02.03.2022

Cyber Security Maturity Self-Assessment Report

XYZ Corporate Office

RiskWatch International

SECURITY ASSESSMENT EXECUTIVE SUMMARY

XYZ Corporate Office

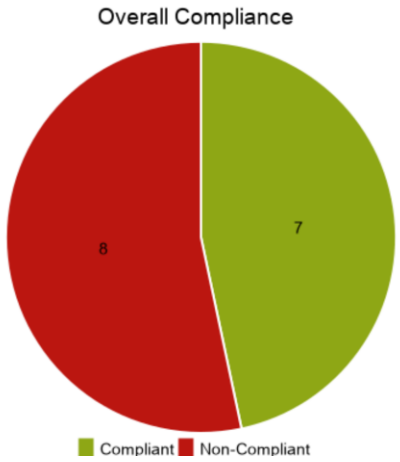
SecureWatch was utilized to conduct a self-assessment for RiskWatch International. In this process, questions surveying the maturity level of select information security controls were distributed, and a compliance percentage was calculated based on those responses. Doug Marsh answered the survey for this assessment.

Overall compliance	47%
Avg. compliance of all respondents	41%
Areas that need improvement	8

- ✓ ***Overall Compliance*** is determined by the percentage of responses that fell in the maturity level range of 4 or 5. If the security maturity level of a control was below 4, that control is deemed “non-compliant.”
- ✓ ***Average Compliance of all Respondents*** is the overall compliance of all organizations across the globe that have participated in this information security maturity assessment. Use this score to see how your organization’s security profile stacks up against other organizations.
- ✓ ***Areas that Need Improvement*** are the number of security controls at a maturity level of 3 or below. Organizations should try to maintain a maturity level of 4 or higher for all the controls included in this assessment. You will be able to see which controls need improvement on page 5.

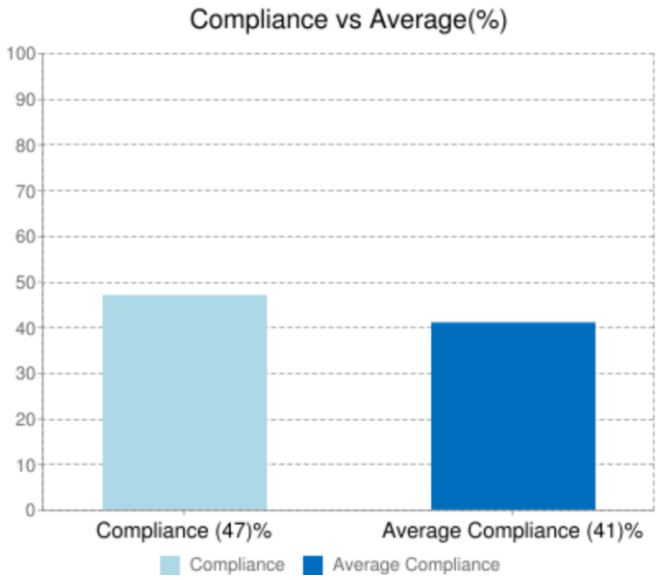
OVERALL CONTROL MATURITY

Breakdown of the percentage of security controls that are below the acceptable maturity level.



GLOBAL COMPLIANCE COMPARISON

This section compares the maturity level of this facility to others around the world that have been assessed with the same criteria.



ASSESSMENT NARRATIVE

About RiskWatch Assessment Applications

In 1993, RiskWatch began developing specialized, easy-to-use risk and compliance assessment software that could be used by clients all over the world for physical security, information security, critical infrastructure security, regulatory compliance, and more. The software was developed in accordance with federal guidelines and a variety of US Federal agencies.

