دامنه ۱ مدیریت امنیت و ریسک (۱ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا سیاست امنیت اطلاعات رسمی، مصوب و ابلاغ شده است؟	تدوین سیاست ISMS ، تصویب در مدیریت، ابلاغ به همه واحدها		
2	آیا ساختار مدیریت ریسک (Risk Assessment) اجرا می‌شود؟	استفاده از روش‌های ISO 27005 یاNIST SP 800-30 ، ثبت ریسک‌ها، ارزیابی سالانه		
3	آیا نقش‌ها و مسئولیت‌های امنیتی تعریف شده‌اند؟	تدوین RACI برای مدیر امنیت، SOC، مدیر شبکه، مدیر سیستم		
4	آیا کارکنان دوره‌های آگاهی‌رسانی امنیتی می‌گذرانند؟	اجرای دوره‌های فیشینگ، پسورد امن، مهندسی اجتماعی هر ۶ ماه		
5	آیا سیاست نگه‌داری و حذف داده وجود دارد؟	تدوینData Retention ، تعیین مدت نگه‌داری و روش حذف امن		
6	آیا قراردادهای امنیتی با پیمانکاران بسته شده؟	افزودن بندهایNDA ، SLA امنیتی، و الزامات حریم خصوصی		
7	آیا ممیزی داخلی امنیت سالانه انجام می‌شود؟	تدوین برنامه ممیزی، گزارش، RCCA ، پیگیری اصلاح		
8	آیا مدیریت تغییرات (Change Management) وجود دارد؟	ایجادCAB ، ثبت تغییرات در سامانه، تأیید قبل از اعمال		
9	آیا طبقه‌بندی داده‌ها در سازمان اجرا شده است؟	ایجاد سطوح حساسیت، لیبل‌گذاری، سیاست دسترسی		
10	آیا کنترل‌های امنیت فیزیکی اجرا شده‌اند؟	نصب کنترل ورود، CCTV، قفل رک‌ها، ثبت ورود/خروج		
11	آیا مدیریت بحران و تداوم کسب‌وکار وجود دارد؟	طراحیBCP/DRP ، تعریفRTO/RPO ، تست بازیابی		
12	آیا مدیریت آسیب‌پذیری‌ها دوره‌ای انجام می‌شود؟	اجرای اسکن ماهانه با Nessus/Qualys و پیگیریPatch		

امتیاز دامنه ۱: ... / ۱۲

دامنه ۲ امنیت دارایی‌ها (۲ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا Asset Inventory کامل و به‌روز دارید؟	ایجاد CMDB و ثبت همه سرورها/شبکه‌ها/کلاینت‌ها		
2	آیا مالک داده (Data Owner) مشخص است؟	تعیین مالک، مسئول پردازش و مسئول نگه‌داری		
3	آیا اطلاعات بر اساس حساسیت طبقه‌بندی شده‌اند؟	ایجاد سطوح.Public/Internal/Confidential/Restricted		
4	آیا دسترسی به داده‌ها بر اساس طبقه‌بندی کنترل می‌شود؟	اعمال ACL مطابق Data Classification		
5	آیا Backup امن و تست‌شده دارید؟	Backup آفلاین، رمزنگاری، تست بازیابی دوره‌ای		
6	آیا رمزنگاری داده‌های حساس انجام شده؟	استفاده از AES-256 ، TLS1.3، Full Disk Encryption		
7	آیا سیاست حذف امن داده وجود دارد؟	استفاده از روش DoD5220.22-M یا Shredding		
8	آیا اطلاعات حساس خارج از شبکه کنترل شده‌اند؟	DLP، ممنوعیتUSB ، Logging فایل‌های خروجی		
9	آیا مدیریت رسانه‌های ذخیره‌سازی دارید؟	نگه‌داری امن، لاگ ورود/خروج، رمزنگاری		
10	آیا دارایی‌های قدیمی Decommission شده‌اند؟	مستندسازی، حذف امن، خارج کردن از شبکه		
11	آیا حسابرسی دسترسی‌ها انجام می‌شود؟	بازنگری فصلی دسترسی کارمندان و پیمانکاران		
12	آیا داده‌ها در Transit و At-rest محافظت شده‌اند؟	TLSبرای انتقال، encryption-at-rest در دیتابیس		

