلاعات موجود در این مطالعه صرفاً با هدف افزایش اطلاعات عمومی است.

۱- برنامه‌ریزی حسابرسی برای DORA: حسابرسی داخلی باید مهلت‌های قانونی مربوط به اقدامات مدیریتی مرتبط با DORA را در نظر گرفته و برنامه حسابرسی را با بازرسی‌های نظارتی احتمالی هماهنگ سازد تا از هم‌پوشانی یا شکاف‌های پوششی جلوگیری

[۷۳] Audit Trail

شود. همچنین، حسابرسی داخلی باید در طول یک برنامه چندساله گردشی، حوزه‌ها و تمرکزهای مختلفی مانند تاب‌آوری عملیاتی، سایبری، عملکردهای حیاتی یا مهم[۷۴] و آزمون‌های بازیابی را در نظر بگیرد. حسابرسی داخلی باید فعالیت‌های حسابرسی را از سال ۲۰۲۴ آغاز نموده (برای مثال، تأیید رویکرد شرکت برای پیاده‌سازی الزامات DORA، مانند تحلیل فاصله مناسب و کامل، ایجاد یک برنامه/ پروژه صحیح با مشارکت تمام بخش‌های مرتبط و اجرای فعالیت‌های عملیاتی مربوطه) و حسابرسی اثربخشی عملیاتی را در سال‌های بعد انجام دهد.

۲-آزمون‌های حسابرسی برای DORA: حسابرسی داخلی به ابزاری نیاز دارد تا فرآیند شناسایی ریسک‌های تمرکز بر تأمین‌کنندگان خدمات فاواشامل وابستگی‌های پایین‌دستی به پیمانکار فرعی[۷۵] را که از نقشه‌های فرآیندی شناسایی شده و منابع، فناوری‌ها و اشخاص ثالث بحرانی را مشخص می‌کنند، بررسی کند. همچنین، حسابرسی داخلی باید تأثیرات چارچوب نظارت سراسری اتحادیه اروپا را راجع به تأمین‌کنندگان فاوا شخص ثالث حیاتی و بر اساس تعریف مراجع نظارتی اروپا درک نموده و چگونگی اطمینان بر تأمین‌کنندگان فاوا و تأثیر آن بر رویکرد حسابرسی را ارزیابی کند (مانند حق حسابرسی، گواهینامه‌ها، ISAE 3402، SOC1 و SOC2).

۳- برنامه حسابرسی DORA: این محتوا به عنوان یک راهنمای جامع حسابرسی برای مقررات DORA طراحی نشده است. بلکه هدف آن برجسته سازی کنترل‌های اصلی سفارشی‌سازی فرآیند بازبینی بر اساس ویژگی‌های خاص نهادهای حسابرسی شونده است. با در نظر گرفتن ویژگی‌های متمایز این نهادها، حسابرسان می‌توانند میزان انطباق را به‌طور مؤثر ارزیابی کرده و نواحی قابل بهبود را شناسایی کنند.

۸،۱. برنامه‌ریزی حسابرسی برای DORA

حسابرسان باید دائماً عملکردهای خطوط اول و دوم دفاعی را به چالش کشیده تا در عین حفظ استقلال خود، کنترل‌ها و نظارت‌های مناسبی را ایجاد و حفظ نمایند. حسابرسی داخلی باید برنامه‌ای ایجاد کند تا از پوشش کافی الزامات DORA در طول سالیان اطمینان حاصل شده و یک حسابرسی اولیه را در سال ۲۰۲۴ برای طراحی و پیاده‌سازی در نظر بگیرد و در سال‌های بعد آن را با حسابرسی اثربخشی عملیاتی تقویت کند. حسابرسی داخلی می‌تواند با انجام حسابرسی‌های عمیق‌تر به جای حسابرسی سالانه در تمام دامنه، از تغییر تمرکز و دامنه برنامه دوره‌ای خود (تاب‌آوری عملیاتی، سایبری، کارکردهای کلیدی، آزمون‌های بازیابی) بهره‌مند شود. همسوسازی برنامه با بازرسی‌های نظارتی بالقوه برای جلوگیری از همپوشانی یا شکاف‌ها الزامی است.

برای رعایت DORA و بهبود تاب‌آوری عملیاتی نهادهای مالی، حسابرسی داخلی باید برنامه‌های حسابرسی خود را برای انطباق با DORA تهیه و به‌روزرسانی کند. برنامه‌ریزی حسابرسی شامل مراحل زیر است:

۱ - ارزیابی تحولات قانونی: حسابرسان برای بهبود تاب‌آوری عملیاتی دیجیتال باید با DORA و ابزارهای سیاست‌گذاری مرتبط شامل دامنه و اهداف آن آشنایی حاصل نمایند.

۲ - ارزیابی ریسک حسابرسی: حسابرسان باید ریسک‌های مرتبط با فاوا ، مانند حملات سایبری، نشت داده‌ها، خرابی‌های سیستم و سایر حوادثی که ممکن است بر کارکرد نهاد تأثیر بگذارد، را ارزیابی کنند. تحلیل احتمال و تأثیر این ریسک‌ها به اولویت‌بندی آنچه که باید به‌طور دقیق بررسی شود کمک می‌کند.

۳ - دامنه و اهداف حسابرسی: حسابرسان باید تصمیم بگیرند که چه فرآیندها، سیستم‌ها و کنترل‌هایی را باید بازبینی کنند و آنها را به‌گونه‌ای تطبیق دهند که تمام جنبه‌های DORA را در یک چرخه پوشش دهد. آنها باید اهداف روشنی مانند بررسی انطباق باDORA ، آزمایش کنترل‌های فاوا و یافتن نواحی قابل بهبود را تعریف کنند.

---

[۷۴] Critical and Important Functions (CIF)

[۷۵] 4th Parties

۴ - تخصیص منابع: حسابرسان باید تیمی برخوردار از تخصص در فاوا، امنیت سایبری و انطباق با مقررات تشکیل دهند. این تیم ممکن است شامل متخصصان داخلی یا خارجی باشد. برای انجام یک حسابرسی جامع، آنها باید منابع کافی مانند بودجه و زمان تخصیص دهند و زمان‌بندی را با مهلت‌های نظارتی و داخلی هماهنگ سازند.

۵ - آزمون‌های حسابرسی: حسابرسان باید روش‌هایی مانند مصاحبه، بررسی مستندات، آزمایش سیستم‌ها و تحلیل داده‌ها را برای جمع‌آوری شواهد انتخاب کنند. آنها باید از تکنیک‌های مختلف حسابرسی مانند آزمون کنترل، برای جمع‌آوری شواهد و ارزیابی کنترل‌ها استفاده کنند. همچنین، حسابرسان باید برای آزمایش کنترل‌ها و معاملات از روش‌های نمونه‌برداری استفاده کنند که از پوشش‌دهی و قابلیت اطمینان نتایج حسابرسی اطمینان حاصل شود. در خصوص الزامات نظارتی، حسابرسان باید با مقایسه روش‌های نهاد با الزامات DORA، هرگونه شکاف یا مشکلات عدم انطباق را شناسایی کنند. آنها باید اطمینان حاصل کنند که تمامی مستندات و شواهد انطباق موجود بوده و به‌طور صحیح نگهداری شده‌اند. آنها باید توجه ویژه‌ای به ارزیابی آزمایش‌های سناریو (از جمله آزمایش‌های نفوذ تهدید محور) و اینکه آیا نتایج ارزیابی‌ها منجر به برنامه‌های اصلاحی شده است، داشته باشند. همچنین، آنها باید بر آمادگی در مقابل حوادث سایبری بحرانی، شامل آموزش و تمرین (مانند شبیه‌سازی‌ها) با مدیریت ارشد، تیم‌های عملیات امنیتی و واحدهای تجاری تمرکز نمایند.

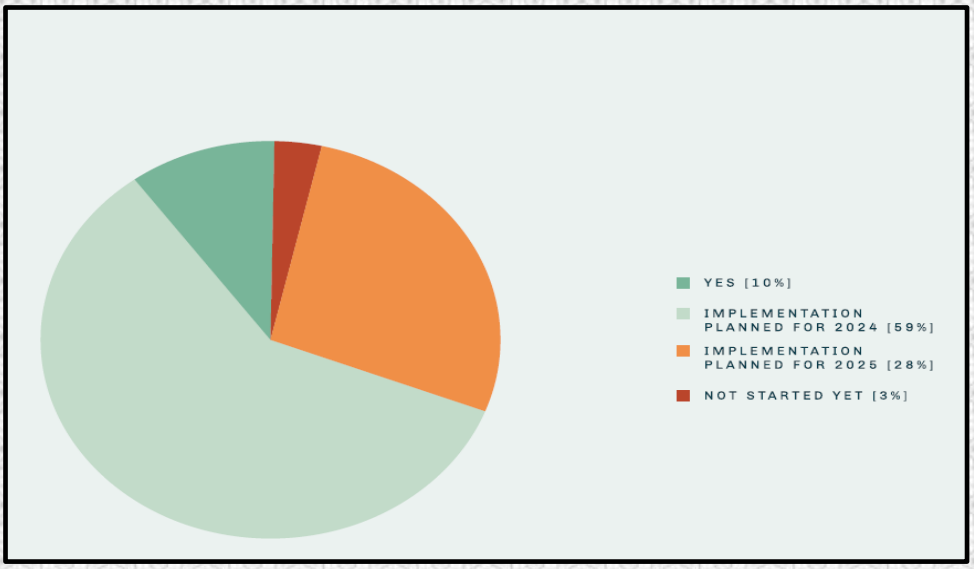
- گزارش‌دهی و پیگیری: حسابرسان باید یک گزارش جامع حسابرسی با یافته‌ها، نتایج و توصیه‌ها بنویسند، نواحی عدم انطباق و نیاز به بهبود را برجسته سازند، پاسخ مدیریت به یافته‌ها و توصیه‌های حسابرسی را دریافت کنند، اطمینان حاصل کنند که تعهدی برای رفع مشکلات شناسایی‌شده وجود دارد، و نیز برای اقدامات پیگیری جهت بررسی پیاده‌سازی توصیه‌ها و اطمینان از مؤثر بودن اقدامات اصلاحی برنامه‌ریزی کنند.

۸,۲. آزمون‌های حسابرسی برای DORA

در زیر، عناصر کلیدی که باید توسط واحد حسابرسی داخلی برای ارائه اطمینان در خصوص الزامات اصلی DORA آزمایش شوند، به همراه شواهد نتایج دقیق نظرسنجی برای هر عنصر خاص، آورده شده است.

۸,۳. تاب‌آوری

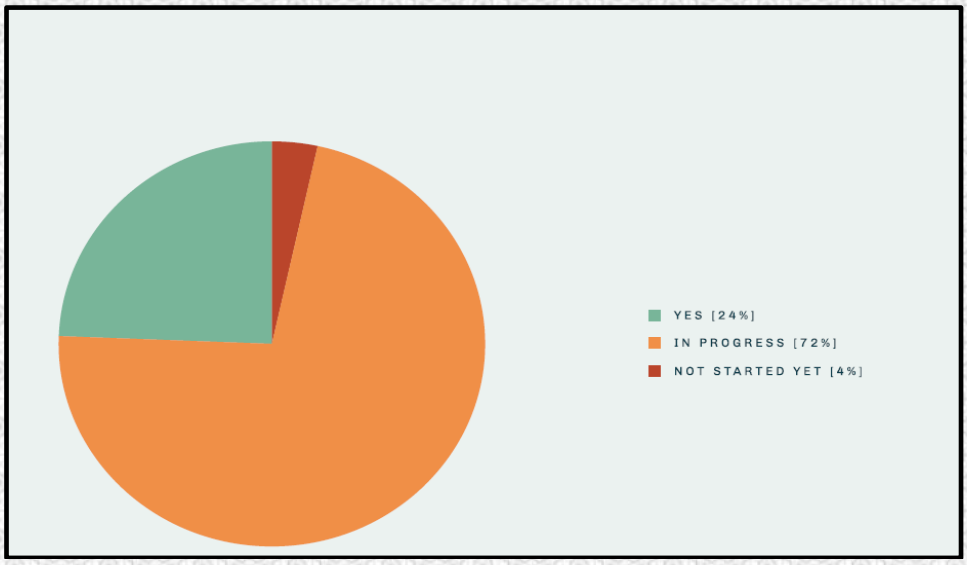
تاب‌آوری امری حیاتی است و نیاز به آزمایش دارد. همان‌طور که نتایج نظرسنجی نشان می‌دهد، تنها ۲۵٪ از شرکت‌ها تاکنون استراتژی تاب‌آوری دیجیتال را مطابق با الزامات DORA، توسعه داده‌اند. حسابرسی داخلی باید ارزیابی تاب‌آوری عملیاتی نهاد مورد حسابرسی را طبق استانداردهای DORA حداقل در سال ۲۰۲۵ در نظر بگیرد. در سال ۲۰۲۴، حسابرسی داخلی می‌توانست اقدامات مختلفی مانند بررسی الزامات پیش از پیاده‌سازی و بازبینی روش‌هایی را که برای این منظور توسط نهادها استفاده می‌شود، انجام دهد.



شکل شماره ۱۰- شرکت‌های بیمه‌ای که استراتژی تاب‌آوری دیجیتال تعیین نکرده‌اند.

۸,۴. کارکردهای حیاتی و مهم (CIF[۷۶])

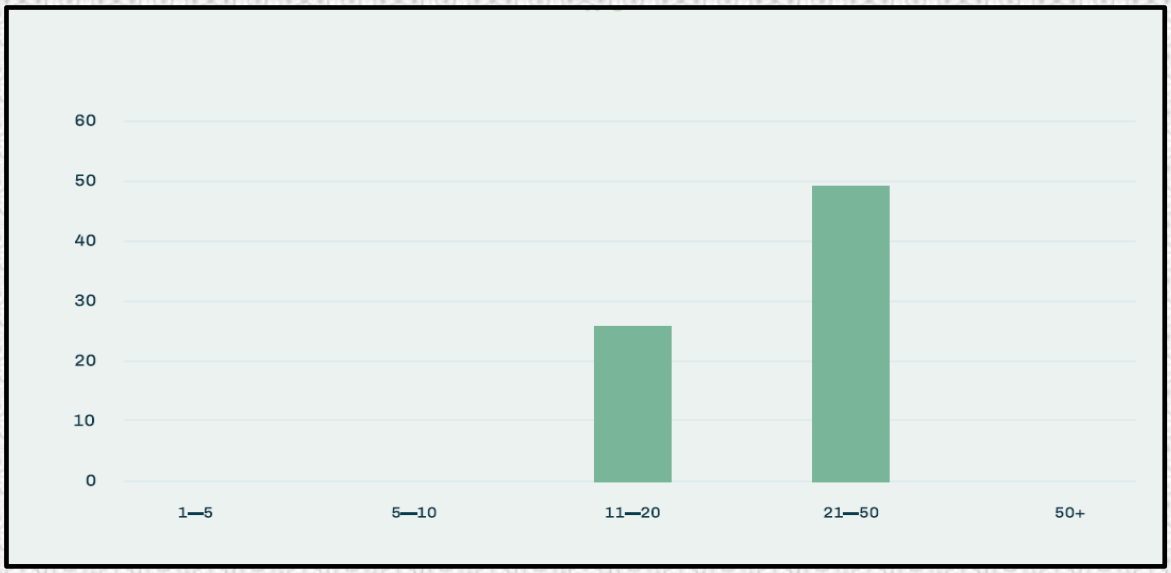
یکی از عناصر کلیدی حاکمیتی در DORA شناسایی کارکردهای حیاتی و مهمی است که در ماده ۳ آمده است. تا پایان سه‌ماهه اول سال ۲۰۲۴، تنها ٪۱۷ از شرکت‌ها گزارش داده‌اند که کارکردهای حیاتی را شناسایی کرده‌اند.



شکل شماره ۱۱- شرکت‌های بیمه‌ای که CIFهای خود را تعیین نموده‌اند.

