Cybersecurity Risk Assessment in Plain Language

It is no Longer Optional

Proactive and effective information security management is no longer optional in today's business environments. It is compelling for several reasons, including:

- Increasingly complex and demanding IT environments
- Growing number and sophistication of control measures required for managing information security
- Resource constraints and shortage of cybersecurity talents
- Customers and business partners' expectations of compliance with regulatory requirements and best practices in information security management.

Without maintaining a good risk register, managing risks is like chasing shadows

Overview

With leading assessment tools, methodology, and expertise we provide you with security assessment(s) to measure, communicate, and mature your cybersecurity and compliance efforts. What you will get includes:

- Comprehensive report of your current security posture
- Roadmap for closing any gaps to improve your overall security posture
- Tool for tracking improvement to your security program in real time.

We provide assessment for leading frameworks and standards, including NIST 800-53, SOC 1,2,3, CMMC, CCM, CIS, HIPAA, PCI-DSS, ISO 27001, and GDPR.

The most critical step in information security management is understanding the risks to organization's information assets through a simple, comprehensive, credible, measurable, and easily understood information security risk assessment. This is the type of assessment solution we offer. We use assessment solution called S2Org, explained in further details in the following sections.

S2Org is a credible, measurable, and easily understood cybersecurity risk assessment solution developed and maintained by SecurityStudio. We have partnered with SecurityStudio to leverage their proprietary assessment solution (S2Org) as part of our resources portfolio to provide excellent assessment services to our clients.

Information security is a proactive management and governance of risks of unauthorized disclosure, modification, and/or destruction of an organization's information assets using operational, physical, and technical controls.

SCHEDULE A DEMO

The following sections provide summarized features of S2Org assessment solution.

Features

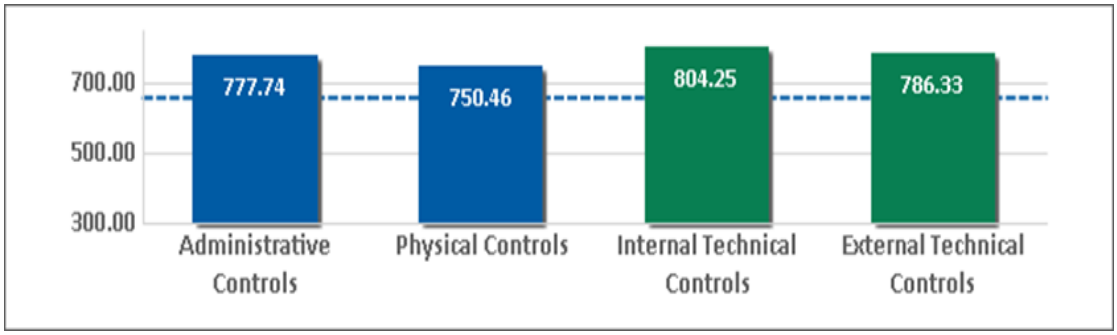
The assessment solution is equiped with indispensable features for a value-adding and actionable assessment result. Those features include:

Simple

Complexity is the worst enemy of security. S2Org removes all unnecessary complexity by maintaining focus on cybersecurity fundamentals. Most cybersecurity incidents and breaches occur because of missing or malfunctioning fundamentals.

Comprehensive

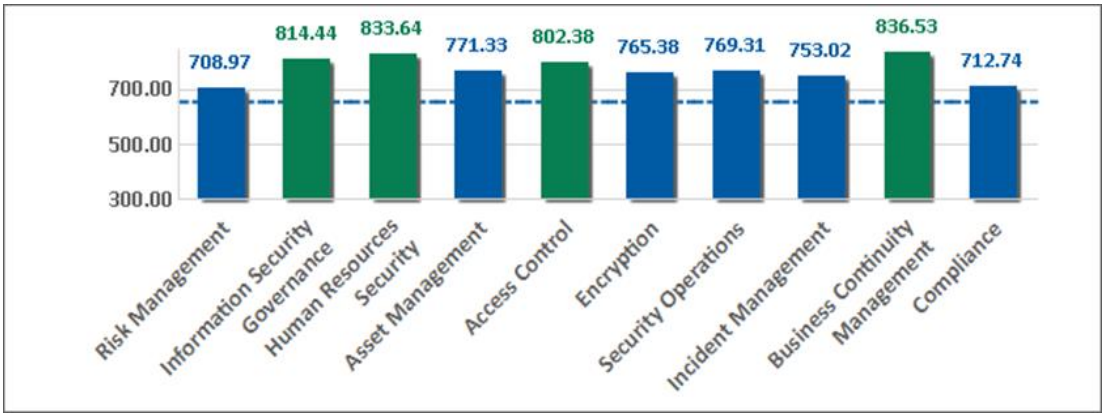
Simplicity is at the core of S2Org, but not at the expense of cutting corners. S2Org assesses risk across four phases, in accordance with our definition of information security, and everything is objectively measured using the S2Score, as depicted in the sample chart below.



S2Org's four areas (phases) across which risks and controls are assessed are discussed briefly in the next section.