امتیاز دامنه ۲: ... / ۱۲

دامنه ۳ مهندسی امنیت و معماری (۳ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا شبکه دارای Segmentation (VLAN/DMZ) است؟	تفکیک شبکه کاربران، سرورها، اینترنت، VoIP		
2	آیا فایروال‌های سازمان Stateful و به‌روز هستند؟	به‌روزرسانی، بازبینیRule ها، اعمال Least Privilege		
3	آیا ارتباطات حساس رمزنگاری شده‌اند؟	استفاده ازIPsec ، SSL/TLS، تونل VPN		
4	آیا امنیت فیزیکی رک‌ها رعایت شده؟	نصب قفل، دوربین، کنترل دسترسی		
5	آیا سیستم‌عامل‌ها Patch شده‌اند؟	ایجاد Patch Cycle هفتگی/ماهانه		
6	آیا سرورها با اصول Hardening امن شده‌اند؟	Disableسرویس‌های غیرضروری، تنظیمات امنیتی CIS Benchmarks		
7	آیا کنترل دسترسی در سطح شبکه پیاده‌سازی شده؟	NAC, 802.1X, Port Security		
8	آیا تجهیزات دارای Firmware امن و به‌روز هستند؟	آپدیت Firmware سوئیچ، روتر، فایروال		
9	آیا مکانیزم ضد حملات DDoS وجود دارد؟	فایروال لایه ۷، WAF، سرویسDDOS Cloud		
10	آیا مکانیزم Logging استاندارد وجود دارد؟	جمع‌آوری Log درSIEM ، نگه‌داری ۱۲ ماه		
11	آیا سرورها Redundancy دارند؟	RAID، HA، Cluster، UPSدوگانه		
12	آیا کنترل‌های Integrity مانند HIDS فعال هستند؟	نصب OSSEC/Wazuh و مانیتورینگ تغییرات فایل		

امتیاز دامنه ۳: ... / ۱۲

دامنه ۴ امنیت شبکه و ارتباطات (۴ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا طراحی شبکه سه‌لایه (Access/Distribution/Core) رعایت شده؟	استانداردسازی ساختار و تفکیک جریان ترافیک		
2	آیا قواعد فایروال Document شده‌اند؟	مستندسازی Rule Base و حذفRule های زائد		
3	آیا IPS/IDS فعال است؟	فعال‌سازی Snort/Suricata و اتصال به SIEM		
4	آیا Wireless با WPA3 یا WPA2-Enterprise محافظت شده؟	مهاجرت ازWPA/WEP ، استفاده از RADIUS		
5	آیا کنترل MAC Filtering یا NAC فعال است؟	فعال‌سازی ۸۰۲.۱X یا NAC		
6	آیاNAT ، PATو Routing ایمن پیکربندی شده؟	جلوگیری ازIP Spoofing ، تنظیم ACL در روتر		
7	آیاPort های غیرضروری بسته شده‌اند؟	انجام Port Audit و محدودسازی در فایروال/سوییچ		
8	آیا VPN سازمانی امن است؟	استفاده از SSL/TLS VPN یا IPsec نسل جدید		
9	آیا ترافیک داخلی رمزنگاری می‌شود؟	فعال‌سازی TLS داخلی، استفاده از mTLS		
10	آیا WireShark/NetFlow Logging فعال است؟	جمع‌آوری Flow برای تحلیل حملات		
11	آیا تجهیزات شبکه از هم ایزوله شده‌اند؟	Private VLAN، غیر فعال‌سازی inter-vlan routing غیرضروری		
12	آیا آنتی‌ویروس و EDR روی کلاینت‌ها هست؟	نصبEDR (CrowdStrike/SentinelOne/Defender)		

امتیاز دامنه ۴: ... / ۱۲

دامنه ۵ مدیریت هویت و دسترسی (۵ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا MFA روی همه حساب‌ها فعال است؟	فعالسازی MFA روی پنل‌ها، VPN، AD		
2	آیا دسترسی کاربران بر اساس RBAC تعریف شده؟	تعریفRole ها و اعمال Least Privilege		
3	آیا فرآیند Joiner/Leaver/Mover وجود دارد؟	طراحی فرآیند HR–IT–Security برای مدیریت حساب‌ها		
4	آیا حساب‌های Shared وجود ندارند؟	حذف حساب مشترک؛ ایجاد حساب فردی با لاگ کامل		
5	آیا احراز هویت مرکزی (AD/LDAP) دارید؟	مهاجرت به Active Directory یا FreeIPA		
6	آیا دسترسی‌های سطح بالا (Admin) محدود شده؟	ایجاد گروه جدا برایAdmin ، استفاده از PAM		
7	آیا Password Policy استاندارد اجرا شده؟	حداقل ۱۲ کاراکتر، Expiration، عدم استفاده مجدد		
8	آیا ورود و خروج کاربران لاگ‌گیری می‌شود؟	اتصال AD/AAA به SIEM		
9	آیا حساب‌های غیر فعال حذف می‌شوند؟	Disableبعد از ۳۰ روز، حذف بعد از ۹۰ روز		
10	آیا سیستم SSO امن وجود دارد؟	استفاده ازSAML ، OAuth2، OpenID Connect		
11	آیا دسترسیAPI ها کنترل‌شده است؟	OAuth2 Tokenو محدودیت دسترسی		
12	آیا دسترسی‌ها ماهانه Audit می‌شوند؟	بازنگری دقیق دسترسی مدیران و کارمندان		

