Risk Assessment Toolkit

HIMSS Security Risk Assessment Guide/Data Collection Matrix

Introduction
One of the major challenges of provider organizations is meeting the required level of security. Keeping current with standards like HIPAA and HITECH is difficult. Even more so, the expense related to keeping current leaves no room for misunderstanding the standards and doing too much or too little. In addition, the reality in many provider organizations is that the responsibility for security may be assigned to individuals with many other duties and little time to develop the needed security program.

The purpose of this document is to help organizations address one particular security implementation specification —the requirement for a Risk Assessment. The HIMSS Security Risk Assessment Guide/Data Collection Matrix is a framework that an internal risk assessor can use to conduct a standards-based organizational information security risk assessment. The guide/data collection matrix is relatively basic and is intended as a starting point. But while it is only a starting point, getting started may be the most important step.

A couple of assumptions were made by the authors1 of this guide/data collection matrix. The intended audience has at least some basic knowledge of risk management, HIPAA, HITECH, the CMS EHR Incentive program, information technology, security and privacy. In addition, the user is in a position within the organization to gather needed resources to participate in the effort. This is not a one-person task; it will take a core team and will involve participation from all aspects of your organization.

Instructions
There are numerous worksheets (tabs) in the Security Risk Assessment Guide/Data Collection Matrix. Used together, the tabs can walk a team through a step-by-step process to identify threats and vulnerabilities, evaluate the likelihood of occurrence and impact, categorize and prioritize risk, establish mitigation strategies, assign responsibility and then report the findings and recommendations to leadership.

In many of the worksheets, sample data is provided to illustrate intended usage. The sample data is in red. Be sure to delete the sample data before entering your data.

---

1 The authors of this document include members of the HIMSS Risk Assessment Work Group – a HIMSS member/volunteer group dedicated to creating useful tools and resources for HIMSS members. A list of work group members can be found in the "Work Group Contributors" section at the end of the document.
**First Three Tabs: Threat Sources, Threat Events (Adversarial), Threat Events (Non-Adversarial)**

The first three tabs give the risk assessment team some understanding of security threats. Threats to a healthcare organization come from numerous sources, internal and external to the organization. The first step in assessing security risk is to understand the threats that create the risks. The use of this guide will help the team evaluate the obvious and subtle threats to their organization. The team must walk through an identification of threats before taking the next steps² (Hare, 1851).

The threat worksheets (first three tabs) provide definitions for “threat”, “threat source” and “threat event”. Take the time to understand the definitions and to read through and evaluate the threat sources and threat events (adversarial and non-adversarial). Make some judgments about which types of threats are most relevant to your organization. It helps to review documentation of security and privacy incidents that have occurred in your organization over the past several years. The team may also wish to do some research about the types of threats that have impacted other organizations. Finally, additional resources on threats can be found in the Risk Assessment Toolkit.

**Fourth Tab: Vulnerabilities**

The next tab provides a definition and simple examples of common vulnerabilities. The list is not comprehensive. However, the team will build upon these examples to examine how identified threats may exploit vulnerabilities in the organization. A “vulnerability” is a flaw or weakness in security procedures, design, implementation, or internal controls that could be exploited (accidentally or intentionally) and result in a security breach or a violation of the organization's security policy³ (NIST SP 800-30). Vulnerabilities are found not just in information systems but in many other aspects of the organization. Vulnerabilities are even found in third-parties that provide services to the organization. Therefore, after conducting a comprehensive identification of threats and vulnerabilities, the team will have identified risks not only in its information technology, but in many other aspects of the organization such as in governance, third party practices, policies, processes, training, and culture. It will have identified risks to all three objectives of security:

- **Confidentiality** (ePHI is accessible only by authorized people and processes)
- **Integrity** (ePHI is not altered or destroyed in an unauthorized manner)
- **Availability** (ePHI can be accessed as needed by an authorized person)

**Fifth Tab: Likelihood, Impact, Risk**

A key step in a risk assessment is prioritizing the threats and vulnerabilities. Of course, no organization can afford to focus scarce resources on every threat and vulnerability. These must be prioritized according to their importance to the organization⁴ (Harris, 78). With respect to the organization’s mission and leadership imperatives, the team must conduct an evaluation of likelihood, impact and risk. A framework for this effort is described in the tab named “Likelihood, Impact, Risk”. The team should take the time to familiarize itself with these definitions and scoring schema as they will use them to evaluate and score each vulnerability. The scoring may be more subjective than objective. That is expected. But, for all findings, a risk level must be determined with input from clinical and business leadership. Keep in mind that the

---

purpose in assessing the level of risk is to guide decisions about allocation of resources (human and financial) to take necessary steps to mitigate (reduce) risk.