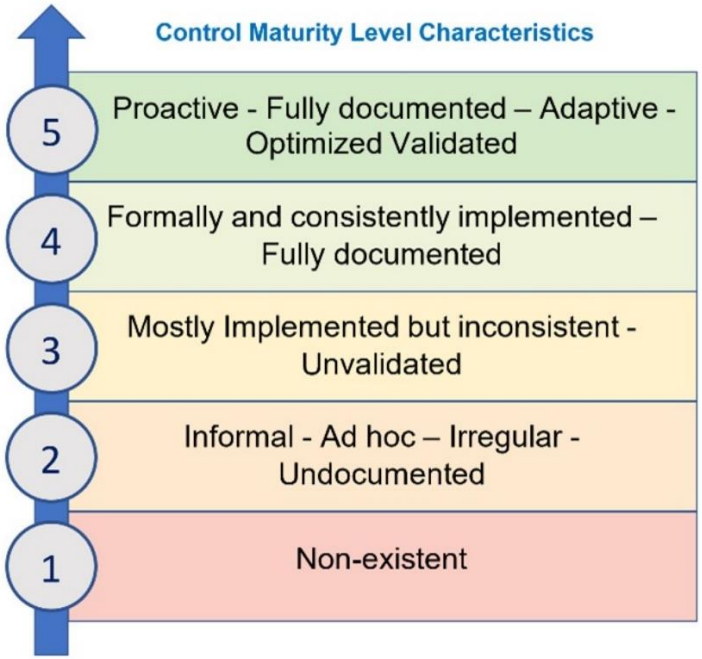
Since then, RiskWatch has been used by State governments in all 50 states and internationally in Belgium, Canada, Dubai, Japan, Malta, Mexico, Romania, Saudi Arabia, South Africa, Sweden, Switzerland, Thailand, and Turkey. From multi-national corporations to community banks, RiskWatch's risk assessment software became one of the world's most adaptable and widely used security risk assessment software platforms.

Purpose of this Assessment

Assessing your information security maturity can help reduce your liability exposure, manage risk, monitor, and maintain security, and track the continuous improvement of your overall security maturity level. This assessment is a very high-level assessment. For a deeper evaluation of your security posture, you can use one of RiskWatch's risk and compliance solutions.

Information Security Maturity Model

The Maturity Model is a way to illustrate the maturity and reliability of an organization's cybersecurity infrastructure to safeguard sensitive information stored or processed within the organization's information systems. The tiered approach can facilitate tracking and documenting improvement through periodic reassessment. Tiers move from non-existent controls to informal and undocumented and up to the top of the maturity scale to a proactive, optimized, and fully documented information security control set.



ASSESSMENT SUMMARY

The following summarizes the assessment responses and compares them to crowd-sourced averages worldwide to illustrate how your organization compares to others who have participated in the self-assessment.

Security Control	Your Maturity Level	Guidance	% of Organizations with a Maturity Level 4 or Higher
IT Governance Framework: Are you certified in an IT Governance framework such as ITIL or ISO 27001?	2. We are preparing for certification in an IT Governance Framework and have most or all required controls in place.	Information security governance ensures proactive implementation and management of appropriate information security controls while managing evolving information security risks. By implementing a governance framework, you can ensure that your information security strategies are aligned with and support your organization's business objectives. Being certified verifies that you have taken the necessary steps to protect your organization and is proof of effective internal security practices.	23%
Privacy Regulations: Are you compliant with all applicable state, national, international, and industry-specific privacy regulations? (example: GDPR, Privacy Act, CCPA, HIPAA, etc.)	3. We are aware of the regulations that apply to the organization, but we are compliant with only some of their requirements.	It is essential to follow all state, federal, and international laws and regulations relevant to your organization's operations. It would be best to be adaptable to and conscious of the ever-shifting regulatory landscape. Non-compliance to regulations can lead to litigation, financial liability, and damage to your organization's reputation and existing relationships. Third-party certifications verify that you have taken all the necessary steps to comply.	36%
Industry Standards: Are you compliant with all applicable standards defined by your industry?	2. We are aware of the standards defined by our industry, but we are not compliant with their requirements.	Industry standards are generally the minimal accepted requirements that the members of that industry follow. Most industries define these standards and best practices through a governing body or advisory group. Not meeting industry standards can expose your organization	45%

Security Control	Your Maturity Level	Guidance	% of Organizations with a Maturity Level 4 or Higher
		to litigation and other penalties.	
Third-party Audit: Have you received a third-party security audit? (example: SSAE-16 SOC Report)	3. Our security controls were audited by a third party over one year ago.	Having an outside firm perform an audit of your security controls demonstrates your organization's commitment to safeguarding customer data and its assets. You should have regular audits to verify that your security posture is being maintained and show continuous improvement.	28%
Compliance with Policies: Do you regularly audit your workforce's adherence to the organization's policies?	4. We require that personnel read the company's policies and sign a document acknowledging their understanding and compliance. Regular INTERNAL audits are performed with disciplinary actions taken for non-conformities.	Your controls are mature in this area	40%
Risk Analysis Process: Have you implemented a formal risk analysis process?	2. We perform ad hoc risk analysis that is not formally documented.	Risk analysis allows you to be conscious of the threats affecting your organization. By cataloging these threats and estimating how often they are likely to occur (likelihood) and how much direct or indirect damage each occurrence could have (impact) on your organization, you can prioritize mitigation efforts. These prioritized threats make up your risk register. You can rate their levels of Risk (likelihood x impact) and compare them to the level of investment required to implement any recommended mitigating controls. Use this information to map your course of action to reduce your risk.	34%
Restrict Physical Access: Are access controls used to restrict physical access to sensitive	5. Locking barriers and doors/gates prevent unauthorized access from the	Your controls are mature in this area	61%