امتیاز دامنه ۵: ... / ۱۲

دامنه ۶ ارزیابی و تست امنیت (۶ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا تست نفوذ سالانه انجام می‌شود؟	انجام Pentest با استاندارد PTES/OWASP		
2	آیا اسکن آسیب‌پذیری ماهانه دارید؟	اجرایNessus/Qualys ، رفع Findings		
3	آیا نتایج تست امنیت اصلاح می‌شوند؟	ایجاد فرآیند Patch & Fix با پیگیری		
4	آیا Security Baseline برای سرورها دارید؟	استفاده از CIS Benchmark		
5	آیا SIEM برای تحلیل امنیت فعال است؟	استقرار Splunk/QRadar/Wazuh		
6	آیا تست فیشینگ دوره‌ای انجام می‌شود؟	اجرا باGoPhish ؛ آموزش کاربران		
7	آیا تست Disaster Recovery انجام شده؟	تست Failover دیتابیس، Backup، سرویس‌های حیاتی		
8	آیا تست Load/Stress امنیتی انجام شده؟	تست با JMeter/K6 برای مقاومت سرویس		
9	آیا Logging سطح بالا فعال است؟	تنظیمSIEM → Syslog ، نگه‌داری ۱۲ ماه		
10	آیا مانیتورینگ ۷/۲۴ دارید؟	ایجاد SOC یا برون‌سپاری MDR		
11	آیا تست امنیت اپلیکیشن انجام می‌شود؟	اجرایSAST/DAST ، ابزار مانند SonarQube		
12	آیا تست امنیت شبکه داخلی انجام می‌شود؟	Pentestداخلی، بررسی VLAN Hopping و ARP Poisoning		

امتیاز دامنه ۶: ... / ۱۲

دامنه ۷ عملیات امنیت (۷ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا فرآیند Incident Response تدوین شده؟	نوشتن IRP شامل مراحل Identification → Eradication		
2	آیا تیم مشخص برای مدیریت حادثه وجود دارد؟	تعیین نقش Incident Manager و تحلیلگر		
3	آیا SIEM Active است و Alert می‌دهد؟	تنظیم Rule وDashboard ، اتصال لاگ‌ها		
4	آیا Backup تست بازیابی دارد؟	تست RTO/RPO هر ۳ ماه		
5	آیا مدیریت Patch منظم دارید؟	زمان‌بندی هفتگی/ماهانه		
6	آیا مکانیزم Forensics وجود دارد؟	ایجادImage گیری، Chain of Custody، ابزار FTK		
7	آیا کنترل USB محدود شده؟	DLP، GPO Restriction، ثبت لاگ		
8	آیا مانیتورینگ رفتار کاربران فعال است؟	UEBAیا Log Behavior Analysis		
9	آیا مدیریت Log امن است؟	ذخیره لاگ خارج از سرورهای عملیاتی		
10	آیا SOP برای عملیات امنیت دارید؟	تدوین رویه‌هایOperational: Backup, Patch, Incident		
11	آیا Secure Disposal انجام می‌شود؟	Shredding، حذف مغناطیسی، کارخانه امحا		
12	آیا آنتی‌ویروس EDR/به‌روز است؟	فعال‌سازی EDR با بخشی واکنش خودکار		

امتیاز دامنه ۷: ... / ۱۲

دامنه ۸ امنیت توسعه نرم‌افزار (۸ از ۸)

	سؤال ارزیابی	راهکار	خیر	بلی
1	آیا SDLC سازمان امن است؟	افزودن چک‌پوینت امنیتی در مراحل معماری → تست		
2	آیا الزامات امنیتی قبل از توسعه تعریف می‌شوند؟	تهیه Security Requirements و تهدیدشناسی		
3	آیا کدها SAST اسکن می‌شوند؟	SonarQube, Checkmarx		
4	آیا تست DAST انجام می‌شود؟	OWASP ZAPیا BurpSuite		
5	آیا CI/CD امن است؟	اضافه‌کردنSecret Manager ، محدودیت دسترسی		
6	آیاAPI ها امن شده‌اند؟	استفاده از Token, Rate Limit, TLS		
7	آیا دسترسی به سورس‌کد محدود است؟	دسترسی Role-based در Git		
8	آیا مدیریت نسخه امن است؟	Branch Protection، Code Reviewاجباری		
9	آیا Dev و Prod جدا هستند؟	جداسازی محیط‌ها، منع اتصال مستقیم		
10	آیا تهدیدشناسی (Threat Modeling) انجام می‌شود؟	STRIDE, DFD Diagramقبل از توسعه		
11	آیاLog های اپلیکیشن امن نگه‌داری می‌شوند؟	Maskingداده‌های حساس، ارسال به SIEM		
12	آیاFramework ها وLibrary ها به‌روز هستند؟	SCA (Software Composition Analysis)و آپدیت دوره‌ای		

امتیاز دامنه ۸: ... / ۱۲

چطور خروجی نهایی شبکه را امتیازدهی کنیم؟

مجموع امتیاز ۸ دامنه:

Total Score = (Domain1 + … + Domain8) از ۹۶

تفسیر سطح امنیت:

وضعیت	امتیاز
امنیت بسیار خوب	**۹۶–۸۰**
امنیت قابل‌قبول	**۷۹–۶۵**
پرریسک – نیازمند اصلاح	**۶۴–۴۵**
خطرناک – شبکه آسیب‌پذیر است	**۴۵>**