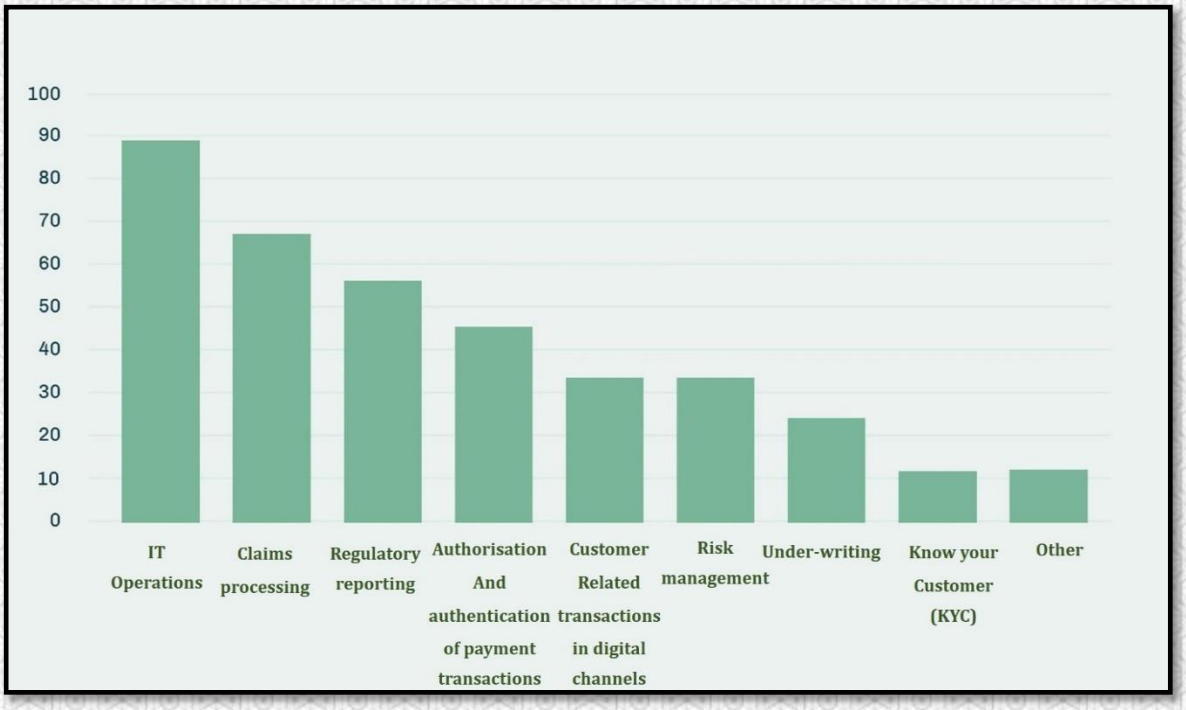
حدود ٪۱۶ از شرکت‌ها بیش از ۵۰ کارکرد حیاتی و مهم (CIF) دارند. هرچه تعداد این کارکردها بیشتر باشد، اجرا و ارائه اطمینان‌بخشی درباره آن‌ها دشوارتر می‌شود. حسابرسی داخلی، چه با انجام دوره‌ای و چه با ارزیابی‌های مبنی بر سناریو، باید برای انتخاب و بررسی کارکردهای حیاتی و مهم، رویکردی مبتنی بر ریسک را در برنامه حسابرسی به‌کار گیرد. حسابرسی داخلی باید فرآیند شناسایی ریسک‌های متمرکز را با ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات که بر کارکردهای حیاتی و مهم تأثیر می‌گذارند (ازجمله وابستگی‌های پایین‌دستی به پیمانکار فرعی)، بر مبنای نقشه‌های فرآیندی نمایش دهنده مهم‌ترین منابع، فناوری‌ها و اشخاص ثالث، آزمون کند.

[۷۶] Critical and Important Functions



شکل شماره ۱۲- تعداد کارکردهای حیاتی و مهم شناسایی شده در شرکت‌های مالی

کارکردهای جاری که به‌عنوان کارکردهای حیاتی و مهم شناسایی می‌شوند شامل عملیات فناوری اطلاعات، پردازش مطالبات، گزارش‌دهی نظارتی و تأیید پرداخت هستند.



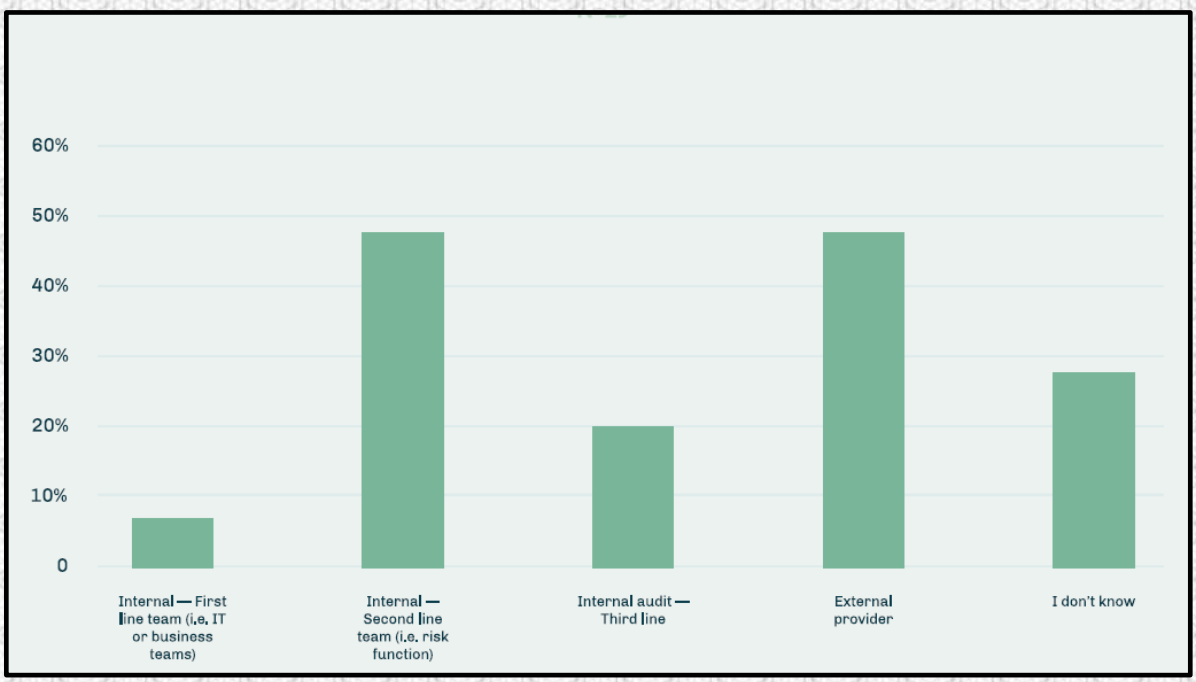
شکل شماره ۱۳- کارکردهای تطبیقی شناسایی شده به‌عنوان کارکردهای حیاتی و مهم

۸.۵. آزمون برنامه‌های بازیابی

هدف آزمون برنامه‌های بازیابی این است که اطمینان حاصل شود این برنامه‌ها اثربخش هستند و در صورت وقوع یک نقص یا فاجعه، به‌طور موفقیت‌آمیز قابل اجرا می‌باشند. همچنین اطمینان حاصل شود که این برنامه‌ها، تمامی ذی‌نفعان، از جمله توسعه‌دهندگان، کارکنان عملیاتی و افرادی که مسئول فرآیند بازیابی هستند، را دربر می‌گیرد.

DORA الزام می‌کند که بر روی تمامی سامانه‌ها و برنامک‌های حوزه فناوری اطلاعات و ارتباطات که برای کارکردهایی که از آنها پشتیبانی می‌کنند حیاتی یا مهم هستند، حداقل یک‌بار در سال، آزمون‌هایی انجام شود.

حسابرسی داخلی معمولاً مسئول انجام آزمون‌های مستقل تاب‌آوری عملیاتی نیست؛ تنها ۱۵٪ از پاسخ‌دهندگان نظرسنجی اظهار داشته‌اند که حسابرسی داخلی شخصا این آزمون‌ها را انجام می‌دهد. آزمون مستقل می‌تواند توسط یک واحد مستقل در خط اول، خط دوم، خط سوم یا توسط ارائه‌دهندگان خدمات اطمینان بخشی خارجی انجام شود. حسابرسان داخلی می‌توانند استراتژی و کارآیی تجاری را برای آزمون‌های بازیابی از طریق رویکردهای مختلف (غیرجامع) مرور کنند:



شکل شماره ۱۴- کسانی که آزمون‌های تاب‌آوری عملیاتی مستقلی را برای شرکت‌های مالی هدایت می‌کنند.

- **آزمون‌های میزگردی**[۷۷]: شرکت‌کنندگان سناریوهای بازیابی بحران را در قالبی مبتنی بر بحث و گفتگو مرور می‌کنند. این کار به شناسایی شکاف‌ها در برنامه‌ها و رویه‌ها کمک می‌کند.
- **آزمون‌های شبیه‌سازی بازیابی پس از فاجعه**: مشارکت‌کنندگان، آزمون‌های شبیه‌سازی را که اختلالات فناوری اطلاعات دنیای واقعی را در یک محیط اختصاصی و بدون تأثیرگذاری بر عملیات واقعی تقلید می‌کنند، اجرا می‌نمایند که می‌تواند شامل اجرای سامانه‌های پشتیبان یا انتقال به سایت‌های جایگزین باشد.
- **آزمون بازیابی پس از فاجعه به‌طور زنده:** آزمون‌های زنده در مواردی که امکان‌پذیر و ایمن باشد، شامل اختلالات واقعی بوده و ممکن است اجرای برنامه‌های تداوم کسب‌وکار را ضروری سازند. این آزمون‌ها می‌توانند طی بازه‌های برنامه‌ریزی‌شده یا در محیط‌های کنترل‌شده انجام شوند.

علاوه‌براین، بسته به دامنه فعالیت‌های آزمون، رویکردهای متفاوتی قابل استفاده هستند:

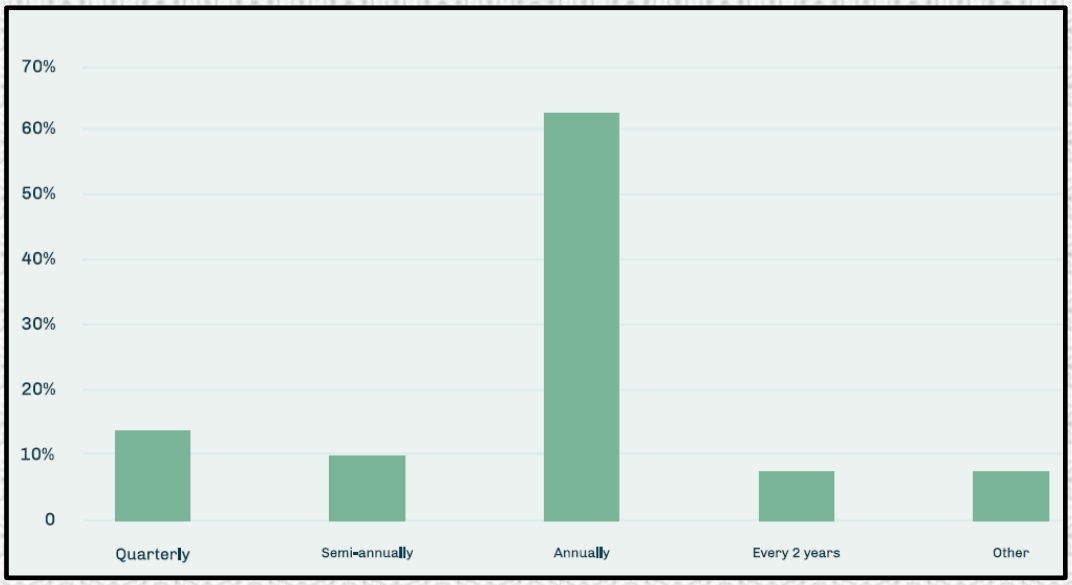
- **آزمون‌های بازیابی پس از فاجعه**: آزمون‌ها می‌توانند تنها شامل سامانه‌های فناوری اطلاعات مانند بررسی کفایت برنامه بازیابی پس از فاجعه برای بازیابی اپلیکیشن‌ها و زیرساخت‌های فناوری اطلاعات باشند. در این حالت، مالکان کسب‌وکاری برنامک‌ها معمولاً برای بررسی ملزومات عینی زمان بازیابی و کارکردهای برنامک‌ها مشارکت داده می‌شوند.

[۷۷] Tabletop Exercises

- **آزمون تداوم کسب‌وکار**: آزمون‌ها با دربرگرفتن سامانه‌های فناوری اطلاعات و فرآیندهای کسب‌وکاری مرتبط، شامل انتقال کارکنان از یک سایت کسب‌وکاری به سایتی دیگر یا آزمون قابلیت‌های دورکاری، از بازیابی مؤثر این فرآیندها اطمینان حاصل می‌کنند.

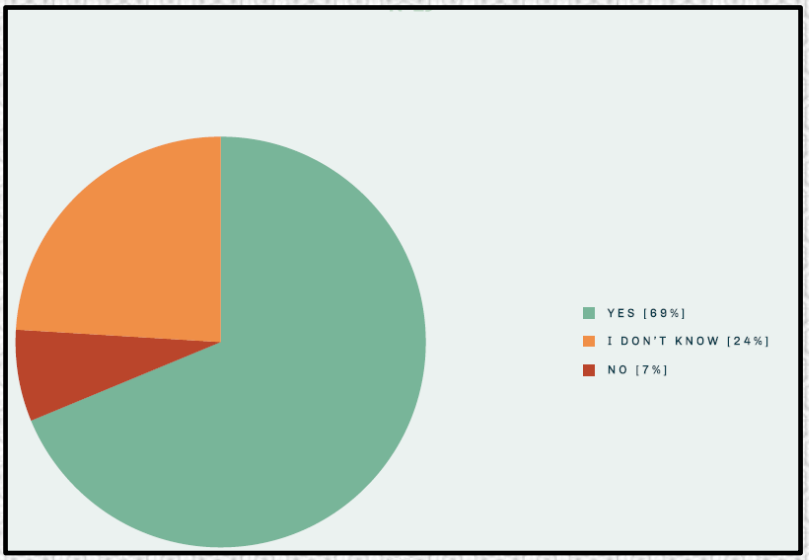
DORA الزام می‌کند که نهادهای مالی با برخورداری از ظرفیت‌های افزونه فناوری اطلاعات و ارتباطات، نیازهای کسب‌وکاری را در حین بروز اختلالات در نظر داشته باشند. این افزونه می‌تواند شامل سامانه‌های پشتیبان، مانند سرورهای اضافی یا زیرساخت‌های مبتنی بر ابر باشد تا بتواند در صورت از کار افتادن سامانه‌های اصلی به‌سرعت جایگزین آن بشود. مطالعه مذکور داده‌هایی را در خصوص دفعات پشتیبان‌گیری، بازگردانی و آزمون بازیابی برای شرکت‌های بیمه گردآوری کرده است.

تعداد آزمون برنامه‌های بازیابی می‌تواند بسته به نوع سازمان و حیاتی‌بودن سامانه‌های مورد آزمون متفاوت باشد؛ با این‌حال، عموماً توصیه می‌شود برنامه‌های بازیابی به‌طور منظم، حداقل یک‌بار در سال یا هر زمان که تغییرات قابل توجهی در زیرساخت، اپلیکیشن‌ها یا فرآیندهای کسب‌وکاری ایجاد می‌شود، آزمون شوند. اغلب شرکت‌های نظرسنجی شده، برنامه‌های بازیابی خود را به‌صورت سالانه آزمایش می‌کنند. تعداد کمی از شرکت‌ها آزمایش‌ها را با دفعات بیشتر و تنها اقلیتی از شرکت‌ها آزمایش را کمتر از دفعات الزامی سالانه انجام می‌دهند.



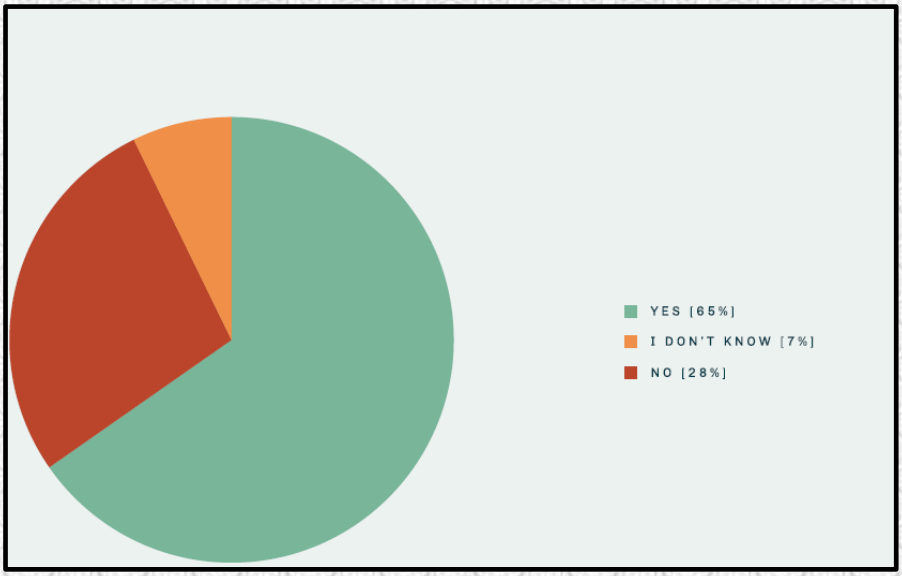
شکل شماره ۱۵- دفعات پشتیبان‌گیری، بازگردانی، و بازیابی رویه آزمون برای شرکت‌های بیمه‌ای

برای واحد حسابرسی داخلی سودمند است به جای آن که صرفاً اسناد آزمون را طی بازبینی‌های دفتری مرور نماید، در آزمون‌های بازیابی پس از حادثه مشارکت داشته و تمرین‌های واقعی را مشاهده کند. بر اساس مطالعات صورت‌گرفته، ۶۹٪ از شرکت‌ها بازیابی برنامک‌ها و سامانه‌ها را به‌عنوان بخشی از آزمون برنامه بازیابی پس از حادثه آزمایش می‌کنند.



شکل شماره ۱۶- شرکت‌هایی که بازیابی اپلیکیشن‌ها را بعنوان بخشی از برنامه بازیابی فاجعه آزمون می‌کنند.

