Risk Assessment Services Data Sheet

Security Risk Assessments

We help companies

- ✓ **Assess Risk**
- ✓ **Prioritize Solutions**
- ✓ **Manage Complex Security**

Compliance Level Risk Assessments

Security Reviews + Testing Services

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.

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 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 tests for security testing are vulnerability tests and penetration tests. These tests can be used to test external networks, Web sites and Web application as well as internal networks. Other tests evaluate areas such as wireless networks, VOIP, security configurations and physical security.

Services Offered

- ☑ **Security Review & Gap Analysis**
- ☑ **Security Tests**
  - ☑ External Scans
  - ☑ Internal Scans
  - ☑ Penetration
  - ☑ Phishing Tests
  - ☑ VOIP Tests
  - ☑ Wireless Tests
- ☑ **Security Projects**

❶ **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.
❷ **Security Tests**		Security Tests diagnose actual vulnerabilities by testing specific areas of your security infrastructure.
Security Tests	**Network Vulnerability Tests:** • **External & Internal**	Automated tests applied from outside &/or Inside your network to identify basic vulnerabilities to common current threats.
	Network Penetration Tests • **Internal Vulnerability Tests**	Targeted attacks to your network by white hat hackers looking for vulnerabilities to sophisticated attacks from the inside or your Network.
	Web Application Penetration	A rigorous testing process that includes a series of fabricated malicious attacks to see the level of security of the Web application system
	Social Engineering Tests (ie. Phishing)	Pretending to be a trusted party to manipulate an authorized user to provide access to confidential business secrets or information about usernames and passwords
	Wi-Fi Review & Testing	Examines the security of the wireless topology and design. Wireless components such as controllers, access points, client workstations and mobile device settings are reviewed to ensure proper security measures
	VOIP Testing	Test your VOIP system for vulnerabilities.
	Security Configuration	Examines the security features and settings of IDS, IPS, UTM security appliances and other security solutions for optimal security configurations.
	Operational Tests	Selected tests of various corporate systems for security controls such as application software tests.
	Physical Security Tests	Testing of physical and environmental infrastructure for appropriate security controls for office and data centers and vulnerability to environmental disasters.

Risk Assessment Services Data Sheet

Risk Assessment Process

- ☑ Plan
- ☑ Discover
- ☑ Analyze
- ☑ Report
- ☑ Discuss

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:**
   a. Key Digital Assets
   b. Objectives
   c. Workflow
   d. Systems & architecture
   e. People & processes
   f. Review of policies
   g. Issues & Threats
   h. Current Controls
   i. 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.

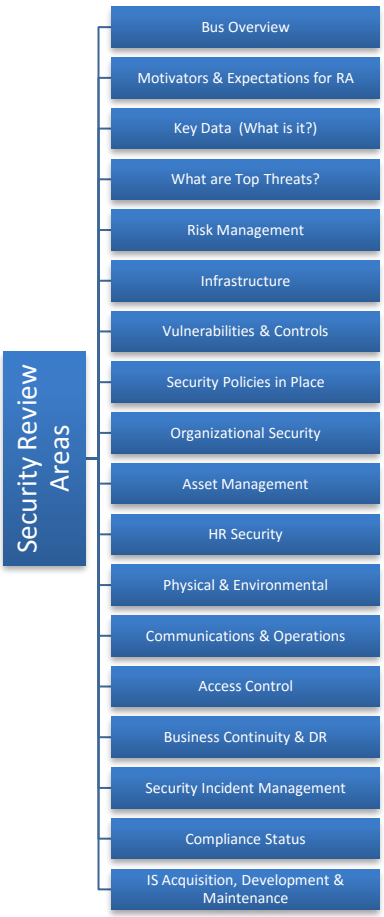
eSecurity Solutions

- **13 Years in Security**
- **Certified**
  - CISA Auditors
  - Ethical Hackers
  - Penetration Tester
- **Complete Security**
  - Risk Assessments
  - Products
  - Managed Security
- **Top Vendor Partners**
- **Affordable SMB – Enterprise Solutions**

Peace of Mind

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 understand 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, business type and size.

Risk Assessment Services Data Sheet

Risk Assessment Results

- ☑ Score
- ☑ Prioritize
- ☑ Analyze
- ☑ Recommend

Next Steps

- ☑ Budgeting
- ☑ Remediation

TRY OUR MANAGED RISK MITIGATION SOLUTIONS

- Managed Firewalls
- Log Monitoring/SIEM
- Intrusion Detection
- Backup & BDR
- 2-Factor Auth.
- SaaS Email
- SaaS Web
- Endpoint

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.

Contact us for a quote or information today:

886-661-6685

sales@eSecuritySolutions.com

www.eSecuritySolutions.com

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 (Factoring Likelihood of Occurrence & Impact of Attack)
5. **Prioritized Gap Solutions**
   - by Threat group
   - by Control group

The analysis and reports provide insight into your specific threats, vulnerabilities and risks in light of the controls you have in place and your security objectives (such as regulation or 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 (by # of Questions)	3.7

SECURITY HEAT MAP

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

eSecurity Solutions will present these findings in report form and review it with your organization. This report can serve as a guide for your future security strategy and IT security budget.

PRIORTIZED CONTROL RECOMMENDATIONS

Priority	Solution	Purpose	Product/Service
1	**Network Firewall with UTM**	Protect network from external attacks, control Internet access for employees, provide secure remote access (VPN) with optional strong authentication, and logging and reporting (visibility of threats, Internet usage, and remote access)	• Firewall w/ UTM Bundle & 24x7 Support/warranty • Optional Firewall HA Unit for failover • Cloud SandBox Services for Firewall (add-on) • Advanced APT Services for Firewall (add-on) • Logging and Reporting Services for Firewall
2	**Full Endpoint Security Suite with Encryption and DLP**	Protect endpoints from viruses and malware, block access to malicious websites or site with bad reputations, protect against system vulnerabilities, encrypt files/folders, removable media and hard drives, control access to removable media, identify and control access to data, and centrally monitor and manage	• Industry Leading Anti-virus/malware • Web Browser Security • Endpoint HIPS and Firewall • Endpoint Encryption and File/Folder Encryption • USB Storage Device Control (Incl. Encryption) • DLP Endpoint Solution • NAC (Network Access Control
3	**Mobile Mgt & Security** • MDM iPhone & Android • Mobile Sec. for Androids	Enforce security policies on mobile devices that access your network, email, and other assets and provide anti-malware for Android devices	• Mobile Device Management (Centrally Managed) • Mobile Security for Android (Centrally Managed)
4	**Patch/Update Management**	Protect against OS and application vulnerabilities by centrally monitoring and management of OS and applications patches and updates	• Patch Management Solutions (Centrally Managed)

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.

Contact us today to see how we can help you with your risk assessment and mitigation needs.