Compliance: A Traditional Risk-Based Audit Approach

The Goal
The goal is to come up with a concise way to translate business and regulatory requirements into technology decisions.

Risk Management
Risk management begins with an inventory of the company's vulnerabilities.

A traditional risk-based audit approach to compliance identifies vulnerabilities in an organization's information systems and takes carefully reasoned steps to assure appropriate controls are implemented for all the components in the organization's information systems.

Controls operate within one or more of the commonly accepted information security principles:

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accountability
- Privacy

The primary deliverable from a traditional risk-based audit approach is a list of vulnerabilities, ranked by criticality of impact. Working from that list, we can assess options, estimate costs, weigh relative merits of options, and gauge the benefits from various control approaches.

Risk = Threat x Vulnerability x Total Cost

- Threat is the frequency of potentially adverse events.
- Vulnerability is the likelihood of success of a particular threat.
- Total Cost is all costs associated with the impact of a particular threat experienced by a vulnerable target.

Risk Analysis – What's Best to Audit?

To help facilitate security audits a Compliance Team should conduct an organization wide threat assessment and at minimum review the data collected on an annual basis. Updates to the collected threat assessment data would occur as new concerns arise. An example threat analysis of a specific entity may include the following areas of interest:

- Asset Value
- Environment Stability
- Controls
- Disaster Recovery
- Information Sensitivity
- Prior Audits
- Size and Complexity
- Management and Staff Input

For compliance to policies and regulations the decisions on what to audit are made based on the level of perceived risk and information gathered on the specific entities during the threat assessment efforts.

A purchased or homegrown Risk Assessment Database application provides a good mechanism that allows the team to rate and record each assessed entity by chosen factors. A rating of one (lowest) to five (highest) is given in each of these categories. A three is considered a medium rating. If no previous audit was present or the item was of average risk, then a standard rating is applied. In the example to follow the team has chosen 8 factors for each entity assessed and has agreed on the percentage of weighting.

Risk factors, their description and the weight given to each follows:

A. Asset Value 15%
This risk factor relates to the asset value of the entity being assessed. The asset value includes the criticality of the application / function to organization operations, size of the organization, etc. Asset value can range from little value to being a critical asset.

B. Environment Stability 15%
This risk factor relates to the level of change the assessed entity is currently experiencing. Environment stability can range from no change to significant change. Note that risks may also increase due to significant changes in policies, practices, and organizational structures, among others.

C. Controls 15%
This risk factor relates to the level of controls in place for an assessed entity. The level can range from no controls to many controls. Controls are the policies, practices, technologies and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. Management organization and involvement, monitoring activities, and user access controls are typically included when assessing this risk factor. Controls operate within one or more of the commonly accepted information security principles: Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability, and Privacy.

D. Disaster Recovery 10%
This risk factor relates to environmental factors that effect an assessed entity. Environmental risks include but are not limited to backup and recovery, power failure, fire, natural disaster, etc. Disaster recovery is used both in the context of data loss prevention and data recovery.

E. Information Sensitivity 10%
This risk factor relates to information sensitivity factors that effect an assessed entity. The more sensitive the information the higher the risk factor. The primary security audit focus is to proactively ensure that sensitive information is not inappropriately released and that regulations are upheld.

F. Prior Audit 10%
This risk factor relates to knowledge of the previous audit findings and history with the assessed entity. The risk factor may range from having a recent audit with favorable results to no audit performed within the past 2 years.

G. Size & Complexity 10%
This factor relates the risk of each assessed entity to its size and / or volume of activity. Size and complexity can range from being very small to very large in size and / or volume. The overall size of the assessed entity is important as the larger the entity, the more impact any corrective action could have. Complexity and the use of technology are also considered in this rating when assessing the entity.

H. Mgt & Staff Consensus 15%
Throughout the year, and particularly as we near the Audit Plan creation date, the Compliance Team solicits feedback from management and staff asking about their concerns. Their feedback is the basis for our ratings here.

Risk Analysis Formula:

Factor >> A B C D >>
Entity_1 Risk = (Rating * Weight) + (Rating * Weight) + (Rating * Weight) + (Rating * Weight) + etc.
Entity_2 Risk = (Rating * Weight) + (Rating * Weight) + (Rating * Weight) + (Rating * Weight) + etc.
Entity_3 Risk = (Rating * Weight) + (Rating * Weight) + (Rating * Weight) + (Rating * Weight) + etc.
…etc.

Example:

Factor >>	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**Risk Ranking**
Entity_1 Risk =	3(.15) +	3(.15) +	4(.15) +	5(.10) +	3(.10) +	2(.10) +	5(.10) +	2(.15) =	**3.3**
Entity_2 Risk =	5(.15) +	2(.15) +	5(.15) +	4(.10) +	5(.10) +	3(.10) +	4(.10) +	5(.15) =	**4.15**
Entity_3 Risk =	1(.15) +	4(.15) +	2(.15) +	2(.10) +	2(.10) +	4(.10) +	3(.10) +	3(.15) =	**2.6**

…etc.

Technology Audit Checklist

When determining what to audit don't overlook performing a detailed assessment of six key entity categories:

1. network security
2. content security
3. hosts security
4. identity management
5. application security
6. information management security

Once the vulnerabilities are identified from your audit findings the next step is to present them to IT management.

Company executives have four possible answers.

- Mitigate the risk - additional controls to safeguard or minimize impact or reduce probability
- Accept the risk - choose to do nothing
- Transfer risk - use other options such as insurance
- Monitor - watch risk to determine if significant safeguards become available.

It is best to get company executives to first agree that there is a problem and only when they ask to see their options, should you lay out the solution.