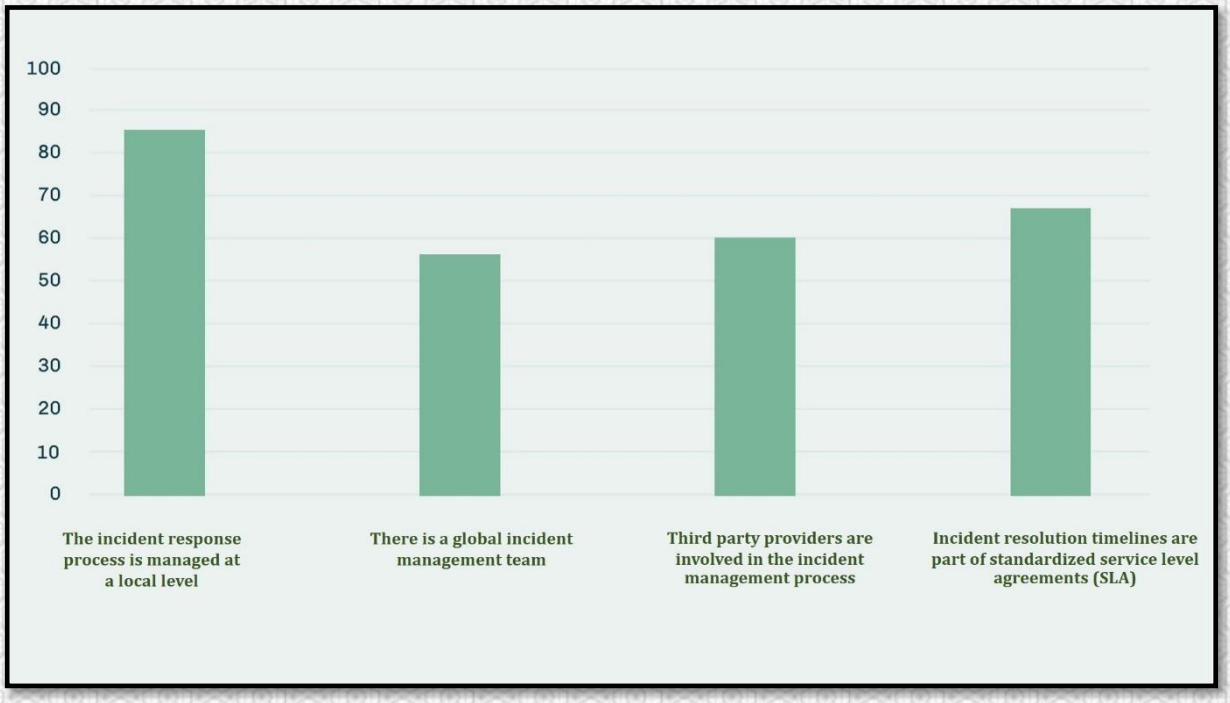
در طی حسابرسی‌های داخلی، حسابرسان برنامه‌های واکنش و بازیابی فناوری اطلاعات و ارتباطات را که شامل برنامه‌های تداوم کسب‌وکار فاوا و برنامه‌های واکنش و بازیابی فاوا هستند، بررسی می‌کنند. ۶۵٪ از شرکت‌ها رعایت کامل این الزامات را گزارش کرده‌اند.



شکل شماره ۱۷- پاسخ‌های فاوا و موضوع برنامه‌های بازیابی به بازبینی‌های حسابرسی داخلی مستقل، شامل برنامه تداوم کسب و کار و پاسخ فاوا و برنامه‌های بازیابی در ارتباط با سامانه‌های فاوا پشتیبان تمامی کارکردها

۸،۵،۱. پاسخ‌گویی به رخداد

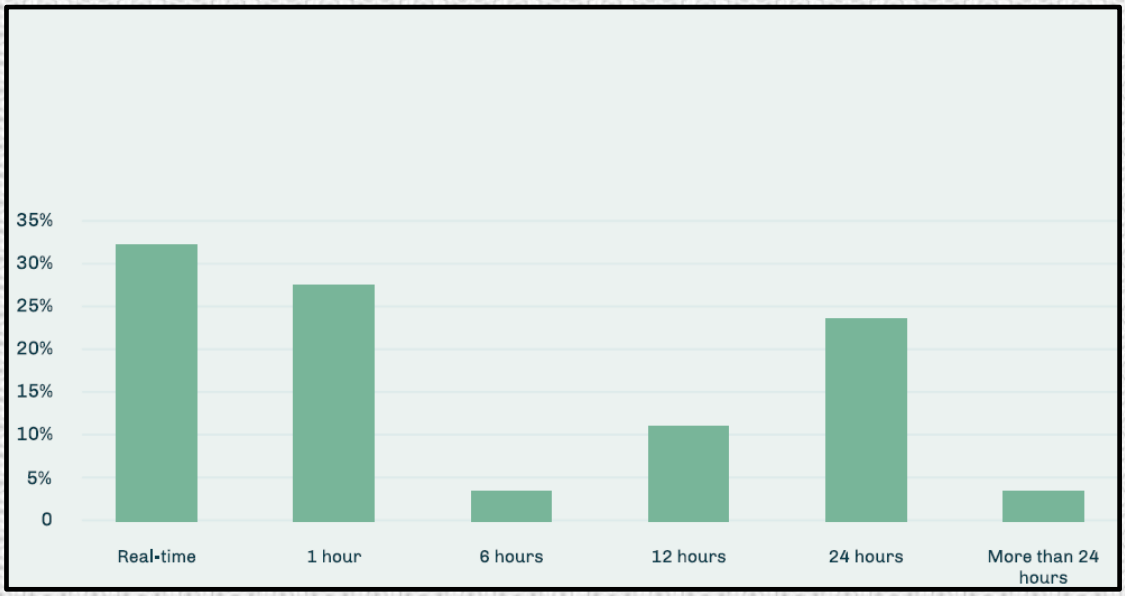
شرکت‌ها برای سامان‌دهی مدیریت رخداد و پاسخ‌گویی به آن، رویکردهای متفاوتی به‌کار می‌گیرند؛ اکثریت شرکت‌ها بر یک فرآیند محلی اتکا می‌کنند و شرکت‌های بزرگ‌تر از یک تیم جهانی شامل ارائه‌دهندگان شخص ثالث برخوردارند. حسابرسان داخلی باید آزمون‌های خود را مطابق با رویکرد سازمانی تعریف کنند. در هر حال، مهم است که گزارش‌دهی در درون سازمان یا به نهادهای ناظر، توسط نهاد مالی به‌صورت اثربخش مدیریت شود.



شکل شماره ۱۸- فرآیند پاسخ به رخداد استاندارد شده شرکت‌های بیمه

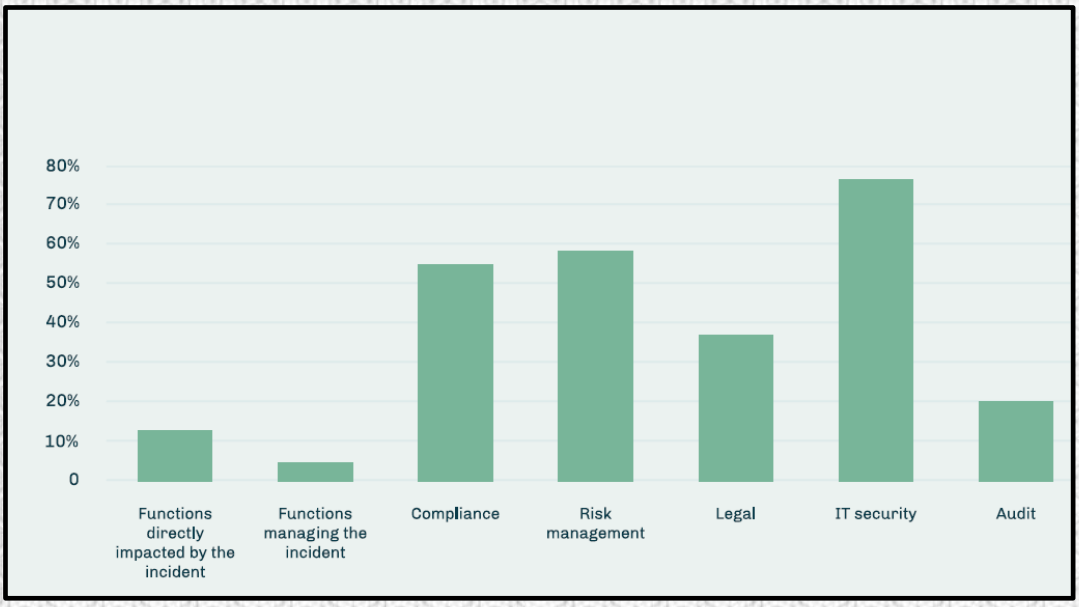
۸،۵،۲ اطلاع‌رسانی به نهاد ناظر

بهترین رویه، شناسایی آنی مسائل فاوا است؛ تنها تعداد کمی از شرکت‌ها در نظرسنجی اظهار کرده‌اند که بیش از ۲۴ ساعت برای شناسایی به زمان نیاز دارند. در مجموع، نتایج این برداشت را ایجاد می‌کند که بسیاری از شرکت‌ها برای دستیابی به الزامات DORA در خصوص ایجاد اعلان اولیه در۴ ساعت، نیاز به سرمایه‌گذاری دارند.



شکل شماره ۱۹- مواردی که شرکت‌های بیمه براساس ماده ۱۰ بعنوان شناسایی سریع مشکلات فناوری اطلاعات در نظر می‌گیرند.

امنیت فناوری اطلاعات و مدیریت ریسک معمولاً نقش‌های دخیل در اطلاع‌رسانی رخداد هستند. بر اساس نتایج مطالعه، حسابرسی داخلی تنها در تعداد اندکی از شرکت‌ها مشارکت داده شده است.



شکل شماره ۲۰- کارکردهای درگیر درفرآیند هشدار رخداد فاوا در شرکت‌های بیمه

۸،۵،۳. حسابرسی‌های فناوری اطلاعات و ارتباطات (فاوا)

مقررات DORA پیامدهای خاصی در ارتباط با فناوری اطلاعات و ارتباطات برای حسابرسی داخلی و رویکرد حسابرسی دارد. حسابرسی داخلی باید آزمون‌های مشخصی را برای الزامات مرتبط با DORA در برنامه حسابرسی خود بگنجاند. حسابرسان فناوری اطلاعات باید برای آزمون الزامات فاوا مندرج در DORA که شامل تعریف الزامات کلیدی امنیت فناوری اطلاعات هستند، از دانش و تخصص لازم برخوردار باشند. این الزامات همه جنبه‌های امنیت فناوری اطلاعات را از مدیریت دارایی‌های فناوری اطلاعات تا رمزگذاری، کنترل‌های رمزنگاری، مدیریت آسیب‌پذیری و وصله، امنیت داده و سامانه، امنیت شبکه، مدیریت پروژه و تغییرات مرتبط با فاوا، خط‌مشی منابع انسانی و کنترل دسترسی، شناسایی و پاسخ‌گویی به رخدادهای مرتبط با فاوا و مدیریت تداوم کسب‌وکار فاوا را پوشش می‌دهند (برای جزئیات به RTS چارچوب مدیریت ریسک مراجعه شود).

امکان آزمون همه این کنترل‌ها در یک مأموریت حسابرسی، حتی برای سازمان‌های بزرگ موجود نمی‌باشد؛ به همین دلیل بسیار توصیه می‌شود که حسابرسی داخلی این کنترل‌ها را بر مبنای رویکرد مبتنی بر ریسک و در چارچوب یک برنامه حسابرسی چند ساله آزمون کند. از آنجا که بسیاری از مفاهیم DORA از پیش برقرار هستند، خطوط اول، دوم و سوم دفاعی در سازمان‌های بزرگ اکثرا از استانداردها و خط‌مشی‌های موجود برای مدیریت الزامات مقرراتی استفاده می‌کنند. غالباً نگاشت خط‌مشی‌ها و الزامات مقرراتی به استانداردهای موجود می‌تواند از ارزیابی ریسک، تعریف کنترل‌ها و رویکرد و پوشش حسابرسی پشتیبانی کند. در هر حال، ضروری است که اصول و الزامات مشخص DORA به‌صورت شفاف ابلاغ، مستندسازی و آزمون شوند.

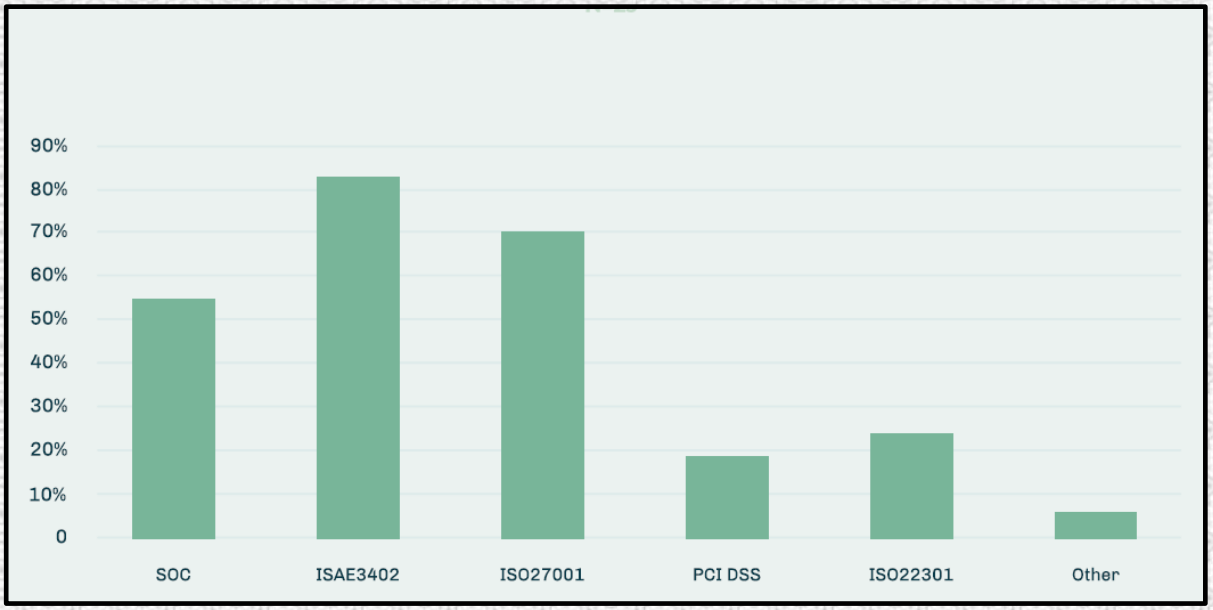
استانداردهای خاص اطمینان‌بخشی اشخاص ثالث می‌توانند نسبت به اطمینان‌بخشی شخص ثالث از چنین آزمونگر مستقلی پشتیبانی کنند. این نوع الزامات اطمینان‌بخشی می‌تواند در توافق‌نامه قراردادی گنجانده شود (حق حسابرسی، الزامات برای گزارش حسابرسی مستقل عمومی یا اختصاصی ـ مطابق استانداردهای ISAE 3402، SOC1 و SOC2). با این حال، چنین استانداردهایی ماهیت عمومی دارند و الزامات خاص DORA را در نظر نمی‌گیرند:

- SOC 2: مجموعه‌ای از رهنمودها برای ارائه‌دهندگان خدمات که داده‌های مشتری را ذخیره می‌کنند. این استاندارد توسط انجمن حسابداران رسمی آمریکا[۷۸] ایجاد شده و چگونگی مدیریت داده‌های مشتری بر اساس پنج "اصل خدمات اعتماد" ـ امنیت، دسترس‌پذیری، یکپارچگی پردازش، محرمانگی و حریم خصوصی ـ را تبیین می‌کند.

[۷۸] American Institute of Certified Public Accountants (AICPA)

- ISAE 3402: یک استاندارد بین‌المللی اطمینان‌بخشی که تعاملات کنترل سازمان خدماتی[۷۹] را تعریف می‌کند و به مشتریان سازمان خدماتی این اطمینان را می‌دهد که سازمان خدماتی دارای کنترل‌های داخلی مناسب است. ISAE 3402 توسط هیئت تدوین استانداردهای حسابرسی و اطمینان‌بخشی بین‌المللی[۸۰] صادر و در سال ۲۰۰۹ توسط فدراسیون بین‌المللی حسابداران[۸۱] منتشر شد. این استاندارد جایگزین SAS 70 شده و تمرکز بیشتری بر پایش و ارزیابی ارزیابی مستمر کنترل‌ها دارد.
- PCI DSS: استاندارد امنیت داده صنعت کارت و پرداخت[۸۲]، مجموعه‌ای از استانداردهای امنیتی است که برای اطمینان از حفظ یک محیط امن توسط تمامی شرکت‌هایی که اطلاعات کارت اعتباری را می‌پذیرند، پردازش می‌کنند، ذخیره و یا منتقل می‌کنند، طراحی شده است.
- ISO 27001: استاندارد بین‌المللی برای سامانه‌های مدیریت امنیت اطلاعات[۸۳] است. این استاندارد چارچوبی برای ایجاد، اجرا، نگهداری و بهبود مستمر یک سامانه مدیریت امنیت اطلاعات فراهم می‌کند.
- استاندارد تاب‌آوری ISO 22316:2017، امنیت و تاب‌آوری: این استاندارد راهنمایی برای ارتقای تاب‌آوری سازمانی برای هر نوع یا اندازه سازمان ارائه می‌دهد و مختص هیچ حوزه و یا صنعتی نیست.