Security Control	Your Maturity Level	Guidance	% of Organizations with a Maturity Level 4 or Higher
areas?	outer perimeter. Formal access control policies and key management systems are used. Sensitive areas have additional access controls in place.		
Fire and Flood Protection: Are your computer rooms and other critical areas protected against fire and flood?	5. We maintain fire suppression and detection devices/systems specifically designed not to damage sensitive assets that are activated automatically and notify emergency responders in the event of a fire. Critical assets are located in areas that would not be affected by flooding. There are documented evacuation procedures that are regularly tested.	Your controls are mature in this area	43%
Intrusion Detection: Do you use security guards or automated intrusion detection systems?	5. We employ an intrusion detection system or CCTV that is continuously monitored. There is a staffed security operations center. A security guard force provides 24/7 surveillance.	Your controls are mature in this area	58%
Security Controls Audit: Do you conduct periodic drills and internal audits to verify the effectiveness of your security controls?	2. We employ ad hoc auditing of our security controls.	It is essential to continuously monitor your controls and conduct tests to ensure your processes are working as designed. You should regularly audit your security controls and conduct drills based on a formal documented process and schedule. You should also employ third-party penetration testing to objectively look at your security posture. Document your results and report them to all relevant stakeholders. Implement remedial action promptly based on audit findings.	29%

Security Control	Your Maturity Level	Guidance	% of Organizations with a Maturity Level 4 or Higher
Information Security Duties: Do you have personnel with dedicated information security duties?	5. We have a department within the organization dedicated to information security.	Your controls are mature in this area	50%
Information Securities Policy: Do you have a documented information security policy?	4. We have documented information security policies that are reviewed and updated at least annually.	Your controls are mature in this area	40%
Security Awareness Training: Do employees receive information security awareness training?	1. We do not provide information security awareness training to employees.	Technical controls can be rendered useless because employees lack cybersecurity awareness training. Employees need to be informed about good cybersecurity practices and understand the crucial role that they play in safeguarding their organization's information assets	30%
Updates and Patches: Do you regularly apply system and security updates/patches?	3. Our Information system is updated or patched based on a schedule.	Information systems inevitably will have vulnerabilities. These vulnerabilities may come from flaws in the ordinal design, new technologies that make the system's original security controls ineffective, or malware introduced into the system. These vulnerabilities will not always be evident. You should consistently be applying any security patches that your system developers provide. You should also routinely employ a vulnerability scanner	43%
Background Checks: Do you perform any employment history or background checks?	4. Employees who have access to or handle sensitive data have had their histories verified and received a background check.	Your controls are mature in this area	43%

RiskWatch

Assessing:

- ✓ Your Organization
- ✓ Sites
- ✓ Information Systems
- ✓ Consulting Clients
- ✓ Vendors
- ✓ Suppliers
- ✓ Projects

Purpose:

- ✓ Risk
- ✓ Compliance
- ✓ Security Control Audit
- ✓ Governance/Policy

Criteria:

- ✓ Regulations
- ✓ Standards
- ✓ Policy
- ✓ Best Practices

www.riskwatch.com
800-360-1898

This report was generated from one of RiskWatch's risk and compliance assessment applications. RiskWatch applications take select assessment criteria and present them to key personnel in the form of a survey. This survey determines what percentage of the requirements are being met. Additionally, the resultant compliance percentage can be leveraged with other metrics to calculate an assessment Risk score.

RiskWatch applications include

SecureWatch ***CyberWatch***
ComplianceWatch ***VendorWatch***
SupplierWatch ***ClientWatch***

This report illustrates just one example of how RiskWatch applications can be employed to conduct an assessment.

Application administrators have complete freedom to customize their assessments.

- White label with your logos and brand colors
- Use your assessment criteria or one of many off-the-shelf options
- Customizable user interface
- Customizable user permissions
- Customizable reports using the built-in text editor
- Customizable email notifications
- Customizable risk and compliance score formula
- Customizable metrics
- Customizable survey content distribution

For more information about RiskWatch applications or to try it for free, visit www.RiskWatch.com