**Sixth and Seventh Tabs: Application Inventory, Hardware Inventory**
The next two tabs are related and extremely important. Each is an inventory of assets within the information technology portfolio. The knowledge of what information technology exists in an organization is vital to any good information security program. These worksheets will guide the team through a detailed inventory process by asking the right questions, gathering valuable information, and resulting in a full assessment of the location, condition, and inter-relatedness of all information technology assets that store, process or transmit electronic protected health information (ePHI).

One piece of information worth noting is that these inventory spreadsheets capture information about biomedical devices and systems as well as equipment and systems that are more traditionally identified with healthcare information technology. While biomedical devices and systems present unique challenges due to the impact of FDA certification and the reality that there are important life safety considerations, the security impact of biomedical devices and systems cannot be overlooked. The risk assessment required by the HIPAA Security Rule is concerned with identifying all risks to Protected Health Information (PHI) in electronic form; whether that means PHI on a backup tape, in an EHR database, a copy machine, a smartphone or a biomedical device such as a sonogram or EKG machine.

**Eighth Tab: Score Card Definitions**
The next tab is called “Score Card Definitions”. This spreadsheet gives the HIPAA requirements and more detail about each required safeguard. The first column of this spreadsheet matches the safeguards listed on the Security Score Card tab. For each HIPAA standard and specification it lists 1 – 4 controls that are relevant.

There is a short description of each control and then a more detailed explanation. The shorter description is numbered. The numbered short descriptions are the controls across the top of the “Security Score Card” tab. When filling out the score card, if more information about a particular control is needed, you can turn to this tab, find the control and read the longer explanation and the corresponding HIPAA requirement.

**Ninth Tab: Security Score Card**
The Security Score Card has about 80 safeguards or controls across the top. It is a tool to evaluate the adequacy of security measures for 1) the organization as a whole, 2) each department and 3) each application. All of the required safeguards should be scored for the organization as a whole. For each department and each application score only the unshaded areas. Each required safeguard is to be scored 0-4.

- 4 indicates full compliance in terms of practice and written policy or standard
- 3 indicates the practice is fully compliant, but no policy or standard is in place
- 2 indicates the practice is not fully compliant, but a policy or standard is in place
- 1 indicates partial, but very inadequate compliance
- 0 indicates complete non-compliance
In the Security Score Card, there are 3 sections. The blue section allows the organization as a whole to be scored against all of the controls, the brown section is to score each department against the controls that relate to departments, the green section is to score each application against the controls that relate to applications. The columns that are shaded brown and green in the department and application sections indicate questions that may not be relevant to departments and applications and therefore may not need to be scored.

**Tenth Tab: Risk Assessment Report**

The final tab, "Risk Assessment Report" provides a template to document findings. It also organizes the necessary processes of identifying the vulnerabilities and threats, evaluating the likelihood of occurrence and the impact to the organization and then, determining the risk level for each vulnerability. The form guides you through assigning a business or clinical process owner for each risk and its mitigation. There is no reason to identify and measure these risks and then have no accountability to finish the job. Each column of the spreadsheet is a component of the risk assessment and the process of remediating the issues. Instructions are provided in each column, along with examples to help clarify the purpose of each column.

**Presentation to Leadership**

Finally, the Risk Assessment report should be presented by your team to the leadership of your organization. That may begin with a presentation to a committee that provides governance over privacy and security or to a compliance committee or an IT committee. But a presentation should also be made to the organization's broader executive leadership. Management of risk in any organization should be overseen by executive leadership. Responding to the risks may require extensive changes in policy and practice. Investments in capital and human resources may be needed to reduce certain risks.

**Additional Resources**

**Suggestions on working with an security professional**

What if an organization doesn't have the required skills or knowledge needed to conduct a risk assessment? HIPAA makes it clear that a risk assessment is necessary. While the resources provided in the HIMSS Risk Assessment Toolkit\(^5\) can go a long way to guide one through the process, adequate knowledge of the HIPAA security requirements and information security risks and standard safeguards is needed. If the knowledge is lacking the only alternatives are for someone in the organization to gain the needed skills and knowledge and then conduct the risk assessment or to work with an outside organization to help with the risk assessment.