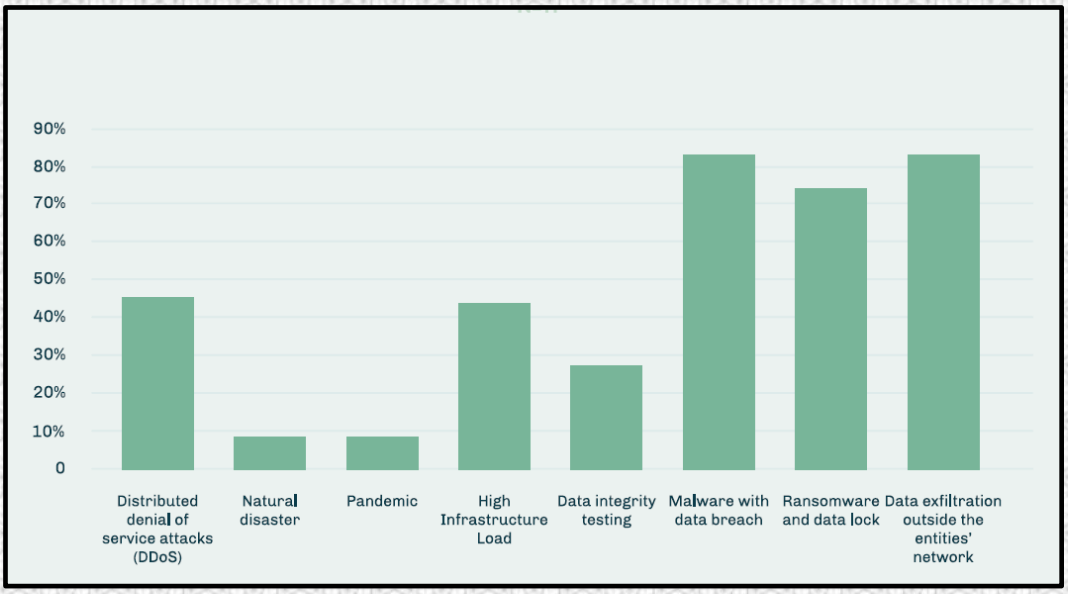
طبق اظهارات پاسخ‌دهندگان نظرسنجی، شرکت‌ها هنگام ارزیابی ریسک طرف سوم، هم به خود استانداردها و هم به گواهینامه‌هایی که اعتبار آن استانداردها را تضمین می‌کنند، اتکا می‌کنند.



شکل شماره ۲۱- گواهینامه‌هایی که شرکت‌ها در حین انجام ارزیابی ریسک شخص ثالث به آن اتکا دارند.

اغلب منطقی است که برخی سناریوها به‌صورت دوره‌ای آزمون شوند تا اطمینان حاصل شود محیط کنترلی در برابر انواع مختلف اختلالات و/ یا حملات احتمالی مقاوم است. حسابرسان داخلی باید سناریوهای معمول، ریسک‌های مرتبط و مزایا/ معایب سناریوهای آزمون را درک کنند. مطالعه نشان داد که سناریوهای سایبری بیشترین دفعات آزمون را دارند، در حالی که سناریوهای مرتبط با زیرساخت، مانند بلایای طبیعی و ریسک‌های فیزیکی، کمتر آزمون می‌شوند.

[۷۹] Service Organization Control (SOC)
[۸۰] International Auditing and Assurance Standards Board (IAASB)
[۸۱] International Federation of Accountants (IFAC)
[۸۲] The Payment Card Industry Data Security Standard
[۸۳] Information Security Management Systems (ISMS)



شکل شماره ۲۲- سناریوهای شرکت‌های بیمه در حین آزمون نفوذ تهدید محور

در زیر فهرستی از برخی عناصر کلیدی برای حملات شبیه‌سازی‌شده آورده شده است.

انواع حمله:

- حملات باج‌افزاری: در این سناریو، یک هکر وارد سیستم می‌شود و کاربران را از دسترسی محروم می‌کند و برای بازگرداندن دسترسی، درخواست باج می‌کند.
- حملات فیشینگ: هدف از آزمون این سناریو، درک چگونگی ارسال ایمیلی ظاهراً بی‌ضرر توسط هکر به یک کارمند است که شامل پیوند یا پیوست مخرب برای سرقت داده‌های حساس یا نصب بدافزار می‌باشد.
- آلودگی با بدافزار: این سناریو شامل نفوذ یک نرم‌افزار مخرب به شبکه سازمان است که می‌تواند منجر به سرقت داده‌ها، آسیب به سامانه یا پیامدهای زیان‌بار دیگر شود.
- حمله DDoS[۸۴]: سناریوی حمله بدافزار امتناع توزیع شده ارائه خدمت، شامل اشباع شبکه، سرویس یا سرور با ترافیک است تا برای کاربران موردنظر غیرقابل دسترسی شود.
- استفاده از آسیب‌پذیری روز صفر[۸۵]: آسیب‌پذیری در نرم‌افزار یا سخت‌افزار که معمولاً برای فروشنده ناشناخته است و هیچ وصله یا اصلاحی برای آن موجود نیست.
- حمله ضعف احراز هویت چندعاملی[۸۶] (همچنین شناخته شده به عنوان بمباران MFA یا هرزنگاری MFA): مهاجم مجموعه‌ای از تلاش‌های ورود را به امید آنکه کاربر حداقل یک بار روی دکمه «قبول» کلیک کند، به او ارسال می‌کند.

مبدأ حمله:

- تهدید داخلی: این سناریو شامل کارمند یا فرد داخلی دیگری است که به‌طور مخرب یا غیرعمد باعث نقض امنیت می‌شود.
- تهدید مکرر پیشرفته: اصطلاح گسترده‌ای است برای توصیف کارزاری که در آن مهاجمان با حضور بلندمدت در شبکه داده‌های بسیار حساس را استخراج می‌کنند. این مهاجمان اغلب باتجربه هستند و ممکن است به صورت دولتی تأمین مالی شوند.

[۸۴] Distributed Denial of Service
[۸۵] Zero Day Exploit
[۸۶] Multi-factor Authentication Fatigue

اهداف حمله:

- حمله زنجیره تأمین: در این سناریو، هکر یک فروشنده یا تأمین‌کننده مورد اعتماد را به‌خطر می‌اندازد تا به سیستم شما دسترسی پیدا کند.
- نقض امنیت ابری: این سناریو شامل دسترسی غیرمجاز یا دستکاری داده‌های ذخیره‌شده در ابر است.
- حمله به برنامه وب: این سناریو شامل بهره‌برداری مهاجم از یک آسیب‌پذیری در برنامه وب برای دسترسی غیرمجاز یا مختل کردن سرویس است.
- حمله به دستگاه‌های تلفن همراه: در این سناریو، یک دستگاه تلفن همراه مانند تلفن هوشمند یا تبلت اغلب از طریق برنامه‌های مخرب یا فیشینگ، به‌خطر می‌افتد تا به داده‌ها یا سامانه‌های حساس دسترسی پیدا شود.

پیامدهای حمله:

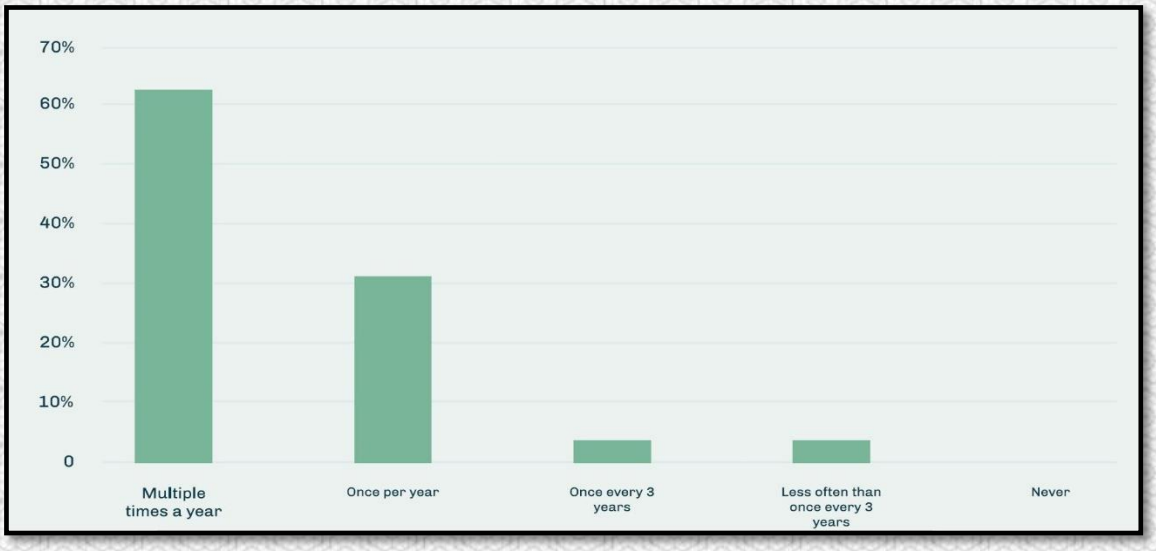
- حداکثر رویداد محتمل: یک حمله همه داده‌ها از جمله داده‌های پشتیبان را حذف یا رمزگذاری می‌کند تا شرکت قادر به ادامه فعالیت نباشد؛ تنها راه‌حل فعلی برای چنین رویدادی، ایجاد نسخه ایزوله‌ای از داده‌ها در محیط تولید[۸۷] است.
- نقض داده‌ها: این سناریو شامل دسترسی غیرمجاز به داده‌های حساس مانند اطلاعات مشتری، داده‌های مالی یا مالکیت فکری است.

۸,۵,۴. آزمون نفوذ

۸,۵,۴,۱. آزمون نفوذ تهدید محور (TLPT)

ماده ۲۶ الزام انجام آزمون پیشرفته ابزارها، سامانه‌ها و فرآیندهای فناوری اطلاعات و ارتباطات را بر اساس آزمون‌های نفوذ تهدید محور مقرر می‌نماید. این آزمون‌ها حملات سایبری شبیه‌سازی‌شده‌ای هستند که بر اساس تهدیدهای جاری انجام می‌شوند تا آسیب‌پذیری‌های امنیتی را شناسایی کنند و حداقل عملکردها و خدمات حیاتی نهاد مالی را پوشش دهند و بر روی سامانه‌های واقعی تولید که از آن‌ها پشتیبانی می‌کنند، اجرا شوند. نهادهای مالی محدوده TLPT را بر اساس ارزیابی کارکردها و خدمات حیاتی، با شناسایی فرآیندها، سامانه‌ها و فناوری‌های مرتبط فاوا، از جمله کارکردها و خدمات برون‌سپاری‌شده یا قراردادشده با ارائه‌دهندگان خدمات فاوا شخص ثالث، تعیین می‌کنند. بر اساس مطالعه، شرکت‌ها معمولاً حداقل یک آزمون در سال انجام می‌دهند، که اغلب توسط خط اول یا دوم دفاعی هدایت می‌شود و به‌ندرت توسط واحد حسابرسی داخلی اجرا می‌شود.

[۸۷] Cybervaulting

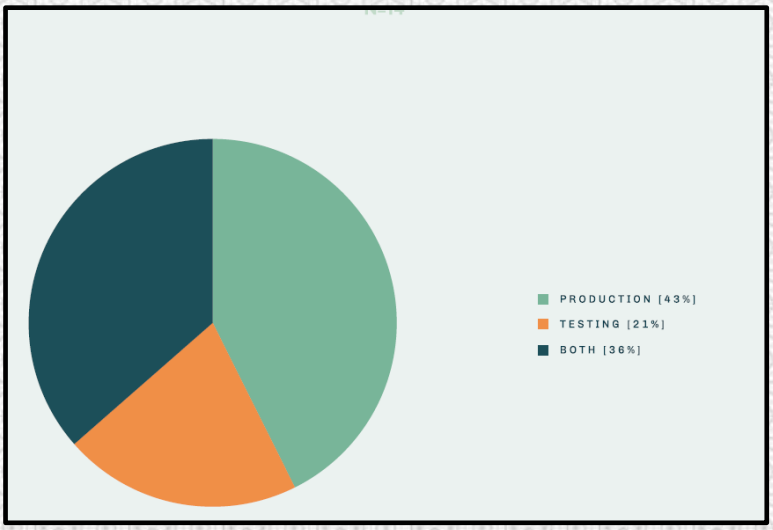


شکل شماره ۲۳- دفعات آزمون نفوذ شرکت‌های بیمه

۸،۵،۴،۲. آزمون TLPT در محیط‌های تولید یا تست

اگر آزمون‌های نفوذ در محیط توسعه انجام شوند، لازم است تا حد امکان با محیط عملیاتی مطابقت داشته باشند تا اطمینان حاصل شود که آزمون قابل اعتماد و آموزنده است. آزمون‌های نفوذ انجام‌شده در محیط‌های تولید می‌توانند انواع مشکلات و شدت تأثیر آن‌ها را در زمان واقعی شناسایی کنند. بنابراین، این امکان فراهم می‌شود که هرگونه شکاف امنیتی به‌موقع اصلاح شود، اما برای جلوگیری از اختلال در کسب‌وکار، نیازمند هماهنگی با کارکردهای کلیدی درگیر است.

بر اساس نتایج مطالعه، اکثر شرکت‌ها آزمون‌ها را در محیط تولید انجام می‌دهند، اما آزمون در محیط‌های تست یا استفاده از رویکردهای ترکیبی نیز نسبتاً رایج است.

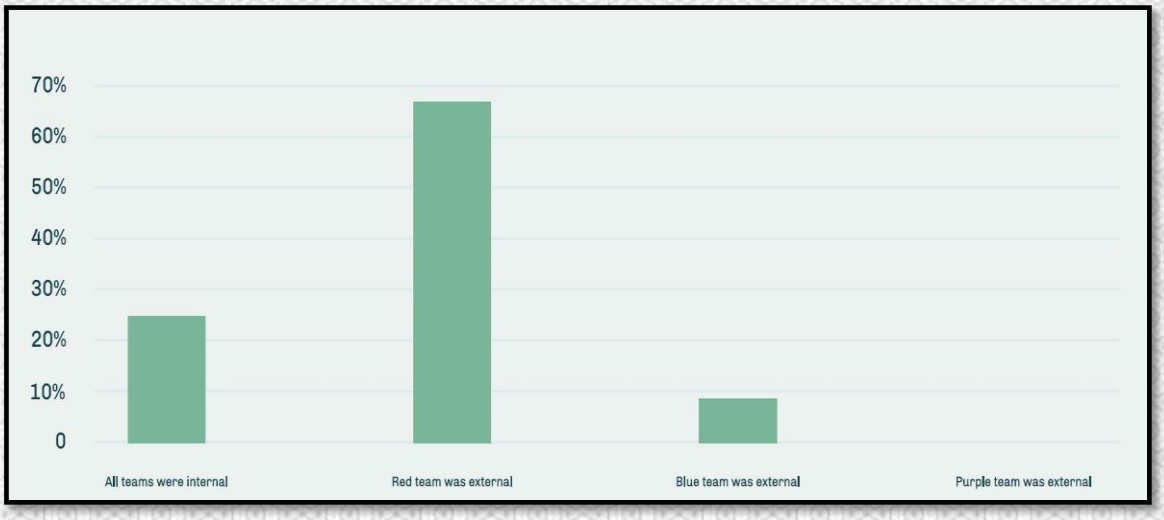


شکل شماره ۲۴- محیط‌هایی که آزمون TLPT به وسیله شرکت‌های بیمه در آنها انجام شده است

ماده ۲۶ DORA الزام دارد که آزمون نفوذ تهدید محور حداقل هر سه سال یک‌بار انجام شود و دست‌کم هر سه آزمون باید توسط تیم موسوم به تیم قرمز[۸۸]، تیم نفوذ خارجی که نقش مهاجم خارجی را شبیه‌سازی می‌کند، و بر اساس اصل تناسب اجرا شود. بر اساس تجربه در صنعت، ترکیبی از تیم‌های داخلی و خارجی بیشترین کارآیی را دارد. همان‌طور که پیش‌تر اشاره شد، این

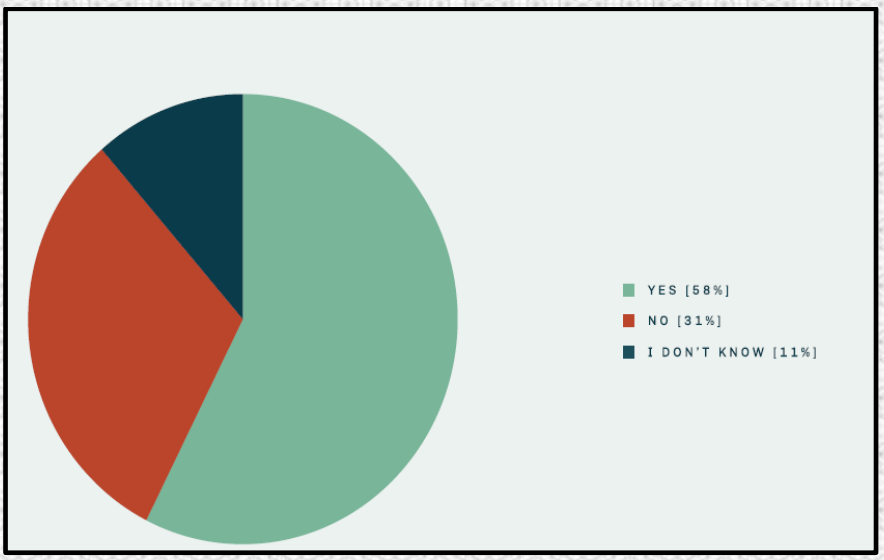
[۸۸] Red Team

آزمون‌ها معمولاً به‌صورت منظم توسط خطوط اول یا دوم دفاعی مدیریت می‌شوند، در حالی که حسابرسی داخلی ممکن است کیفیت این آزمون‌ها و کنترل‌های مربوطه را به‌صورت مستقل ارزیابی کند. مؤسسات اعتباری که طبق ماده ۶ مقررات (EU) شماره 1024/2013 در رده مؤسسات مهم طبقه‌بندی شده‌اند، مطابق با DORA (ماده ۲۷) صرفاً باید از آزمونگران خارجی استفاده کنند.



