



Compliance-Level Risk Assessments for Your Business Needs

Comprehensive Risk Analysis: Prevention, Protection, & Remediation

Security Risk Assessments

Our risk assessment experts provide comprehensive solutions to identify potential risks, define gaps in your current processes, and prioritize the best course of action to mitigate them. Our proven methodologies and advanced tools ensure that you can make informed decisions on managing risks effectively.

Risk Assessment Process

Plan

Discover

Analyze

Report

Discuss

Service Summary

Risk assessments are essential to discovering risk and for defining appropriate security and risk mitigation strategies that fit your company's objectives. There are two components to risk assessments: 1) Security Reviews (often called audits) provide a complete process for defining risk strategies based upon your objectives, security posture and status. 2) Security Tests diagnose actual vulnerabilities in specific areas of your security infrastructure.

20 Years in Security

Leading Partner for Top Security Vendors.

We help companies

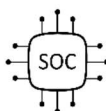
- ✓ Assess Risk
- ✓ Define Gaps

Prioritize Solutions

- ✓ Manage Complex Security

Security You Can Trust

At eSecurity Solutions, security is our only business. Since 2003, we have focused exclusively on securing your business. We don't sleep until your data and business is secure and compliant. We provide you peace of mind with our affordable SMB to enterprise security solutions.



SIEM-Based
SOC



Cloud &
Zero Trust



MDR for
EDR



Managed
Firewalls



Backup &
BDR



2-Factor
Authentication



SaaS
Email

Complete Solution

Risk Assessments, Security Products, Managed Security

Certified Experts

CISA Auditors, Ethical Hackers, Penetration Testers

Security Reviews & Gap Analysis

The most important part of risk assessments is clearly the Security Review & Gap Analysis. It is the glue that ties the entire risk assessment solution together. As with a security audit, there must be a process for assessing a company's risk profile. In a security review, we review your key assets, current security strategy, controls, and IT infrastructure, and prioritize your top vulnerabilities, risks, and recommended security control solutions. The resulting report is suitable for defining your future security strategy, defining budgets and the order to implement security mitigation solutions.

Security Review & Gap Analysis		Audit your security strategy, and controls and they are appropriate to protect your key digital assets. Recommends Prioritized list of Controls.
Security Testing		Security Tests diagnose actual vulnerabilities by testing specific areas of your security.
Security Tests	Compliance Scan	Automated scan of key assets to gather compliance information for the Security Review & Gap Analysis
	Network <u>Vulnerability</u> Tests	Automated tests applied from outside &/or inside your network to identify <u>basic</u> vulnerabilities.
	Network <u>Penetration</u> Tests	Targeted attacks by white hat hackers looking for vulnerabilities from the inside or outside your Network.
	Web Application Penetration	Web application system testing process that includes a series of fabricated malicious
	Social Engineering Tests (ie. Phishing)	Pretending to be a trusted party to manipulate an authorized user to provide access to confidential systems
	Wi-Fi Review & Testing	Examines the security of the wireless topology and design including wireless access points, clients & mobile.
	VOIP Testing	Test your VOIP system for vulnerabilities.
	Security Configuration	Examines the security configuration firewalls & other key security for optimal security.
	Operational Tests	Selected tests of various corporate systems for security controls such as application software tests.
	Physical Security Tests	Testing of physical infrastructure for appropriate security controls for offices and data centers

Security Testing

Security Tests diagnose actual vulnerabilities by testing specific areas of your security infrastructure. They can be performed with or without a Security Review. Each test has separate goals and a different process, but all are designed to identify vulnerabilities and to assign a probability of occurrence so that a plan can be defined related to controlling that risk. Consult your security expert to determine which tests might be appropriate for your environment.

The most common security tests are vulnerability scans and penetration tests. These tests can be used to evaluate external networks, Web sites and Web applications as well as internal networks. Other tests evaluate areas such as wireless networks, VOIP, security configurations and physical security.

Two Kinds of Security Risk Assessments:

1. One-Time Risk Assessment Project
2. Ongoing Compliance-a-a-S Readiness: Risk Assessment with Quarterly Updates & Adjustments

Pick Audit Standards



Security Review Process

Security Reviews have a structured process for revealing your security gaps and recommended strategy. This process is designed to provide a complete top-down review of your security. Process steps include:

1. Discovery about your:

- Key Digital Assets
- Objectives
- Workflow
- Systems & Architecture
- People & Processes
- Review of Policies
- Issues & Threats
- Current Controls
- Likely Vulnerabilities

2. Deep Dive on Risk Areas

3. Analysis of Risks

4. Reporting

5. Discussion



This process uses a question-based model for discovery supplemented by other relevant documents provided by the company such as architectural diagrams, and policy manuals.