For many, working with an outside security professional may be the best choice. However, the organizational leadership must still take ownership of the risk assessment and ensure that risks are not only identified, but adequately addressed. While some security risks are technical in nature and can be addressed by a consultant many security risks are not technical but are cultural, dealing with the behavior and practices of the workforce. An outside security professional can facilitate the identification of these risks but can do little to resolve them.

When working with an outside security professional here are a few suggestions to identify a good assessor:

---

\(^5\) [http://www.himss.org/riskassessment](http://www.himss.org/riskassessment)
• Consider contacting your nearest Regional Extension Center for references or advice on selecting a vendor. You can find your Regional Extension Center here: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3519

• Look for a credentialed security professional that has experience in healthcare risk assessments. While there are many valid security credentials the most well-respected include:
  o CISSP: Certified Information Systems Security Professional and others from ISC2 www.isc2.org
  o CISM: Certified Information Security Manager; CISA: Certified Information Systems Auditor; CRISC: Certified in Risk and Information Systems Control and others from ISACA www.isaca.org
  o CSF Assessor: Common Security Framework Assessor from HITRUST www.hitrustalliance.net
  o CIPP: Certified in Information Privacy Professional from IAPP www.privacyassociation.org
  o CEH: Certified Ethical Hacker from EC-Council www.eccouncil.org
  o GIAC certifications: Global Information Assurance Certifications (Various targeted areas of information assurance) www.giac.org

• Look for documented past performance (check references)

• Review sample deliverables. Look for thoroughness and concrete, actionable recommendations

• Ensure that the scope of the risk assessment matches the HIPAA requirements. The HIPAA requirement for a risk assessment is found at 45 CFR 164.308 (a)(1)(ii)(A) and states:

  Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

• A risk assessment should include at least the following elements:
  o A complete HIPAA security compliance evaluation
  o Evaluation with respect to the HITECH requirements, especially the data breach notification requirement
  o Technical evaluation – such as a vulnerability assessment and a review of technical controls such as firewalls, wireless configuration, web servers and antivirus tools
  o Administrative assessment – look at policies and administrative controls required by HIPAA
  o Assessment of each application and system that stores, processes or transmits ePHI including biomedical devices
  o Assessment of the practices of each department that uses or discloses ePHI
  o Evaluation of all three objectives of information security:
    ▪ Confidentiality
    ▪ Integrity
    ▪ Availability
Conclusion
The authors of this Security Risk Assessment Guide/Data Collection Matrix intend this to be a complement to the broader focus of the HIMSS Privacy and Security efforts, as well as a resource to provider organizations of all sizes that are seeking to develop an effective approach to risk assessment. One of the most crucial components of an effective privacy and security program will certainly be a Risk Assessment of the organization. ARRA and Meaningful Use have emphasized its importance by requiring a Risk Assessment as a Core Measure in Stage 1 attestation⁶ (HHS, 42745). But again, many, provider organizations lack the ability to provide full-time dedicated risk assessment resources. And when they are able to assign personnel to come together as a risk assessment team, where do they start? The documents related to this introduction paper are intended to be that first step on a long and highly important journey in managing security risks and protecting patient privacy.

Work Group Contributors
The HIMSS Risk Assessment Toolkit and the HIMSS Security Risk Assessment Guide/Data Collection Matrix were developed by the HIMSS Risk Assessment Work Group. Contributors include:

Work Group Chair
Jeffrey Bell, CISSP, CPHIMS, ACHE
CareTech Solutions

Work Group Members
Nasrin Barbic
George Washington University Hospital

Margaret Bond, MSc, MBA, CISM, CRISC, CHS-V
IASIS Healthcare

Anatoly Elberg
Paranet Solutions, LLC

Sharon Finney CISSP, CISM
Adventist Health System

Nicholas Heesters, JD
Quality Insights of Delaware

Jerome Hesita
US Oncology

Bowe Hoy
Sword & Shield Enterprise Security, Inc.

Montra May, MBA
Georgia Department of Community Health

Glenn Mills, CIPP
Boilermakers National Funds

Sean Murphy, CISSP, CPHIMS, FACHE
SAIC

David Scott St Laurent, CISSP, CISA, CISM
Fallon Community Health Plan

Connie J. Sadler
Lucile Packard Children's Hospital at Stanford

Protik Sandell
Potomac Data Systems Corp.

Dennis M. Seymour, CISSP, PMP
Ellumen

James Sheldon-Dean BS, MS
Lewis Creek Systems, LLC

Thanh Tran
Ernst & Young

Louise Welch, CISA
Johns Hopkins University

Jason Zellmer
Kaiser Permanente