شکل شماره ۲۵- راه اندازی تیم در طول آزمون TLPT

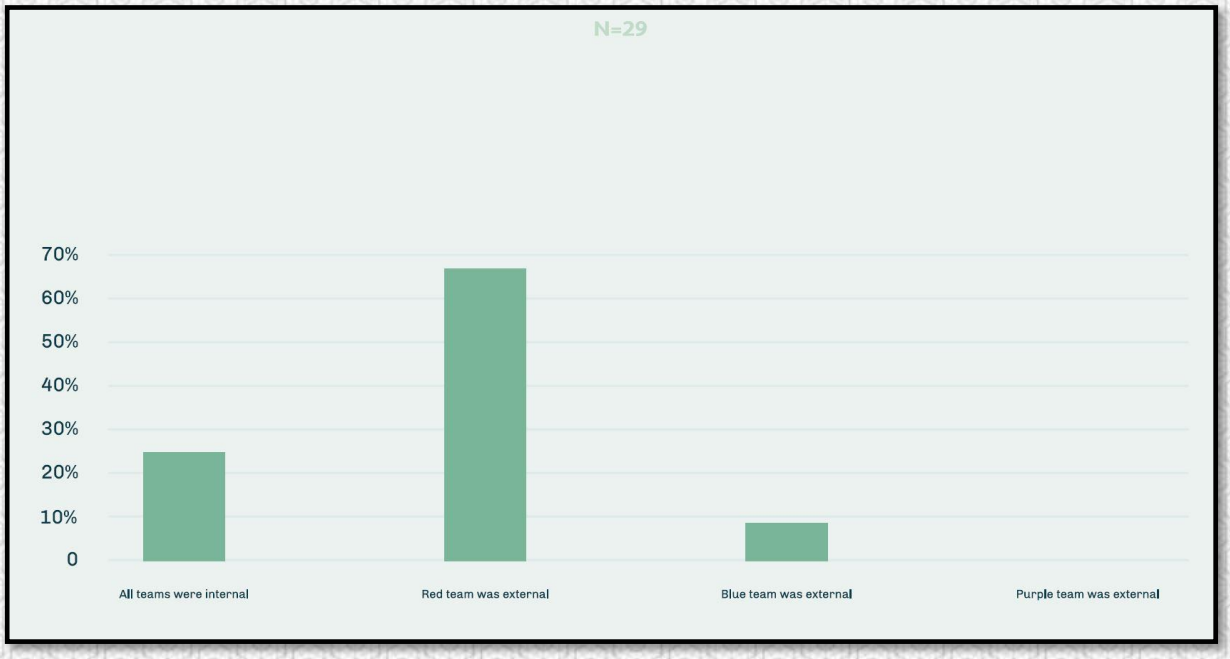
نظرسنجی تأیید می‌کند که اکثریت شرکت‌ها طرفین خارجی را در فعالیت‌های آزمون نفوذ خود درگیر می‌کنند.



شکل شماره ۲۶- شرکت‌هایی که اشخاص ثالث را در آزمون TLPT شان درنظر می‌گیرند.

اکثر شرکت‌های مورد بررسی به‌طور رسمی شکاف‌های امنیت سایبری خود را مدیریت می‌کنند، اما هیچ‌یک بودجه مشخصی برای رفع این شکاف‌ها تخصیص نمی‌دهند. با این حال، تنها حدود ۴۰٪ از شرکت‌ها اصلاح آن‌ها را به‌عنوان یک فرآیند کسب‌وکاری روزمره[۸۹] در نظر می‌گیرند؛ این بدان معنا است که حدود ۶۰٪ از شرکت‌ها بودجه مشخصی برای این شکاف‌ها ندارند و همچنین آن‌ها را در فرآیند کسب‌وکاری روزمره خود لحاظ نمی‌کنند، که ممکن است نشان‌دهنده عدم تخصیص بودجه برای این کمبودها باشد.

[۸۹] Business as Usual (BAU)



شکل شماره ۲۷- چگونگی برخورد شرکت‌های بیمه با شکاف‌های شناسایی شده در طول آزمون نفوذ

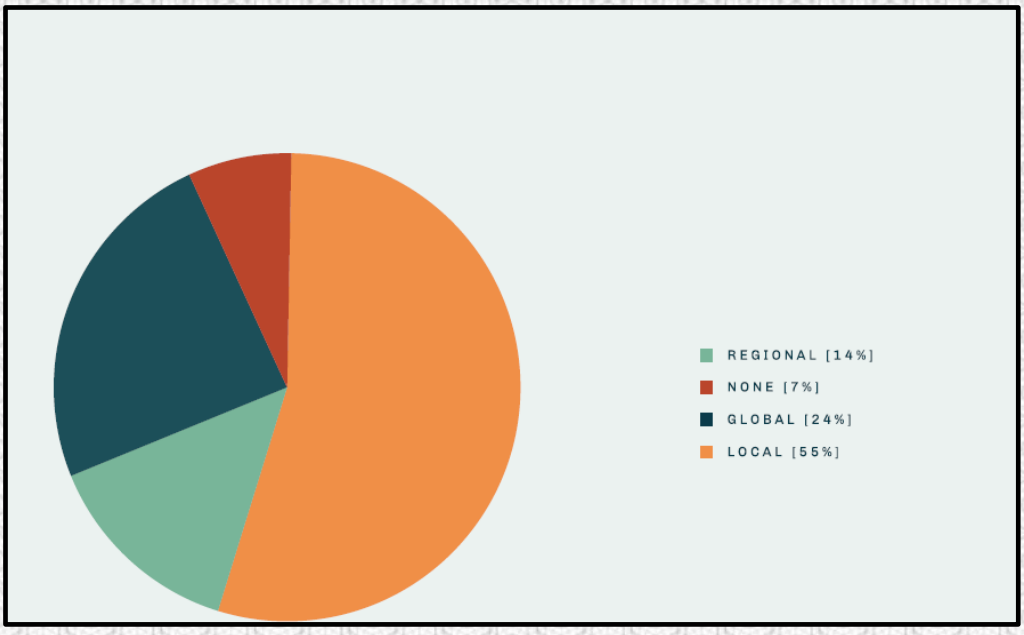
۸،۵،۵. مدیریت ریسک برون‌سپاری

۸،۵،۵،۱. حسابرسی‌های شخص ثالث

DORA الزامات بسیار مشخصی درباره ریسک شخص ثالث در فناوری اطلاعات و ارتباطات دارد و الزام می‌کند که کنترل‌ها در طول کل چرخه مدیریت شخص ثالث اعمال شوند (ماده ۲۸). به‌ویژه، به‌عنوان بخشی از مسئولیت خط سوم، حسابرسی داخلی باید حاکمیت کلی، مسئولیت مدیریت فاوا شخص ثالث و گزارش‌دهی مربوطه را آزمون کند. مؤسسات مالی موظف‌اند حداقل سالی یک‌بار درباره تعداد برنامه‌های جدید در استفاده از خدمات فاوا به مراجع ذی‌صلاح گزارش دهند (ماده ۲۷ RTS چارچوب مدیریت ریسک فاوا، قالب و محتوای گزارش بررسی چارچوب مدیریت ریسک فاوا را مشخص می‌کند که باید به ناظر ارائه شود)، و همچنین مدیریت برنامه‌های قراردادها از جمله استراتژی خروج برای خدمات فاوا که از عملکردهای حیاتی یا مهم پشتیبانی می‌کنند را ارزیابی کنند.

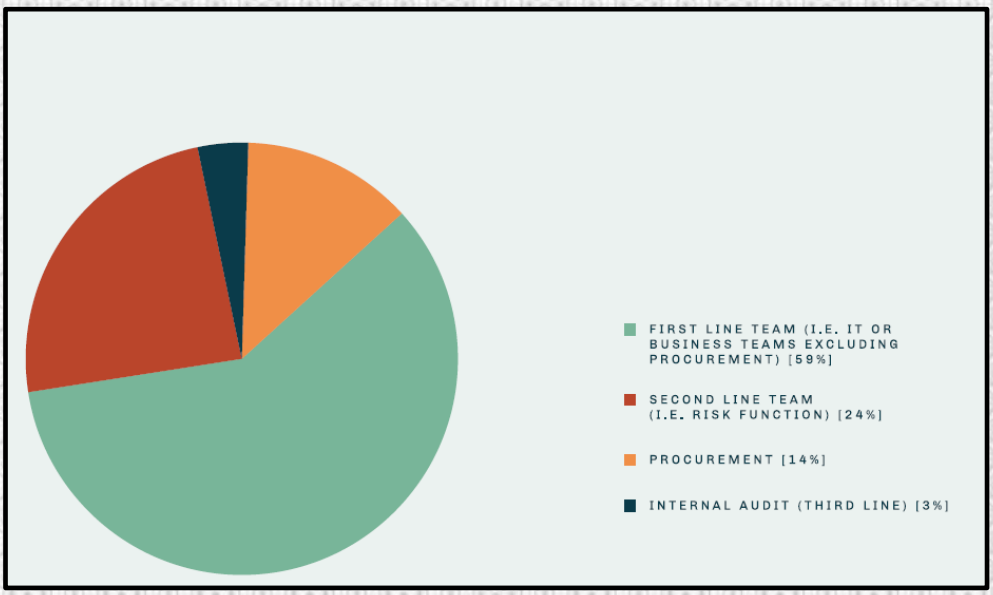
یکی از اهداف اصلی DORA، ارزیابی و نظارت بر ریسک‌هایی است که از همکاری با اشخاص ثالث ناشی می‌شود. چارچوب RTS برای مدیریت ریسک فاوا، قوانین و استانداردهایی را تعریف می‌کند که مؤسسات مالی باید هنگام تکیه بر ارائه‌دهندگان خدمات فاوا اشخاص ثالث[۹۰] رعایت کنند. این چارچوب دستورالعمل‌ها و الزامات لازم را برای مؤسسات مالی هنگام قرارداد با ارائه‌دهندگان خدمات فاوا شخاص ثالث مشخص می‌کند. اکثر شرکت‌ها (۵۵٪) مدل نظارت محلی برای شخص ثالث دارند، در حالی که ۳۸٪ از آنها از مدل نظارت جهانی یا محلی استفاده می‌کنند.

[۹۰] third-party service providers



شکل شماره ۲۸- مدل نظارتی استفاده شده برای تامین‌کنندگان شخص ثالث

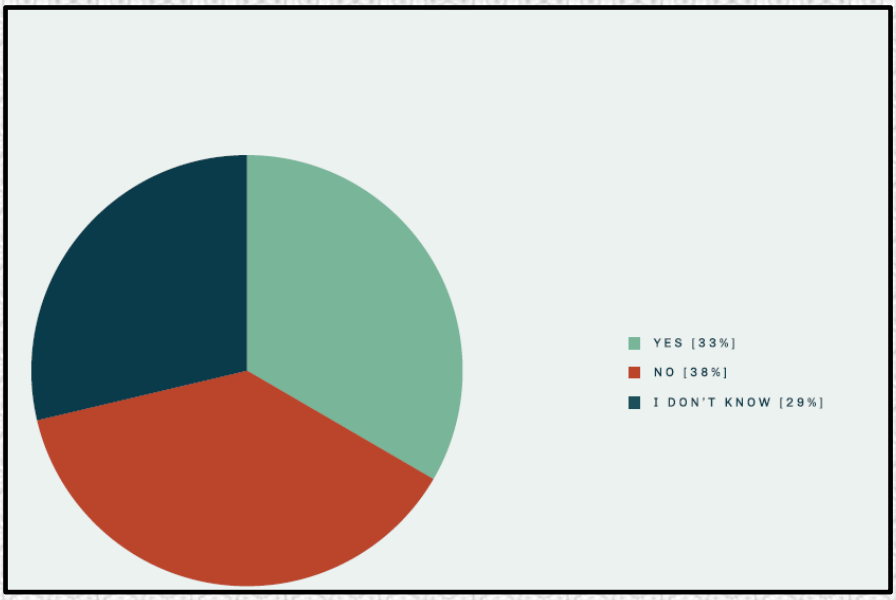
بر اساس نتایج نظرسنجی، اکثریت شرکت‌ها اصل خط اول را برای مسئولیت ارزیابی ریسک شخص ثالث اعمال می‌کنند، در حالی که این مسئولیت به عملکرد مدیریت ریسک خط دوم تخصیص داده نمی‌شود.



شکل شماره ۲۹- افرادی که در شرکت‌های بیمه مسئول اجرای ارزیابی ریسک شخص ثالث هستند.

نتیجه دیگر این پرسشنامه نشان می‌دهد که مدیریت اشخاص ثالث باید بیش‌تر تقویت شود. تنها یک‌چهارم پاسخ‌دهندگان اعلام کرده‌اند که راهبرد چندین تأمین‌کننده[۹۱] فاوا که در ماده ۶ بند ۹ DORA شرح داده شده و الزامی است، در شرکت آن‌ها برقرار شده است. راهبرد چندتأمین‌کننده فاوا برای شناسایی وابستگی‌های کلیدی به ارائه‌دهندگان خدمات فاوا شخص ثالث و برای تبیین منطق ترکیب تأمین[۹۲]، مورد نیاز است.

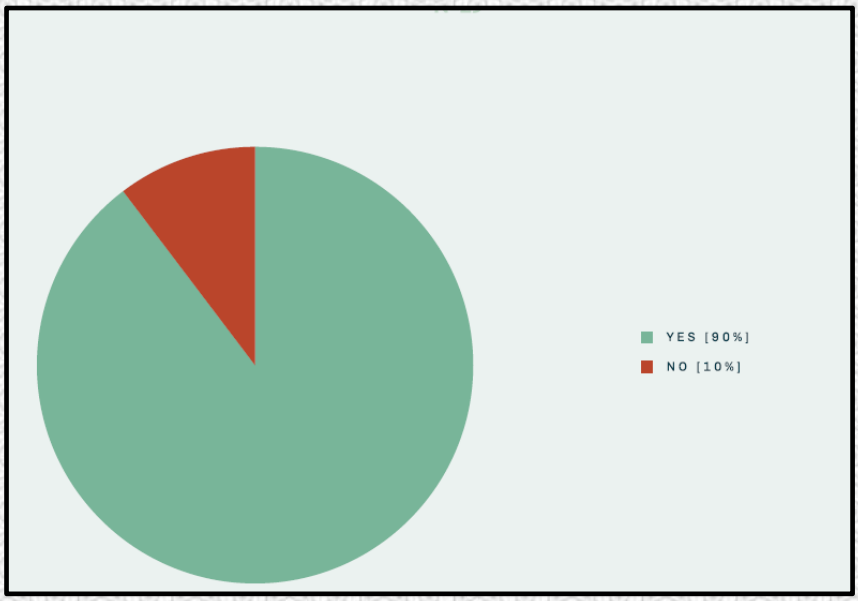
[۹۱] multi-vendor strategy
[۹۲] procurement mix



شکل شماره ۳۰- شرکت‌های بیمه‌ای که یک استراتژی چند تامین‌کننده‌ای ایجاد کرده‌اند.

۸,۵,۵,۲. استانداردها برای حسابرسی شخص ثالث و حق حسابرسی

پیام مثبت در این زمینه این است که اکثریت قاطع (۹۰٪) شرکت‌کنندگان در نظرسنجی، حقوق حسابرسی را در قراردادهای شخص ثالث خود تعریف کرده‌اند، که امکان اجرای حسابرسی بر روی ارائه‌دهنده را فراهم می‌آورد. چنین حسابرسی‌هایی می‌توانند توسط یک آزمونگر مستقل انجام شوند.

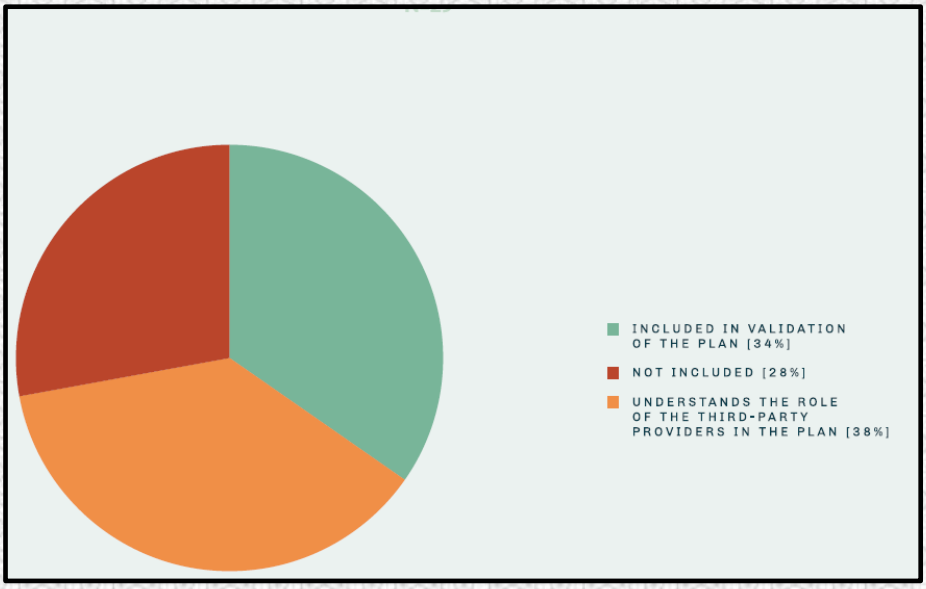


شکل شماره ۳۱- شرکت‌های بیمه که در قراردادهای شخص ثالث خود حقوق حسابرسی را لحاظ کرده‌اند.