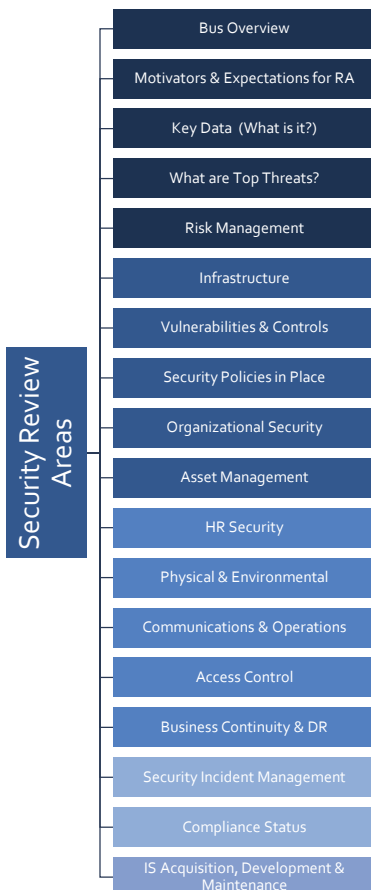
Security Review Areas

To properly review your security, eSecurity Solutions follows the CISA security auditing process to review all relevant areas of your security. We review all areas of security as defined by ISO and other security standards to provide a complete picture of your business. All relevant areas of your business are probed to understand relevant security posture as it pertains to your security objectives. The general flow of discovery and analysis starts with a better understanding of your key assets and your business. We peel back the onion to analyze all components referenced in “security best practices” and specific security regulations.

The ISO security model and most major regulations require an evaluation of:

1. Key Assets
2. Policies and Procedures
3. Physical Security
4. 3rd Party Controls
5. Internal Security Controls
6. Compliance-Level Activities

The goals are to measure your security posture against your specific compliance goals as well as “best practices” security as it relates to a company of your type and size.



Security Review Deliverables

A Security Review and Gap Analysis provides results that show how your security risks, gaps and control recommendations relate to your vulnerabilities. Results are provided in the following areas:

1. Discovery Summary & Risk Score

2. Risk Heat Map

3. Current Controls

4. Prioritized:

- Security Threats
- Security Vulnerabilities
- Prioritized Risk Gaps

5. Prioritized Gap Solutions

- by Threat group
- by Control group

The analysis and reports provide insight into your specific threats, vulnerabilities, and risks considering the controls you have in place and your security objectives (such as regulation, board-of-director compliance, or audit avoidance).

Discovery Risk Score	
Risk Management	1.8
Vulnerabilities & Controls	3.2
Security Policies	2.7
Organizational Security	6.0
Asset Management	4.5
HR Security	5.4
Physical & Environmental	4.0
Communications & Operations	4.0
Access Control	4.9
Business Continuity & DR	1.3
Security Incident Management	1.0
Compliance Status	3.2
IT Sys. Acquisition, Dev & Maintenance	3.3
Weighted Average Score	3.7

SECURITY HEAT MAP																				
Risk Assess VA etc.	Policies Process HR	Physical Security	3rd Party Controls	Gateway Protection				Wireless Protection	Enhanced Endpoint Security		Access Control			Data Protection (Encryption, DLP)				Continuity	Compliance	
				Firewall	Web	Mail	WebApp		EP	Mobile	Remote	NAC	Strong Auth.	Laptop/ Servers	Removable	DLP	Secure		SIEM	Archiving
		Incl. Media Handling					Ecom., Websites		AV, Web, Encrypt, Patch, HIPS	AV, NAC, DLP	Remote Access	& NW Segment ing	2-Factor Policies Privileges	Whole Disk & Ext. Storage	Removable Storage	Network & Endpoint	Communica tions	BDR	Monitor/ Alert/ Report	
4	2	3	2	4	4	2	2	1	3	3	3	3	3	3	3	3	3	3	4	2

Security Reports & Follow-up

eSecurity Solutions will present findings in detailed and summary reports and review it with your organization. These reports will focus on defining prioritized risks/gaps and the recommended solution areas.

Once this process is complete, specific vendor alternatives for recommended products and services can be explored as a follow-on activity for gap remediation. We will be with you every step of the way to guide you through the process.

PRIORTIZED CONTROL RECOMMENDATIONS (Sample)

Priority	Solution	Purpose	Recommended Product/Service
1	MFA with SSO	Increase access control security for remote applications, internal infrastructure, M365, remote users to meet best practices.	• MFA with SSO supporting all target environments
2	Security Monitoring & Response	Acquire a 24x7 security monitoring solution that monitors all security controls and key IT to provide maximum detect and response capabilities per best practices & regulations.	• 24x7 SIEM based SOC service (SOCaaS)
3	Enhanced security for cloud servers	Increase security for cloud servers & data per shared responsibility model. Protect, detect and response.	• Server EDR solution • SIEM/SOC monitoring (per #2)
4	Implement zero trust security for remote workers	Ensure access control for remote workers in terms of authentication, usage, and visibility. Implement for employees, partners, customers, and all 3 rd parties.	• MFA w/SSO • Zero trust granular solution

Contact Us to Learn More

sales@esecuritysolutions.com