Administrative Controls

Controls in this category provide governance, context, and direction for your information security investments. These controls are sometimes referred to as "operational" or "people" controls. Within S2Org, there are ten control families (or topics) in this category as shown in the table below:



When organization don't take the time to map controls to the risks and the compliance requirements they address, it's easy to create duplicative controls, resulting in an expensive inefficiency

Cybersecurity is NOT an IT only issue, it is an organizational issue; therefore, focusing on technical controls only is ineffective.

SCHEDULE A DEMO

When risks are not managed in an integrated fashion, things fall through the cracks

The maturity, S2SCORE, Score Description, and Grade for each section in a sample assessment is summarized in the following table.

Control Section	Maturity	S2SCORE	Description
Risk Management	4.00	708.97	Good
Information Security Governance	4.51	814.44	Excellent
Human Resources Security	4.57	833.64	Excellent
Asset Management	4.29	771.33	Good
Access Control	4.60	802.38	Excellent
Encryption	4.50	765.38	Good
Security Operations	4.26	769.31	Good
Incident Management	4.03	753.02	Good
Business Continuity Management	4.75	836.53	Excellent

Physical Controls

These controls are often overlooked within the context of cybersecurity, but they're used to prevent physical damage or theft to your information assets. The table below shows the four control families in this category within S2Org.

There are four (4) sections within physical location. The four (4) sections within the Physical Controls assessment are further divided into fifteen (15) controls. The Maturity, S2SCORE, Score Description, and Grade for each section in a sample assessment is summarized in the following table.

Control Section (Headquarters)	Maturity	S2SCORE	Description
Crime Index	N/A	555.97	Poor
Natural Disasters	N/A	557.00	Poor
Facility Security	4.30	782.20	Excellent
Equipment and Information	4.46	796.29	Excellent

Internal Technical Controls

Within S2Org, technical controls are separated into two categories "internal" and "external". Internal technical controls are primarily focused on information protection after a technical perimeter has been crossed (or breached). Within S2Org, there are nine covered sections (or topics) in this category as listed in the table below.

The maturity, S2SCORE, Score Description, and Grade for each section in a sample assessment is summarized in the following table.

Control Section	Maturity	S2SCORE	Description
Network Connectivity	4.25	792.04	Excellent
Remote Access	4.16	782.06	Excellent
Directory Services	4.26	798.54	Excellent
Servers and Storage	4.44	721.74	Good
Client Systems	4.64	819.65	Excellent
Mobile Devices	4.38	787.32	Excellent
Logging, Alerting, and Monitoring	5.00	850.00	Excellent
Vulnerability Management	4.44	823.46	Excellent
Backup and Recovery	5.00	850.00	Excellent

In addition, S2Org can process and risk-rate (score) vulnerability scan data. The risks discovered from such scan data are put into context for the related risk sections.

SCHEDULE A DEMO

Compliance remains a compelling driver for information security investments.

External Technical Controls

These controls are primarily focused on the public "footprint" of the organization (meaning the systems and services the organization makes available to the public) and how the organization is keeping attackers out. There are four sections in this phase of S2Org as shown in the table below.

The maturity, S2SCORE, Score Description, and Grade for each section in a sample assessment is summarized in the following table.

Control Section	Maturity	S2SCORE	Description
Best Practices	3.72	662.98	Good
Reconnaissance	1.43	471.88	Very Poor
Enumeration	5.00	850.00	Excellent
Vulnerabilities	5.00	850.00	Excellent

The four (4) sections within the External Technical Controls assessment are further divided into six (6) controls.

Relying on only a snapshot of security posture at a point in time to meet compliance requirements is not sufficient to assure security – Continuous Monitoring is the best practice

Credible

S2Org is used by more than 5,000 organizations across industries in the private and public sectors to manage risk in the most effective manner possible. S2Org has held up to regulatory scrutiny in healthcare, financial services, and critical infrastructure, among many others.

S2Org is based on National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and the controls are mapped to all major industry standards, including:

- ISO 27002:2013
- NIST SP 800-53
- CIS Controls
- Others

Cost Effective

Compliance remains a compelling driver for information security investments. S2Org is used to aid and justify compliance for multiple regulatory security requirements, including:

- HIPAA
- GLBA/FFIEC
- CMMC
- Others

S2Org provides a foundational building block for cost-effective and sustainable information security programs that drive business and demonstrate compliance.

Measurable

Everything in S2Org is measured using the S2Score algorithm. The S2Score is a definitive measurement of information security risk calculated within the range of 300 and 850, and weights are applied based upon current real-world threats, as depicted in the figures on the next page.

As mentioned, S2SCORE is calculated in a range from 300 to 850. The lower the score, the higher the risk. And vice versa. A S2SCORE of **660.00** or "**Good**" is acceptable to most organizations and should be the minimum goal for any Company.

SCHEDULE A DEMO

Regulatory and industry compliance requirements are increasing, and IT environments are increasingly becoming more complex

S2SCORE Scale

S2SCORE Average Across Industries

Industry: Offices of Other Health Practitioners(6213)

The average self-assessment S2SCORE is **697.46** for Offices of Other Health Practitioners(6213). According to our calculations, there is roughly 12.3% less risk in the Test ABC Company Inc information security program than other programs in similar organizations.

Easily Understood

Information security is not a native language for most people, especially executive management personnel who are tasked with making prudent risk decisions. S2Org translates information security jargon into plain English for non-information security professionals. This serves the purpose of the business, but also allows personnel with varying degrees of expertise to work from the same playbook. At the highest level, the S2SCORE is organized into Phases, Sections, and Controls:

Phases

There are four phases (as alrady discussed): Phase 1 - Administrative Controls, Phase 2 - Physical Controls, Phase 3 - Internal Technical Controls, and Phase 4 - External Technical Controls.

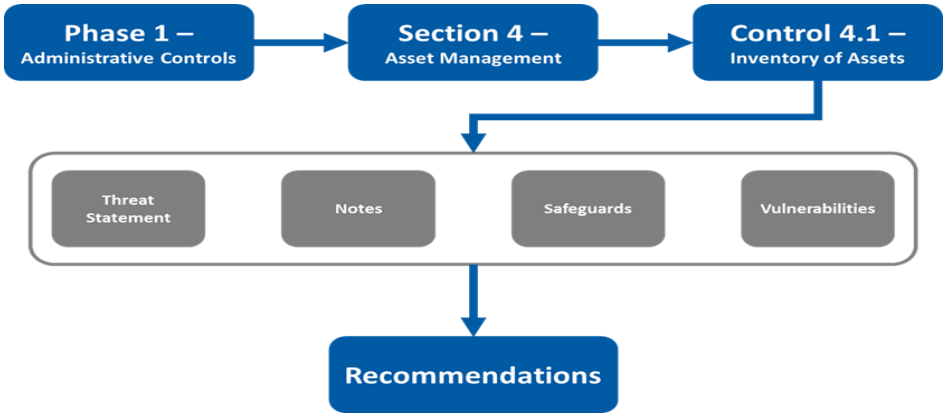
Sections

Each of the four phases is divided into one or more control sections. Phase 1 - Administrative Controls for instance is divided into ten (10) control sections.

Controls

Each of the control sections is further divided into one or more controls. As an example, let's look at the controls within the Phase 1 - Administrative Controls, Section 4 - Asset Management. There are four controls within the Asset Management section. They are: 4.1 Inventory of assets, 4.2 Classification of information, 4.3 Management of removable media, and 4.4 Disposal of media

The reporting structure looks like this:



SCHEDULE A DEMO

There continues to be shortage of cybersecurity talents, while bad actors are becoming more sophisticated with their attacks

Threat Statements
Threat statements apply whenever and wherever there are gaps in a control. If there are no gaps in a control and there are no "vulnerabilities" cited (see: Vulnerabilities below), then the threat statement does not apply.

Notes
The notes cited for a control contain the Information Security Analyst's observations about the control, and often reflect the positive aspects of the information security program related to the control. Note statements are often positive.

Safeguards
Safeguards are protections implemented to support a control objective and reduce risk. Some safeguards have a more significant impact on the S2SCORE than others. Safeguards are put in place in response to a known risk and represent the results of a successful information security program. Safeguards are positive and demonstrate a commitment to reducing risk.

Vulnerabilities
Vulnerabilities are the gaps in a control where there is risk. Some of the vulnerabilities have a more significant impact on the S2SCORE than others. Vulnerabilities often focus on the negative aspects of the information security program related to the control.

Recommendations
Each vulnerability statement cited in the report must be accompanied by a recommendation. The implementation of the recommendations cited for the control will all have a significant positive impact on the S2SCORE associated with the control.

Deliverables

The following deliverables are provided as part of the S2Org Information Security Risk Assessment:

Executive Summary Report – Customized report of assessment results for executive management and/or board of directors' consumption. This concise report summarizes all the assessment activities and findings, bringing attention to only the top five recommendations in each phase.

Full Report – A very detailed report containing all controls, findings, recommendations, and technical data supporting S2Scores. This report is generally used by operational personnel who will be engaged in developing road maps and remediation.

Action Plan – The data from the Full Report in .csv format. The Action Plan is useful for offline sorting of assessment results and import into other database systems.

NIST CSF Report – A very detailed report, correlating all assessment activities, findings, and recommendations to the NIST CSF. This is a helpful report for organizations who have chosen the NIST CSF as their framework for managing information security.

Vulnerability Scan Risk Report – Technical data report showing the risks related to all vulnerabilities discovered during vulnerability scanning. This report is useful for personnel who are engaged in patching and configuration management

Optional Deliverables

CMMC Readiness Report (if requested) – CMMC stands for the "Cybersecurity Maturity Model Certification" developed by the Office of the Under Secretary of Defense for Acquisition & Sustainment for Department of Defense (DoD) purchasing.

Assessment Notes and Evidence (if requested) – notes written by our assessor and evidence collected during the assessment.

Next Step

Our team of experienced consultants will provide necessary assessments, invaluable insights, recommendations, and support you need. Give us a call or schedule a demo to get things started.

SCHEDULE A DEMO