۸,۵,۵,۳. مدیریت رخداد و شخص ثالث

به‌عنوان نمونه‌ای از ضرورت بالای حسابرسی شخص ثالث، این پرسش مطرح شد که تا چه حد ارائه‌دهندگان خدمات شخص ثالث در اعتبارسنجی طرح‌های پاسخ به رخداد دخیل هستند. نتایج نشان داد که تنها ۳۴٪ پیمانکاران را در اعتبارسنجی طرح‌های پاسخ به رخداد لحاظ کرده‌اند، در حالی که ۳۸٪ با نقش ارائه‌دهندگان خدمات شخص ثالث در این طرح‌ها آشنایی

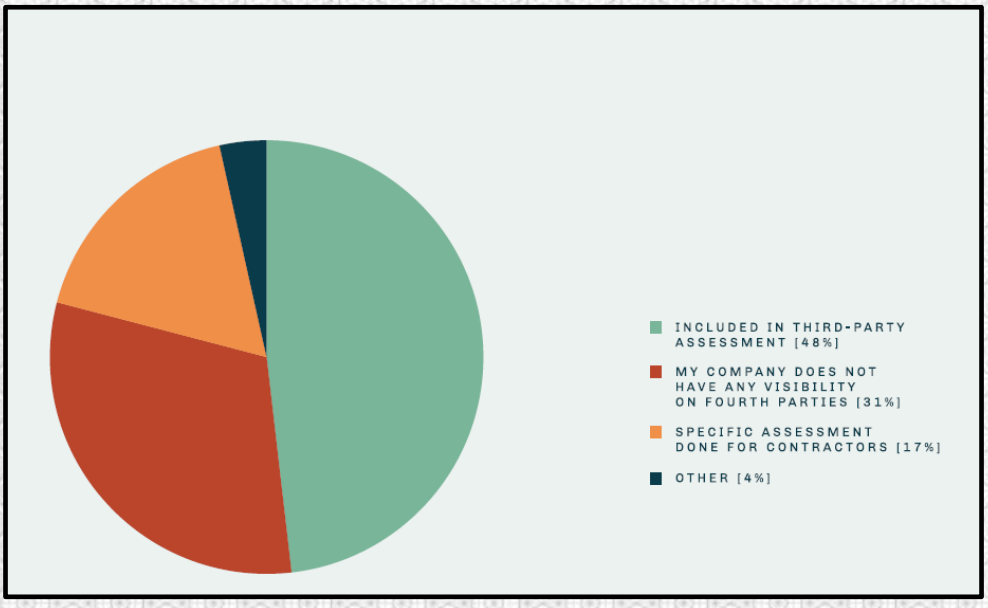
داشته و آن را ارزیابی کرده‌اند. حدود ۲۸٪ از شرکت‌ها پیمانکاران را در طرح‌های پاسخ به رخداد خود لحاظ نکرده‌اند، که این امر ریسک قابل توجهی ایجاد می‌کند و باید در طول ماموریت‌های حسابرسی ارزیابی شود.



شکل شماره ۳۲- شرکت‌های بیمه‌ای که در تایید برنامه(های) پاسخ به رخداد، اشخاص ثالث را دخیل نموده‌اند.

۸،۵،۵،۴. پیمانکاران فرعی

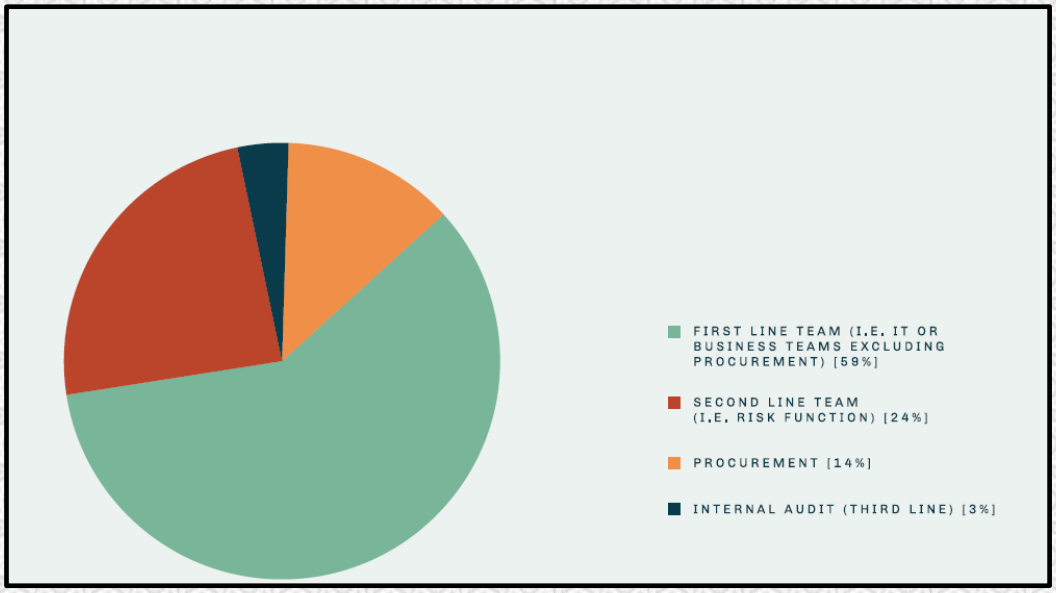
ریسک پیمانکار فرعی اصطلاحی است که برای توصیف خطرات و نقاط ضعف احتمالی ناشی از پیمانکاران فرعی، فروشندگان یا ارائه‌دهندگان خدماتی استفاده می‌شود که با پیمانکاران مستقیم سازمان همکاری می‌کنند. نظرسنجی نشان داد که ریسک پیمانکار فرعی عمدتاً از طریق ارزیابی‌های شخص ثالث پوشش داده می‌شود:



شکل شماره ۳۳- چگونگی رسیدگی شرکت‌های بیمه به پیمانکار فرعی

ماده ۲۸ بند ۶ DORA بیان می‌کند که "*در استفاده از حقوق دسترسی، بازرسی و حسابرسی بر ارائه‌دهنده خدمات فاوا شخص ثالث، نهادهای مالی باید بر اساس رویکرد مبتنی بر ریسک، تناوب حسابرسی‌ها و بازرسی‌ها و همچنین حوزه‌هایی که مورد*

حسابرسی قرار می‌گیرند را پیش از اجرا تعیین کنند و این امور را با پایبندی به استانداردهای حسابرسی پذیرفته‌شده عمومی و مطابق هر دستور نظارتی در خصوص استفاده و ادغام چنین استانداردهایی انجام دهند."



شکل شماره ۳۴- افرادی که در شرکت‌های بیمه مسئول انجام ارزیابی ریسک شخص ثالث هستند.

فناوری اطلاعات و ارتباطات اشخاص ثالث دارای چارچوب نظارتی مخصوص به خود هستند که در DORA تعیین شده است و حقوق بازرسی ناظر اصلی در مواد ۳۹ و ۴۰ مشخص شده‌اند.

ماده ۳۰ DORA تعهدات شخص ثالث را چنین تعریف می‌کند: "*تعهد ارائه‌دهنده خدمات فاوا شخص ثالث به همکاری کامل در طول بازرسی‌ها و حسابرسی‌های حضوری است که توسط مراجع ذی‌صلاح، ناظر اصلی، نهاد مالی یا شخص ثالث منصوب‌شده انجام می‌شوند؛ و نیز تعهد به ارائه جزئیات در خصوص دامنه، رویه‌های قابل پیروی و تناوب چنین بازرسی‌ها و حسابرسی‌هایی است*".

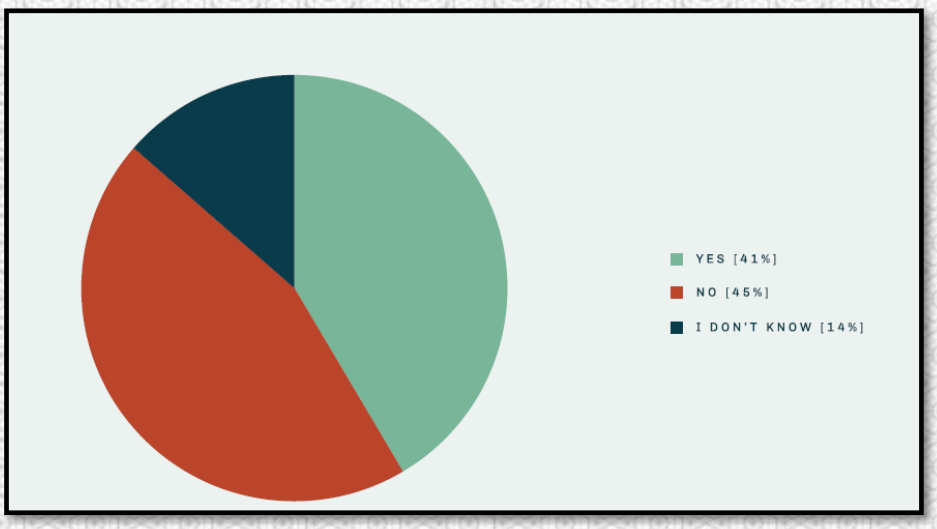
اکثر شرکت‌هایی که در نظرسنجی شرکت کردند، پاسخ دادند که حسابرسی شخص ثالث توسط واحد حسابرسی داخلی انجام می‌شود. با این حال، منطقی است که خطوط اول و دوم نیز بر اساس مسئولیت‌های خود، ارزیابی‌های مربوط به شخص ثالث را انجام دهند تا از صحت چارچوب کنترلی ارائه‌دهنده خدمات فاوا شخص ثالث اطمینان حاصل شده و صرفاً به خط سوم تکیه نشود.

شکل شماره ۳۵- افرادی که حسابرسی شخص ثالث را در شرکت‌های بیمه انجام می‌دهند.

۸،۵،۵،۵. حسابرسی‌های اشتراکی (تجمیعی) برای اشخاص ثالث

DORA بر اهمیت حسابرسی پیمانکاران تأکید می‌کند و به گزینه استفاده از منابع حسابرسی تجمیعی برای دستیابی به این هدف مشترک اشاره می‌کند.

تجربه استفاده از حسابرسی‌های تجمیعی متفاوت است و به نظر می‌رسد که تعداد شرکت‌هایی که پیش‌تر تجربه‌ای در این زمینه داشته با آن‌هایی که این روش برایشان کاملاً جدید است، تقریبا برابر باشند. اکثریت شرکت‌هایی که در این زمینه تجربه کسب کرده‌اند، از بخش بانکی هستند که به نظر می‌رسد این موضوع از مدت‌ها قبل در میان آن‌ها مطرح شده باشد.



شکل شماره ۳۶- شرکت‌های بیمه‌ای که حسابرسی تجمیعی را با تامین کنندگان شخص ثالث انجام می‌دهند.

مزیت اصلی استفاده از منابع حسابرسی تجمیعی برای رسیدگی به ریسک‌ها، کمک به توسعه و تثبیت مهارت‌ها و دانش مناسب است. علاوه بر این، این روش فرصتی را برای یادگیری متقابل فراهم می‌کند تا اطمینان حاصل شود که فعالیت‌های حسابرسی به‌طور مؤثر برای ارزیابی و نظارت بر ارائه‌دهندگان خدمات انجام می‌شود. همچنین این کار منابع انسانی لازم را برای ارزیابی محیط پیچیده و غیرمعمول و همچنین بررسی جامع تعداد کنترل‌هایی که ارائه‌دهندگان خدمات فناوری اطلاعات ایجاد کرده‌اند، فراهم می‌کند.

یکی دیگر از مزایای رویکرد تجمیعی این است که قدرت بیشتری در برابر پیمانکاران بزرگ ایجاد می‌کند و این امکان را میسر می‌سازد که تعداد قابل توجهی از مشتریان به شکلی مؤثر از حقوق خود برخوردار شوند. همچنین، این رویکرد برای ارائه‌دهندگان شخص ثالث هم‌افزایی ایجاد می‌کند؛ چرا که دیگر نیازی ندارند برای مشتریان اختصاصی خود حسابرسی‌های بسیاری را مدیریت و هماهنگ سازند؛ بلکه می‌توانند یک یا تعداد کمتری حسابرسی تجمیعی را به‌صورت مناسب و مؤثر انجام دهند.

با اینکه این ایده یا رویکرد کاملاً جدید نیست، اما اکنون توسط قوانین اروپایی مورد استقبال قرار گرفته و مقرر شده است. گروهی از مؤسسات مالی، گروه همکاری حسابرسی ابری (CCAG)[۹۳] را برای صنعت خدمات مالی در اتحادیه اروپا تشکیل دادند. این گروه انجمنی برای عضویت مؤسسات مالی ایجاد کردند که تمرکز اصلی آن‌ها بر ارائه‌دهندگان خدمات ابری است و در حال حاضر بر سه ارائه‌دهنده بزرگ (Microsoft، Amazon وGoogle) تمرکز دارند، اما آماده‌اند دامنه ارزیابی خود را بر اساس نیازهای اعضا گسترش دهند.

[۹۳] Collaborative Cloud Audit Group (CCAG)

چشم‌انداز CCAG چنین است: "*حمایت از بخش‌های حسابرسی داخلی اعضای گروه CCAG، در تطابق با مقررات اتحادیه اروپا برای صنعت مالی با استفاده از روش‌شناسی حسابرسی مشترک مشارکتی، به منظور ایجاد اطمینان مستقل و عینی نسبت به خدمات ابری. انجمن CCAG رویکردی بهینه و مقیاس‌پذیر با سهمی منصفانه برای اعضای خود فراهم می‌کند.*"

علاوه بر چشم‌انداز و استراتژی عمومی گروه، یک چارچوب حسابرسی مستحکم شامل روش‌شناسی روشن و توضیحات فرآیندها نیز همراه آن ارائه شده است. این سازمان غیرانتفاعی، یک مدیریت مرکزی شامل یک پلتفرم فناوری اطلاعات مشترک، همکاری ساختاری میان اعضای CCAG و ایجاد تیم‌های اصلی برای هر ارائه‌دهنده خدمات ابری فراهم می‌کند.

مرور دقیق بند ۶ ماده ۲ DORA، برای بررسی اینکه آیا یک طرح ابتکاری مانند CCAG، نیازمندی‌های DORA نسبت به پیمانکاران را برآورده می‌کند یا خیر، مفید است: "*در استفاده از حقوق دسترسی، بازرسی و حسابرسی بر ارائه‌دهنده خدمات فناوری اطلاعات و ارتباطات شخص ثالث، مؤسسات مالی باید بر اساس رویکرد مبتنی بر ریسک، پیشاپیش دفعات حسابرسی و بازرسی و حوزه‌های مورد حسابرسی را تعیین نموده و از استانداردهای حسابرسی معمول پذیرفته‌شده پیروی کنند. هرگاه توافقات قراردادی با ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات شخص ثالث از نظر فنی پیچیده باشد، مؤسسه مالی باید از مهارت و دانش حسابرسان داخلی، خارجی، و یا گروهی از آنها برای انجام مؤثر حسابرسی و ارزیابی‌های مربوطه اطمینان حاصل کند.*"

برای درک تطابق رویکرد CCAG با این الزامات، باید روشن شود که فرآیند حسابرسی گروه CCAG در پنج مرحله ذیل انجام می‌شود:

۱. پیش‌آمادگی
۲. آماده‌سازی حسابرسی
۳. مشاهدات میدانی
۴. گزارش‌دهی نتایج
۵. درس‌آموخته‌ها

به‌طور مشخص، مرحله اول، پیشاپیش نیازمندی ناظران برای رویکرد مبتنی بر ریسک و تعیین دفعات حسابرسی را پوشش می‌دهد. در این مرحله، این گروه تعیین می‌کند که کدام اعضا بر اساس ارزیابی ریسک و نیازهای حسابرسی خود در یک حسابرسی برنامه‌ریزی‌شده شرکت می‌کنند. به این ترتیب، هر عضو امکان پیروی از رویکرد مبتنی بر ریسک خود را دارد. در مرحله پیش‌آمادگی، مشخص می‌شود که تیم حسابرسی چگونه به نظر می‌رسد و کدام حسابرسان و با چه مهارت‌هایی در این فعالیت حسابرسی شرکت می‌کنند. بنابراین، هر مؤسسه می‌تواند قبل از آغاز مرحله آماده‌سازی حسابرسی، ارزیابی کند که آیا مهارت و دانش لازم برای انجام مؤثر حسابرسی وجود دارد و در صورت نیاز اقدام متقابل انجام دهد. اما از آنجا که هر مؤسسه مالی شرکت‌کننده حداقل یک حسابرس فراهم می‌آورد، بسیار بعید است که منابع مورد نیاز از نظر کیفیت یا کمیت فراهم نشود.

سه مرحله بعدی مطابق با استانداردهای حسابرسی معمول انجام می‌شوند، زیرا اعضا عموماً از استانداردهای جهانی حسابرسی پیروی می‌کنند و بنابراین این مراحل با آن الزامات هماهنگ هستند. مرحله پنجم و آخر با عنوان درس‌آموخته‌ها و به منظور بهره‌گیری از تجارب حسابرسی و بهبود رویکرد آتی انجام می‌شود.