A good approach is to create a tier of service levels, **GOOD, BETTER and BEST**, etc. and spell out how each service level addresses the risk and what it will cost, so that the solution is directly linked to corporate policy and regulatory requirements..

For additional reference…

IT Compliance Institute:

The Global Authority for IT Compliance Information and Alerts
http://www.itcinstitute.com

The site provides some useful information including a searchable regulations database by industry. You'll also find information on the Unified Compliance Project (UCP). The UCP simplifies the multitude of complex regulations into a single holistic IT compliance view.

NIST Risk Assessment Summary of Activities:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

NIST Special Publication 800-30
Risk Management Guide for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

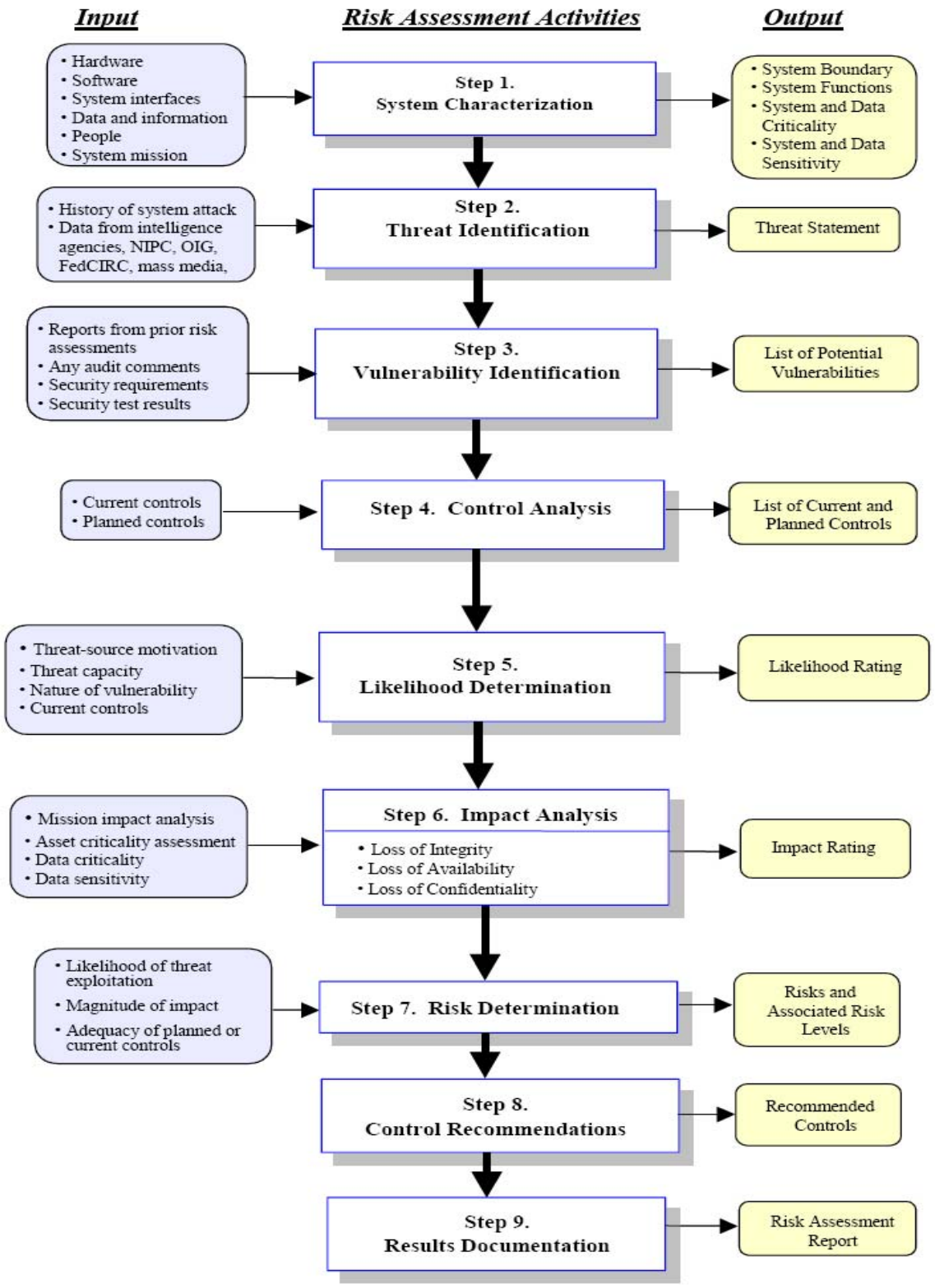

Figure 3-1. Risk Assessment Methodology Flowchart

NIST Special Publication 800-30
Risk Management Guide for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

HIPAA Security Rule Matrix

Appendix A to Subpart C of Part 164--Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see Sec. 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Regulations:

USA PATRIOT Act (USAPA)

- Effective 2001 - Activities deemed suspicious by law enforcement, ranging from book selections in public libraries to unusual cash transactions, may be the subject of investigations that require IT to track, interpret, and report on customer data.
- Requires businesses to provide customer information to law enforcement agencies with greatly relaxed restrictions on warrants
- Increased demands to detect and report suspected money-laundering activities

Gramm-Leach-Bliley

- GLB, GLBA, or Financial Modernization Act of 1999
- Requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information.

Sarbanes Oxley Act of 2002

- Passed in the wake of several corporate scandals and failures as an attempt to improve visibility into the financial management of public firms
- Section 302
  - Corporate responsibility for financial reports
- Section 404
  - Management assessment of internal controls
- Section 409
  - Real time issuer disclosures

HIPAA

- Health Insurance Portability and Accountability Act of 1996
- Provisions that establish national standards for electronic health care transactions, and mandate security and privacy for health care data.

NOTES: