Simplified Risk Analysis

The following is a simplified sample of a combination qualitative and ranking approach risk analysis. It can be expanded upon as needed (refer to other attachments in this risk analysis policy/procedure/process document).

Risk Analysis Steps High Level:

- Review assets (hardware, software, data, facilities, etc.)
- Identify threats and vulnerabilities
- Evaluate existing security controls
- Assess likelihood
- Consider impact on organization
- Determine the risk

Asset Inventory:

- Review Data Systems
- Hardware (including portable hardware)
- Software
- Data storage locations (network, portable, shared storage, archiving and backup storage)
- Modes of data transit
- Data sensitivity
- Primary users (internal and external)
- Facilities
- Remote access assets (e.g., hardware, software, users)

Identify Threats:

- Natural/Environmental disasters
- Electrical storm, flood, tornado, chemical spill
- Human threats
- Accidental data entry or deletion
- Internal inappropriate access for personal use or out of curiosity
- Hackers, viruses, malware, theft, vandalism

Identify Vulnerabilities:

- Internal weaknesses or flaws (e.g., anti-virus signature file not updated regularly, data not backed up regularly, data backups stored at workforce member home, remote users communicating PHI unencrypted, etc.)
- Technical, physical, administrative
- Personnel (internal and external)

Sample Specific Threat Identification:

Physical

- Walk through office
- Develop and use walkthrough survey based on security rule physical security safeguards
- Visitor access
- Alarm systems

Administrative

- Presence or absence of policy/procedure
- Apply accountability to workforce
- Presence of training

Evaluate Security Controls:

Preventive

- Access restrictions (minimum necessary; internal and external)
- Authentication – passwords, biometrics, tokens
- Effective staff training
- Personnel management, background checks, work history
- Environmental controls

Detective

- Audit trails/audit programs
- Alarms – anti-virus applications, malware detection, intrusion detection, firewalls, etc.
- Assess Likelihood

Risk Matrix Creation:

- Threat source motivation, capability and vulnerability assessment
- Existence and effectiveness of current controls

Likelihood Threat/Vulnerability Realized:

This represents the first step in determining the risk level. Each threat/vulnerability and associated security control needs to be assed to determine the likelihood a threat or vulnerability will impact the practice. The likelihood will be assigned a value.

- High – controls required
- Medium – controls appropriate/balance against business requirements
- Low – controls if cost effective (if not, document)

Consider Impact:

The purpose of evaluating adverse impacts to the practice if threat is successful is the second step in determining the risk level.

Consider

- How important is the activity affected
- How critical is system or data to operations
- How sensitive is the data
- Other external adverse impacts (such as loss of business, civil suits, etc.)

Impact Description Examples

- Loss or degradation of any one or combination of integrity, availability or confidentiality
- Intangible or indirect impacts include:
- Lost revenue stream
- Repair/personnel costs
- Civil liability
- Public loss of confidence, credibility
- Data release/misuse
- Manipulation/corruption
- Temporary or permanent inaccessibility
- Temporary data erasure
- Backup copies available?
- Recovery of backed up data tested?
- Frequency and cost of each event

Magnitude of impact – Qualitative measures would rank impact as:

- High – controls required
- Medium – controls appropriate/balance against business requirements
- Low – controls if cost effective (if not, document)

Sample Risk Matrix:

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** **100 X 1.0 = 100**
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.05 = 25	**Medium** **100 X 0.5 = 50**
Low (0.1)	**Low** **10 X 0.1 = 1**	**Low** **50 X 0.1 = 5**	**Low** **100 X 0.1 = 10**

Risk Scale: High (>50 – 100), Medium (>10 – 50), Low (1-10)

Recommended Actions Based on Risk Level:

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation or finding is evaluated as a medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation or finding is evaluated as a low risk, the risk analysis team must determine whether corrective actions are still required or decide to accept the risk.

Interpretation of Risk Level:

(Risk scale represents the degree of exposure and possible actions needed to manage risk)

- Low Risk –
  - no action and accept risk
  - minimal action needed
- Medium Risk –
  - some response needed in reasonable time
  - look at controls
- High Risk –
  - take action now, urgency present
  - additional protections, new systems, new applications

Documentation:

Each step of a thorough risk analysis requires documentation ranging from documenting the inventory, documenting the threats, documenting security controls and so forth. At this point, it is important to document the risks that have been identified and related action to be taken. Even if Covered Entity elects to accept the risk because it is a low risk to the organization, it is important to document the fact that Covered Entity will accept the risk and why.

Also, for all risks which action is deemed necessary it is important to develop a thorough mitigation plan that includes these 5 essentials:

1. Risk and needed mitigation (e.g., policy/procedure change, adding new locks, increasing training frequency, technical solutions, etc.)
2. Mitigation time line (when mitigation will begin and end)
3. Necessary resources (staff and fiscal)
4. Desired end result
5. Review date to determine if mitigating action addressed identified risk

Risks to be mitigated should be prioritized – the highest risks addressed first. Also, if deviations from the initial mitigation plan are required, they need to be documented at the point of deviation. A review of the success of any mitigating action (or whether mitigation actually occurred) becomes one of the criteria that is part of the **annual compliance audit**.