یک مخاطب تیزبین ممکن است متوجه شود که مرحله پیگیری در فرآیند حسابرسی CCAG وجود ندارد. این مسئله به دلیل آن است که گروه مذکور نتایج کلیدی را خلاصه می‌کند، اما گزارش حسابرسی اختصاصی، توسط هر مؤسسه مالی به‌صورت جداگانه صادر می‌شود. بنابراین، فرآیند پیگیری نیز توسط هر مؤسسه مالی به‌صورت مستقل انجام می‌شود.

این رویکرد تجمیعی حسابرسی اشتراکی که در زمینه ارائه‌دهندگان خدمات ابری آزمایش شده است، می‌تواند به‌عنوان یک نمونه عملی خوب برای اجرای الزامات DORA در عمل در نظر گرفته شود.

۸,۵,۶. برنامه حسابرسی DORA

هدف از بیان مطالب ذیل ارائه یک راهنمای کامل حسابرسی برای مقررات DORA نیست. بلکه تمرکز آن بر استخراج کنترل‌های کلیدی حسابرسی است تا فرآیند بازبینی بر اساس ماهیت خاص هر نهاد حسابرسی‌شونده طراحی شود. با در نظر گرفتن ویژگی‌های منحصربه‌فرد این نهادها، حسابرسان می‌توانند عامل انطباق را به‌طور مؤثر ارزیابی کنند و زمینه‌های بهبود را شناسایی نمایند.

۸,۵,۷. حاکمیت و سازماندهی

حوزه	الزامات DORA	موارد پیشنهادی برای بررسی
حاکمیت و سازماندهی	عمومی	• ابتدا، تیم حسابرسی باید ارزیابی کند که آیا سازمان، تحلیل شکاف را برای شناسایی الزامات بالقوه DORA که اجرا نشده‌اند یا سطح اجرای آن‌ها کافی نیست، تکمیل کرده است. خروجی این تحلیل شکاف باید برنامه اقدام جامع برای رسیدگی به کنترل‌هایی باشد که به‌طور کامل برآورده نشده‌اند. تیم حسابرسی باید تأیید کند که آیا این تحلیل انجام شده و وضعیت برنامه‌های اقدام مرتبط چگونه است. • اصل تناسب باید اندازه سازمان و پروفایل کلی ریسک آن، و همچنین ماهیت، مقیاس و پیچیدگی خدمات، فعالیت‌ها و عملیات را در نظر بگیرد. بنابراین، تیم حسابرسی باید بررسی کند که این اصل چگونه در سازمان تعریف و اجرا شده است. این امر بقیه تلاش‌ها را برای اطمینان از رعایت DORA تعیین می‌کند. • با در نظر گرفتن اصل تناسب، گام بعدی شناسایی کارکردهای حیاتی یا مهم سازمان است. حسابرس باید کامل بودن و کفایت فرآیندی را که برای تعیین این کارکردها دنبال می‌شود، ارزیابی کند.

۸,۵,۸. مدیریت ریسک فناوری اطلاعات و ارتباطات (فاوا)

حوزه	الزامات DORA	موارد پیشنهادی برای بررسی
مدیریت ریسک فناوری اطلاعات و ارتباطات (فاوا)	نهادهای مالی باید تمام دارایی‌های اطلاعاتی و دارایی‌های فاوا، از جمله دارایی‌های سایت‌های دور، منابع شبکه و تجهیزات سخت‌افزاری را شناسایی کنند و آن‌هایی را که حیاتی تلقی می‌شوند، نگاشت کنند. آن‌ها باید پیکربندی دارایی‌های اطلاعاتی و فاوا و پیوندها و وابستگی‌های متقابل بین دارایی‌های اطلاعاتی و فاوا مختلف را نگاشت کنند.	به این منظور، تیم حسابرسی باید ارزیابی کند که نهاد مربوطه چگونه موجودی دارایی‌های فاوا را مدیریت می‌کند. به عنوان مثال، برای ساده‌سازی این تلاش، برخی شرکت‌ها ممکن است از نرم‌افزار پایگاه داده مدیریت پیکربندی استفاده کنند.
مدیریت ریسک فاوا	نهادهای مالی باید تمام فرآیندهایی را که به ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث وابسته هستند، شناسایی و مستند کنند و اتصالات داخلی با ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث را که خدماتی ارائه می‌دهند و از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند، شناسایی کنند.	تیم حسابرسی داخلی باید فهرست ارائه‌دهندگان خدماتی را که هر یک از کارکردهای حیاتی یا مهم را پشتیبانی می‌کنند، درخواست کند و میزان کامل بودن و دقت آن را ارزیابی کند.
مدیریت ریسک فاوا	چارچوب مدیریت ریسک فاوا باید حداقل شامل استراتژی‌ها، سیاست‌نامه‌ها، رویه‌ها، پروتکل‌های فاوا و ابزارهایی باشد که برای حفاظت از تمام دارایی‌های اطلاعاتی وفاوا (نرم‌افزار کامپیوتری، سخت‌افزار، سرورها، اجزای فیزیکی و غیره) لازم است. همچنین، این چارچوب باید مستند شده و حداقل سالی یک بار یا به صورت دوره‌ای در مورد بنگاه‌های کوچک، و همچنین پس از وقوع حوادث عمده مرتبط با فاوا بازبینی شود.	تیم حسابرسی داخلی باید چارچوب مدیریت ریسک فاوا را به‌طور منظم مطابق با برنامه حسابرسی نهادهای مالی بازبینی کند.

حوزه	الزامات DORA	موارد پیشنهادی برای بررسی
مدیریت ریسک فاوا	نهادهای مالی باید از جداسازی و استقلال مناسب کارکردهای مدیریت ریسک فاوا، عملکردهای کنترل و حسابرسی داخلی را طبق مدل سه خط دفاعی، یا مدل مدیریت و کنترل ریسک داخلی، اطمینان حاصل کنند.	حسابرسی داخلی باید در تمام تعاملات حسابرسی خود تضمین کند که استقلال مورد نیاز تمامی کارکردها تأمین شده است؛ حسابرسی داخلی باید مستقل باشد.
مدیریت ریسک فاوا	چارچوب مدیریت ریسک فاوا باید استراتژی جامع چندفروشندگی فاوا را در سطح گروه یا نهاد تعریف کند که وابستگی‌های کلیدی به ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث را نشان داده و منطق پشت ترکیب خرید ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث را توضیح دهد.	حسابرسی داخلی باید استراتژی چندفروشندگی فاوا را بازبینی کند.
مدیریت ریسک فاوا	نهادهای مالی باید سیاست‌نامه‌ها، رویه‌ها، پروتکل‌ها و ابزارهای امنیتی فاوا را طراحی، تهیه و اجرا کنند که هدف آن‌ها تضمین تاب‌آوری، تداوم و در دسترس بودن سیستم‌های فاوا، به ویژه آن‌هایی که از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند است.	برخی کنترل‌های حداقلی برای حسابرسی عبارتند از: سیاست‌نامه امنیت اطلاعات؛ کنترل‌های دسترسی فیزیکی یا منطقی به دارایی‌های فاوا؛ مکانیسم‌های احراز هویت قوی (برای مثال، احراز هویت چندعاملی)؛ سیاست‌نامه‌ها، رویه‌ها و کنترل‌های مستند برای مدیریت تغییرات فاوا؛ سیاست‌نامه‌های مستند برای وصله‌ها و به‌روزرسانی‌ها.
مدیریت ریسک فاوا	نهادهای مالی باید به عنوان بخشی از چارچوب مدیریت ریسک فاوا، سیاست‌نامه تداوم کسب‌وکار فاوا جامعی شامل تحلیل تأثیر کسب‌وکاری را اجرا کنند. علاوه بر این، نهادها باید برنامه‌های پاسخ و بازیابی فاوا را اجرا کنند.	این مستندات باید توسط تیم حسابرسی داخلی ارزیابی شود و اطمینان حاصل شود که نهاد مورد نظر در صورت اختلال در عملیات کسب‌وکاری، منابع کافی برای تضمین بازیابی کارکردهای حیاتی یا مهم خود تخصیص داده است.
مدیریت ریسک فاوا	نهادهای مالی باید: (۱) برنامه‌های تداوم کسب‌وکار فاوا و برنامه‌های پاسخ و بازیابی فاوا را در رابطه با سیستم‌های فاوا که از تمامی کارکردها پشتیبانی می‌کنند، حداقل سالی یک بار آزمایش کنند، و همچنین در صورت هرگونه تغییرات اساسی در سیستم‌های فاوا که از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند؛ (۲) برنامه‌های ارتباط بحرانی تدوین‌شده را آزمایش کنند.	تیم حسابرسی داخلی باید تمام مستندات آخرین برنامه تداوم کسب‌وکار فاوا و همچنین فرآیندی را که برای آزمایش مجدد در هنگام تغییرات اساسی در سیستم‌های فاوا تعریف شده، درخواست کند. علاوه بر این، برنامه ارتباط بحران شامل هرگونه شواهد پشتیبان از فعال‌سازی برنامه ارتباط، در صورت قابلیت اجرایی بودن باید درخواست و ارزیابی شود.
مدیریت ریسک فاوا	نهادهای مالی باید تابع مدیریت بحران داشته باشند.	حسابرسان باید تأیید کنند که آیا این تابع شامل تعریف مسئولیت‌های مربوطه به‌طور مناسب رسمی‌سازی شده است.
مدیریت ریسک فاوا	واحدهای مالی موظف‌اند در صورت درخواست مقامات ذی‌صلاح، برآوردی از کل هزینه‌ها و زیان‌های سالانه ناشی از حوادث عمده مرتبط با فاوا را به ایشان گزارش دهند.	برای این منظور، حسابرسان داخلی باید رویه‌های دستی و/یا خودکاری را که برای محاسبه و گزارش هزینه‌ها و زیان‌های ناشی از حوادث فاوا تعریف شده‌اند، مورد ارزیابی قرار دهند.
مدیریت ریسک فاوا	واحدهای مالی موظف‌اند موارد زیر را تدوین و مستند نمایند: ۱-سیاست‌ها و رویه‌های پشتیبان‌گیری که بر اساس حیاتی بودن اطلاعات یا سطح محرمانگی داده‌ها، محدوده داده‌های مشمول پشتیبان‌گیری و حداقل دفعات پشتیبان‌گیری را مشخص می‌کند؛ ۲-رویه‌ها و روش‌های بازیابی و بازگردانی داده‌ها؛	این مستندات باید توسط تیم حسابرسی داخلی ارزیابی شود تا اطمینان حاصل شود که پشتیبان‌گیری به‌درستی انجام می‌شود و در صورت نیاز، امکان بازیابی اطلاعات وجود دارد.
مدیریت ریسک فاوا	آزمایش رویه‌های پشتیبان‌گیری و روش‌های بازیابی و بازگردانی داده‌ها باید به صورت دوره‌ای انجام شود.	نتایج آخرین آزمون‌های بازیابی باید در اختیار تیم حسابرسی داخلی قرار داده شود. همچنین باید تأیید گردد که آزمون‌های بازیابی، تمامی دارایی‌های فاوا را که پشتیبان کارکردهای حیاتی یا مهم هستند، پوشش می‌دهند.
مدیریت ریسک فاوا	هنگامی که واحدهای مالی از سامانه‌های خود برای بازیابی داده‌های پشتیبان استفاده می‌کنند، باید از سامانه‌های فاوایی	برای دستیابی به این هدف، حسابرسان داخلی باید بررسی کنند که آیا جداسازی فیزیکی و منطقی بین شبکه‌های

حوزه	الزامات DORA	موارد پیشنهادی برای بررسی
	بهره گیرند که به صورت فیزیکی و منطقی از سیستم فاوای منبع تفکیک شده‌اند. این سیستم‌ها باید به گونه‌ای امن در برابر هرگونه دسترسی غیرمجاز یا تخریب محافظت شوند و در صورت نیاز، امکان بازیابی به‌موقع خدمات را با استفاده از پشتیبان‌های داده و سیستم، فراهم آورند.	عملیاتی (شبکه اصلی در حال کار) و شبکه‌های پشتیبان وجود دارد. همچنین، کنترل‌های دسترسی به شبکه‌های پشتیبان باید تا حد ممکن محدود شود.
مدیریت ریسک فاوا	محل پردازش ثانویه (محل پشتیبان) باید دارای ویژگی‌های زیر باشد: ۱ -در فاصله جغرافیایی مناسبی از محل پردازش اولیه (محل اصلی) قرار گیرد، به‌گونه‌ای که پروفایل ریسک متمایزی داشته و از رویدادی که محل اصلی را تحت تأثیر قرار داده است، متأثر نشود؛ ۲ -قادر باشد تداوم کارکردهای حیاتی یا مهم را دقیقاً مشابه محل اصلی تأمین کند، یا سطحی از خدمات را ارائه دهد که برای انجام عملیات حیاتی نهاد مالی در چارچوب اهداف بازیابی، ضروری است؛ ۳- بلافاصله برای کارکنان نهاد مالی قابل دسترسی باشد تا در صورت از کار افتادن محل پردازش اولیه، تداوم کارکردهای حیاتی یا مهم تضمین گردد.	این سه کنترل باید به عنوان بخشی از برنامه کاری حسابرسی گنجانده شوند تا در دسترس بودن محل پردازش ثانویه (محل پشتیبان) در مواقع اختلال و بروز حادثه تضمین گردد. شایان ذکر است کفایت ظرفیت محل پردازش ثانویه باید به اندازه‌ای باشد که بتوان تمامی سیستم‌هایی را که پشتیبان هر یک از کارکردهای حیاتی یا مهم هستند، به درستی بازیابی کرد.

۸،۵،۹. مدیریت، طبقه‌بندی و گزارش‌دهی حوادث مرتبط با فناوری اطلاعات و ارتباطات

حوزه	الزامات DORA	موارد شاخص جهت بررسی
مدیریت، طبقه‌بندی و گزارش‌دهی رخدادهای مرتبط با فناوری اطلاعات و ارتباطات	نهادهای مالی موظف‌اند فرآیندی برای مدیریت رخدادهای فاوا تعریف، ایجاد و پیاده‌سازی نمایند تا بتوانند حوادث این حوزه را شناسایی، مدیریت نموده و در مورد آنها اطلاع‌رسانی نمایند. این نهادها باید تمامی حوادث مرتبط با فاوا و نیز تهدیدات سایبری مهم را ثبت نمایند. همچنین، باید رویه‌ها و فرآیندهای مناسبی ایجاد شود تا پایش، رسیدگی و پیگیری منسجم و یکپارچه رخدادهای فاوا تضمین گردد و ریشه حوادث شناسایی، مستند و مرتفع شود تا از وقوع مجدد چنین رخدادهایی پیشگیری به عمل آید.	تیم حسابرسی باید فرآیندهایی را که برای شناسایی، مدیریت، اصلاح، اطلاع‌رسانی و کمی‌سازی حوادث مرتبط با خدمات فاوا، شامل تهدیدات سایبری، تعریف شده‌اند بررسی کند.
مدیریت، طبقه‌بندی و گزارش‌دهی رخدادهای مرتبط با فناوری اطلاعات و ارتباطات	[RTS 18.1] نهادهای مالی باید رخدادهای مرتبط با فاوا را طبقه‌بندی کنند و تأثیر آن‌ها را بر اساس معیارهای زیر تعیین کنند: • تعداد و/ یا اهمیت مشتریان یا طرف‌های مالی تحت تأثیر و در صورت لزوم میزان یا تعداد تراکنش‌های تحت تأثیر رخداد مرتبط با فاوا و اینکه آیا این رخداد، تأثیری بر شهرت سازمان داشته است یا خیر. • مدت زمان رخداد مرتبط با فاوا، شامل زمان توقف خدمت. • گستره جغرافیایی نواحی تحت تأثیر این رخدادها، به‌ویژه اگر بیش از دو کشور عضو را تحت تأثیر قرار دهد. • میزان از دست رفتن داده‌هایی که رخداد مرتبط با فاوا به همراه دارد، در ارتباط با دسترس‌پذیری، اصالت، یکپارچگی یا محرمانگی داده‌ها. • میزان حیاتی بودن خدمات تحت تأثیر، شامل تراکنش‌ها و عملیات نهاد مالی. • اثر اقتصادی، به‌ویژه هزینه‌ها و زیان‌های مستقیم و غیرمستقیم این رخدادها، چه به‌صورت مطلق و چه نسبی.	معیارهای تعریف‌شده برای طبقه‌بندی رخدادهای مرتبط با فاوا باید توسط حسابرسان ارزیابی شوند تا هم‌راستایی آن‌ها با الزامات DORA تضمین شود.

