Understanding a NIST CSF Security and Risk Assessment
by Tom Kirkham, Founder and CEO, IronTech Security

The National Institute of Standards and Technology (NIST) offers risk assessment guidelines that can provide senior leaders and executives with the information they need to understand and make decisions about their organization's current information security risks and information technology infrastructures. Risk is the likelihood of a threat event's occurrence and potential adverse impact should the event occur

Risk assessments are an important tool for managers. With 30,000 websites hacked daily, and 64% of companies worldwide having experienced at least one form of a cyber attack, risk assessments provide important information to guide and inform the selection of appropriate defensive measures so organizations can respond effectively to cyber-related risks.

If any of these four scenarios apply to an organization, a risk assessment is in order:
1) The organization relies on an IT specialist for cybersecurity. Cybersecurity is not an IT job. It is a security job. They have different objectives.

2) Antivirus such as Norton, McAfee, or Bit Defender is the sole form of protection. This simply provides a false sense of security. Antivirus is essentially useless.

3) Company leaders who must educate and justify protection to a general manager, managing partners, board of directors, or a governing authority. Unbiased, the assessment will clearly show where vulnerabilities, where risks lie.

4) Believing a cyber attack will not happen. Organizations of all sizes are at risk. No one is too small. Hackers use automation so size becomes irrelevant for return on investment.

The ultimate objective is to protect all stakeholders. It goes beyond the organization, employees, and vendors. For many, it could be the community, the state, or a region of the country. Everyone an organization touches is a potential stakeholder.

How a NIST CSF Risk Assessment Works
Risk, and its contributing factors, can be assessed in a variety of ways. Quantitative analysis supports cost-benefit analyses of alternative risk responses or courses of action. Qualitative methods assess risk using categories or levels (very low, low, moderate, high, very high). This type of assessment supports communicating risk results to decision makers. Finally, semi-quantitative assessments typically employ a set of principles for assessing risk that uses bins, or representative numbers.

The National Institute of Standards and Technology first provided a Cybersecurity Framework in 2014 and updated it in 2017. Outlining standards, guidelines, and practices to promote the protection of critical infrastructure, the NIST Cybersecurity Framework applies to businesses of every size. It gives guidance on managing and reducing cybersecurity risk. What it does not do is provide advanced state-of-the-art administrative controls or technical controls. This is why an Infosec specialist should play an important role on the team. An Infosec specialist will understand the vulnerabilities revealed in the risk assessment and recommend best of breed technology for protection.

The NIST Framework is composed of five functions: Identify, Protect, Detect, Respond, and Recover. The risk assessment occurs in the Identify stage.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

A new NIST publication, *Guide for Conducting Risk Assessments*, focuses exclusively on risk assessment. The guidance covers the four elements of a classic risk assessment: threats, vulnerabilities, impact to missions and business operations, and the likelihood of threat exploitation of vulnerabilities in information systems and their physical environment to cause harm or adverse consequences. Even the questions themselves directly correlate to one of those five categories, and it lists them as critical, high, medium, or low.

In the “Identify” stage the initial assessment occurs. By answering questions the Infosec specialist asks, the state of the system is revealed. Expect to examine how many machines are involved, who the email provider is, what current protections are in place, and the organization’s security maturity.

The organization’s security maturity is also examined. Do people reuse passwords? Are passwords shared among a team? Is there one account for the website, or does each involved team member have a unique account? If the answer to any of those questions is yes, then the assessment will call for security awareness training and most likely a password manager as well.

The Infosec specialist should be expected to quickly provide a follow-up report that maps directly to the NIST 800-53 requirements.

There are informative references where all other standards, both national and international – International Standards Organization (ISO), COBIT, CIS and NIST can be studied. For example, awareness and training directly tie to ISO 27001 specifications developed in 2013 (see below).

	Category	Subcategory	Informative References
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their	**CIS CSC** 5, 17, 18

Once identified, weaknesses can often be addressed immediately by changing some basic business policies even before cybersecurity awareness training happens. Suddenly, the risk of a breach is cut in half.

Part of the process will center on determining who the threat actors are. For businesses, most often they are criminal hackers. Any part of the critical infrastructure such as the power grid or water supply face serious threats from nation-states because their goals lie in harm and disruption as well as monetary gain.

Steps Beyond the Risk Assessment

Both initial and ongoing assessments lead an organization to the defensive controls that must be put in place.

As risk assessments are updated and refined, organizations should use the results to update the risk management strategy, incorporate lessons learned into risk management processes, improve responses to risk, and build a solid foundation of threat and vulnerability information tailored to organizational missions/business functions.

The White House National Security Office offers recommendations for five steps organizations can take to protect against ransomware attacks:

1) Multi-factor authentication. This calls for a third credential, typically a six or eight digit random number that is generated. It is time-sensitive and is information a hacker can't access.

2) An endpoint detect and response platform (EDR). EDRs use artificial intelligence and machine learning to monitor what the computer is doing. Unlike an antivirus tool, it does not look for a virus signature. Ransomware has no virus signature identify it. EDRs examine what is happening on the device. If it detects an Excel spreadsheet starting a macro that calls the Windows encryption service, it stops it because it knows that is not usual behavior. EDRs learn from experience. If an anomaly is occurring, it can quickly be investigated by skilled Infosec specialists.

3) Utilize disk encryption. All data for the organization should be encrypted, especially portable devices.

4) Form a *skilled* security team. This is not the organization's IT team. The security team should be comprised of professionals who understand cybersecurity and it entails. This team does not replace IT, it serves a completely different purpose. Many organizations are establishing the role of Chief Information Security Officer (CISO). A CISO is responsible for establishing security strategy and ensuring data assets are protected. CISOs traditionally work alongside the chief information officer (CIO) to achieve information security goals. All leaders need to buy in completely. It is their role to set the tone by walking the talk. Go through superficial motions will not protect the organization.

5) Share and incorporate threat into defenses. Understand what's going on in the criminal, nation-state, and terrorist worlds to stay up-to-date on defenses. The skilled security team must be charged with this task every day. They must read all alerts which can be dozens a day, and analyze them asking, "Is that a threat to any of our clients? Do we need to respond right now?"

Insist on best of breed products and services and even the administrative controls/procedures. The Infosec team should be researching changes in policy, hold discussions with peers. If it makes sense, we'll make the change. If we find a better EDR, we rip and replace. Best of breed everything.

Lastly, embrace Security Orchestration Automation Response (SOAR). This is orchestration of everything through an Infosec Command Center - the automated response and the human response. At times, attacks require additional skillsets from sources including vendors. It is not unusual to call upon multiple vendors on a single attack. Practicing SOAR means having all resources at the ready at all times.

In the final analysis, solid security means committing to a security first environment. Organizations must move beyond believing security is a hassle to set up, deploy, and use. The ultimate goal is to minimize the threat vectors.

About the Author
Tom Kirkham is founder and CEO of Kirkham IT. Tom founded IronTech Security to focus on cybersecurity defense systems that protect and secure data for the financial, law, and water utility industries. IronTech focuses on educating and encouraging organizations to establish a security-first environment with cybersecurity training programs for all employees to prevent successful attacks. Tom brings more than three decades of software design, network administration, and cybersecurity knowledge to the table. During his career, Tom has received multiple software design awards and founded other acclaimed technology businesses. He is an active member of the FBI's Arkansas InfraGard Chapter and frequently speaks about the latest in security threats. Watch for Tom's new book: The Cyber Pandemic Survival Guide - Protecting Yourself From The Coming Worldwide Cyber War.

December 6, 2021