حوزه	الزامات DORA	موارد شاخص جهت بررسی
مدیریت، طبقه‌بندی و گزارش‌دهی رخدادهای مرتبط با فناوری اطلاعات و ارتباطات	نهادهای مالی باید تهدیدات سایبری را بر اساس میزان حیاتی بودن خدمات در معرض خطر، شامل تراکنش‌ها و عملیات نهاد مالی، تعداد و/ یا اهمیت مشتریان یا طرف‌های مالی هدف قرار گرفته و گستره جغرافیایی نواحی در معرض خطر، به‌عنوان تهدیدات مهم طبقه‌بندی کنند.	معیارهای تعریف‌شده برای طبقه‌بندی تهدیدات سایبری باید توسط حسابرسان داخلی ارزیابی شوند تا هم‌راستایی با الزامات DORA تضمین شود.
مدیریت، طبقه‌بندی و گزارش‌دهی رخدادهای مرتبط با فناوری اطلاعات و ارتباطات	نهادهای مالی باید رخدادهای عمده مرتبط با فاوا را به مقام ذی‌صلاح مربوطه گزارش دهند و اطلاعات زیر را ارائه کنند: • اطلاع‌رسانی اولیه. • گزارش میانی پس از اطلاع‌رسانی اولیه، به‌محض اینکه وضعیت رخداد اولیه به‌طور قابل‌توجهی تغییر کرده یا رسیدگی به رخداد عمده مرتبط با فاوا که بر اساس اطلاعات جدید در دسترس تغییر یابد؛ در ادامه، در صورت لزوم، هر بار که به‌روزرسانی مرتبط با وضعیت حادثه در دسترس قرار گیرد و همچنین به درخواست خاص مقام ذی‌صلاح، اطلاعیه‌های به‌روز شده ارسال گردد. • گزارش نهایی، زمانی که تحلیل ریشه‌ای حادثه تکمیل شده باشد (صرف نظر از این که اقدامات اصلاحی و کاهش اثر حادثه پیاده‌سازی شده باشند یا نه) و همچنین زمانی که داده‌های واقعی میزان تأثیر حادثه به جای تخمین‌های قبلی قابل ارائه باشد.	تیم حسابرسی داخلی باید فرآیند گزارش‌دهی رخدادهای عمده مرتبط با فاوا به مقامات ذیصلاح مربوطه را مورد بازبینی قرار دهد تا تایید کند که تمامی اطلاعات موردنیاز به‌طور کارآمد و به‌موقع ارائه می‌شوند.

۸،۵،۱۰. آزمون تاب‌آوری عملیاتی دیجیتال

حوزه	الزامات DORA	موارد شاخص جهت بررسی
آزمون تاب‌آوری عملیاتی دیجیتال	DORA "تاب‌آوری عملیاتی دیجیتال" را به عنوان توانایی یک نهاد مالی در ایجاد، تضمین و بازبینی یکپارچگی و قابلیت اتکای عملیاتی خود تعریف می‌کند. که این کار را به‌طور مستقیم یا غیرمستقیم و با استفاده از خدماتی که ارائه‌دهندگان شخص ثالث در حوزه فناوری اطلاعات و ارتباطات فراهم می‌کنند انجام می‌دهد. هدف نهایی، تأمین همه قابلیت‌های مرتبط با فاوا است، به گونه‌ای که امنیت شبکه و سامانه‌های اطلاعاتی مورد استفاده مؤسسه مالی تأمین شود و این سامانه‌ها بتوانند تداوم و کیفیت خدمات مالی را حتی در زمان بروز اختلالات و بحران‌ها حفظ کنند.	برخی از کنترل‌های کلیدی که باید توسط تیم حسابرسی مورد بازبینی قرار بگیرند عبارتند از: • تایید آنکه راهبرد تاب‌آوری عملیاتی دیجیتال مستند، تصویب و ابلاغ شده است. • ارزیابی شود که آیا دامنه راهبرد تاب‌آوری عملیاتی دیجیتال حداقل عناصر زیر را پوشش داده است: • سطح تحمل ریسک برای ریسک فاوا. • اهداف امنیتی. • راهبرد ارتباطی در صورت وقوع رخدادهای مرتبط با فاوا. • طرح تداوم کسب‌وکار (BCP). • تحلیل تاثیر بر کسب‌وکار (BIA). • ظرفیت سایت پردازش ثانویه (پشتیبان) و برنامه‌های آزمون آن. • چارچوب مدیریت ریسک فاوا. • مدیریت پشتیبان‌گیری و قابلیت‌های بازیابی داده. • مدیریت رخدادهای مرتبط با فاوا و تهدیدات سایبری. • مدیریت ریسک تامین‌کنندگان. • سایر تلاش‌های آزمون تاب‌آوری عملیاتی مانند آزمون‌های نفوذ، تمرین‌های تیم قرمز، مدیریت آسیب‌پذیری‌ها و غیره.

۸,۵,۱۱. ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات توسط شخص ثالث

حوزه	الزامات DORA	موارد پیشنهادی برای بررسی
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	مدیریت ریسک ناشی از ارائه‌دهندگان شخص ثالث در حوزه فاوای نهادهای مالی باید بر اساس اصل تناسب پیاده‌سازی شود و موارد زیر را مورد توجه قرار دهد: (۱) ماهیت، مقیاس، پیچیدگی و اهمیت وابستگی‌های مرتبط با فاوا، (۲) ریسک‌های ناشی از توافقات قراردادی که در خصوص استفاده از خدمات فاوا با پیمانکاران منعقد شده است؛ با در نظر گرفتن حیاتی یا مهم بودن خدمات، فرآیند یا کارکرد مربوطه، و تأثیر بالقوه بر تداوم و در دسترس بودن خدمات و فعالیت‌های مالی، چه در سطح فردی چه در سطح گروهی.	تیم حسابرسی باید ارزیابی کند که آیا این الزامات در سازمان اجرا و رسمی‌سازی شده‌اند.
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	واحدهای مالی موظفند به عنوان بخشی از چارچوب مدیریت ریسک فناوری اطلاعات و ارتباطات خود، یک دفتر ثبت اطلاعات را نگهداری و آن را به‌روز نمایند. این دفتر شامل تمام توافقات ثبت شده در قراردادهای منعقد شده با پیمانکاران حوزه فاوا است. این کار باید در سه سطح انجام شود: سطح واحد (خود شرکت مالی)، سطح زیرتلفیقی(هر یک از زیرمجموعه‌ها یا بخش‌های گروه به صورت مجزا) و سطح تلفیقی(کل گروه مالی به صورت یکپارچه و جمع‌شده). قراردادها باید به درستی مستند شوند و در آنها مشخص گردد که کدام قراردادها از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند و کدام یک چنین نقشی ندارند.	حسابرسان باید فهرست تمامی خدمات ارائه‌شده توسط اشخاص ثالث را، هم در سطح هر زیرمجموعه به صورت مجزا و هم در سطح کل گروه به صورت یکپارچه، درخواست کرده و صحت و کامل بودن آن را بررسی کنند.
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	نهادهای مالی موظف‌اند حداقل سالی یک بار به مقامات ذی‌صلاح گزارش دهند که این گزارش در مورد تعداد توافقات جدید برای استفاده از خدمات فاوا، دسته‌بندی ارائه‌دهندگان شخص ثالث در این حوزه، نوع توافقات قراردادی و خدمات فاوا و کارکردهایی است که توسط آنها ارائه می‌شود.	فرآیند گزارش‌دهی دوره‌ای به مقامات ذی‌صلاح باید محدوده بازبینی احتمالی حسابرسی گنجانده شود.
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	پیش از انعقاد هرگونه قرارداد در زمینه استفاده از خدمات فاوا، نهادهای مالی موظف‌اند اقدامات زیر را انجام دهند: ۱- ارزیابی کنند که آیا توافقات مندرج در قرارداد، استفاده از خدمات فاوایی را که از کارکردهای حیاتی یا مهم پشتیبانی می‌کنند مورد پوشش قرار می‌دهد یا خیر؛ ۲- بررسی کنند که آیا الزامات نظارتی مربوط به انعقاد قرارداد رعایت شده است یا خیر؛ ۳- تمامی ریسک‌های مرتبط با توافقات مندرج در قرارداد را شناسایی و ارزیابی کنند، از جمله این احتمال که چنین قراردادی ممکن است باعث شود تشدید ریسک تمرکز یا وابستگی بیش از حد به یک ارائه‌دهنده خاص در حوزه فاوا گردد. ۴-کلیه بررسی‌های دقیق و همه‌جانبه را در مورد ارائه‌دهندگان بالقوه خدمات فاوای شخص ثالث انجام دهند و در سراسر فرآیند انتخاب و ارزیابی، اطمینان حاصل کنند که پیمانکار مذکور مناسب و واجد شرایط است؛ ۵- هرگونه تضاد منافع احتمالی ناشی از توافقات مندرج در قرارداد را شناسایی و ارزیابی کنند. نهادهای مالی تنها مجاز به انعقاد قرارداد با آن دسته از پیمانکاران حوزه فاوا هستند که با استانداردهای مناسب امنیت اطلاعات مطابقت داشته باشند.	به‌عنوان بخشی از فرایند مناقصه (فراخوان و انتخاب تأمین‌کننده)، تیم حسابرسی باید بررسی کند که آیا الزامات پیش‌گفته مقرره DORA در این فرایند لحاظ می‌شوند یا خیر؛ در غیر این صورت، فرایند مذکور باید تقویت گردد.
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	در هنگام اعمال حقوق دسترسی، بازرسی و حسابرسی بر روی ارائه‌دهنده خدمات شخص ثالث فاوا، نهادهای مالی باید بر اساس رویکرد مبتنی بر ریسک، و از پیش تعداد دفعات حسابرسی و بازرسی و همچنین حوزه‌هایی که باید حسابرسی شوند را با پایبندی به استانداردهای معمول حسابرسی و مطابق با دستورالعمل‌های نظارتی درباره نحوه اعمال این استانداردها، تعیین کنند. در مواردی که توافقات قراردادی منعقدشده با پیمانکاران در حوزه خدمات فاوا، دارای پیچیدگی فنی بالایی باشد، نهاد مالی باید تأیید کند که حسابرسان، چه داخلی چه خارجی، یا	برای رعایت این الزام، تیم حسابرسی باید حداقل چک کند که کدام تیم مسئول حسابرسی و بازرسی از ارائه‌دهنده خدمات فاوا است، همچنین روش کار، محدوده و تناوب (بازه‌های زمانی) آن را نیز بررسی کند.

حوزه	الزامات DORA	موارد پیشنهادی برای بررسی
	گروهی از آنها، دارای مهارت و دانش مناسب برای انجام مؤثر حسابرسی و ارزیابی‌های مربوطه هستند.	
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	نهادهای مالی موظف‌اند اطمینان حاصل کنند که قراردادهای مربوط به استفاده از خدمات فاوا در هر یک از شرایط زیر قابل فسخ باشد: ۱- نقض عمده قوانین، مقررات یا شرایط قرارداد توسط پیمانکار فاوا؛ ۲-شرایطی که در فرآیند نظارت بر ریسک ارائه‌دهنده شخص ثالث فاوا شناسایی می‌شود و به گونه‌ای است که می‌تواند کارآیی خدمات مندرج در توافقات قرارداد را تغییر دهد. از جمله تغییرات اساسی که بر توافقات مندرج در قرارداد یا وضعیت پیمانکار فاوا تأثیر می‌گذارد؛ ۳-ضعف‌های اثبات‌شده پیمانکار فاوا در مدیریت کلی ریسک فاوای خود، به ویژه نحوه تضمین دسترس‌پذیری، اصالت، یکپارچگی و محرمانگی داده‌ها، خواه داده‌های شخصی، خواه حساس یا غیرشخصی؛ ۴- مواردی که مقام نظارتی ذیصلاح دیگر نتواند به دلیل شرایط مربوط به توافقات آن قرارداد، به شکل مؤثری بر نهاد مالی نظارت داشته باشد.	به‌عنوان بخشی از فرآیند مناقصه، تیم حسابرسی باید تأیید کند که آیا الزامات یادشده DORA در نظر گرفته می‌شوند یا خیر؛ در غیر این صورت این فرآیند باید تقویت شود.
ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات اشخاص ثالث	برای خدمات فاوایی که پشتیبان کارکردهای حیاتی یا مهم هستند، نهادهای مالی باید استراتژی خروج (پایان همکاری یا فسخ قرارداد) را تدوین کنند. استراتژی‌های خروج باید ریسک‌هایی را که ممکن است در سطح ارائه‌دهندگان خدمات شخص ثالث فاوا پدید آیند، در نظر بگیرند؛ به ویژه شکست احتمالی از سوی آنها، کاهش کیفیت خدمات فاوای ارائه‌شده، هرگونه اختلال در کسب‌وکار ناشی از ارائه نامناسب یا ناموفق خدمات فاوا، یا هر ریسک عمده‌ای که در ارتباط با اجرای درست و بی‌وقفه خدمات فاوا ایجاد می‌شود.	به عنوان بخشی از محدوده حسابرسی، تیم حسابرسی باید هر دو فرآیند فسخ و پایان همکاری را برای خدمات شخص ثالث فناوری اطلاعات در نظر بگیرد تا تأیید کند که آیا الزامات DORA رعایت می‌شوند یا خیر.

۹. قدردانی

کنفدراسیون اروپایی مؤسسات حسابرسی داخلی (ECIIA)[۹۴] نهاد حرفه‌ای نماینده ۳۴ مؤسسه ملی حسابرسی داخلی در گستره اروپا و حوزه مدیترانه است. مأموریت ECIIA این است که: از حرفه حسابرسی داخلی دفاع کند و نقش و ارزش حسابرسی داخلی و حاکمیت شرکتی قدرتمند را نزد قانون‌گذاران و سایر ذی‌نفعان اروپایی ترویج کند و از مؤسسات ملی در دفاع از حرفه و خدمات مربوطه پشتیبانی کند.

۱۰. کمیته بیمه ECIIA

ECIIA در سال ۲۰۱۲ کمیته بیمه‌ای را با حضور بزرگ‌ترین شرکت‌های بیمه اروپایی تشکیل داد. مأموریت این کمیته چنین است: "به‌عنوان صدای واحد حرفه حسابرسی داخلی در بخش بیمه اروپا عمل کند، با قانون‌گذاران و سایر نهادهای ذی‌نفوذ در سطح اروپا تعامل داشته باشد و حرفه حسابرسی داخلی را به‌عنوان بخشی از حاکمیت شرکتی مطلوب در سراسر شاخه بیمه در اروپا نمایندگی نموده و آن را توسعه دهد". ECIIA حدود ۵۵۰۰۰ حسابرس داخلی را نمایندگی می‌کند که نزدیک به ۱۲۰۰۰ نفر از آنان در بخش بیمه فعال هستند.

[۹۴] European Confederation of Institutes of Internal Auditing

کارگروه شرکت کنندگان بنیاد NOREA[۹۵] در تهیه چک‌لیست‌های کنترلی DORA

گزارش و چارچوب مطالعاتی توسط اعضای زیر از گروه ویژه نظارتی NOREA (گروه ویژه سابق DORA) بررسی شده است:

نام	نقش	شرکت
Harry Boersen	CTO	ANVA
Danny Bos	Senior manager Cybersecurity & Privacy	Eraneos
Ibrahim Dogan	Register IT-Auditor	Brightlyn
Otto Hulst	Beleidsadviseur	Pensioenfederatie
Arno Kroese	Director IT Assurance & Advisory	KPMG
Marvin Kruin	Register IT-Auditor	MNK Risk, Audit & Advisory Services
René Zendijk	Head of Internal Audit	Scildon
Shairesh Algoe	CISOManager IT Security	Quantum Gateway FoundationBNG Bank
Andrey Prozorov	Cybersecurity and Privacy Expert	ISMS PRO
Jesper de Boer	Director IT Audit & Assurance	Deloitte
Wilfred Hanekamp	Partner IT Assurance & Advisory	Afier

برای مشاهده فهرست کامل اعضا و محتوای بیشتر ایجاد شده توسط این کارگروه، لطفاً به آدرس https://www.norea.nl/dora مراجعه کنید یا ما را در لینکدین دنبال کنید: https://www.linkedin.com/showcase/taskforce-dora

تاییدیه‌های گزارش مطالعاتی و چارچوب

گزارش مطالعاتی و چارچوب کنترلی ارائه شده در مستند چک‌لیست‌ها چارچوب کنترلی (چک‌لیست‌ها) توسط انجمن‌های صنایع مالی زیر تأیید شده است:

nederlandse vereniging van banken | VERBOND VAN VERZEKERAARS | PENSIOEN FEDERATIE | VBDN

گزارش مطالعاتی و چارچوب کنترلی DORA با بانک مرکزی هلند (DNB[۹۶]) و AFM[۹۷] به اشتراک گذاشته شده است. مقامات نظارتی پاسخ مشترک زیر را ارائه دادند:

"DNB و AFM چارچوب تهیه‌شده توسط NOREA را برای ارائه راهنمایی به صنعت در مورد اجرای عملی DORA مورد توجه قرار دادند. DNB و AFM در توسعه آن نقشی نداشتند. همچنین این چارچوب توسط DNB و AFM از نظر محتوا ارزیابی نشده است. با این حال، توسعه چنین چارچوب‌هایی مطابق با درخواست‌های قبلی DNB و AFM برای همکاری در این بخش برای افزایش تاب‌آوری سایبری کلی این بخش و در صورت تمایل، توسعه و به‌روزرسانی متقابل استانداردهایی است که می‌توانند به این امر کمک کنند. DNB و AFM تأکید می‌کنند که رعایت قوانین و مقررات مربوطه در هر زمان مسئولیت این نهاد است. هیچ اطمینانی از استفاده از چنین چارچوبی مبنی بر اینکه طرفین مطابق با قوانین و مقررات عمل می‌کنند، نمی‌توان به دست آورد."

چارچوب کنترلی DORA که در این گزارش مطالعاتی ارائه شده است، با همکاری Schuberg Philis توسعه داده شده است.

---

[۹۵] سازمان حرفه‌ای حسابرسان فناوری اطلاعات در هلند

[۹۶] Dutch Central Bank (DNB)

[۹۷] The Dutch Authority for the Financial Markets (AFM); [*has been responsible for supervising the operation of the financial markets since 1 March 2002.*]