



Safe  
Systems



# Simplifying the Risk Assessment Process

Presented By:  
Tom Hinkel, Director of Compliance  
Safe Systems, Inc.

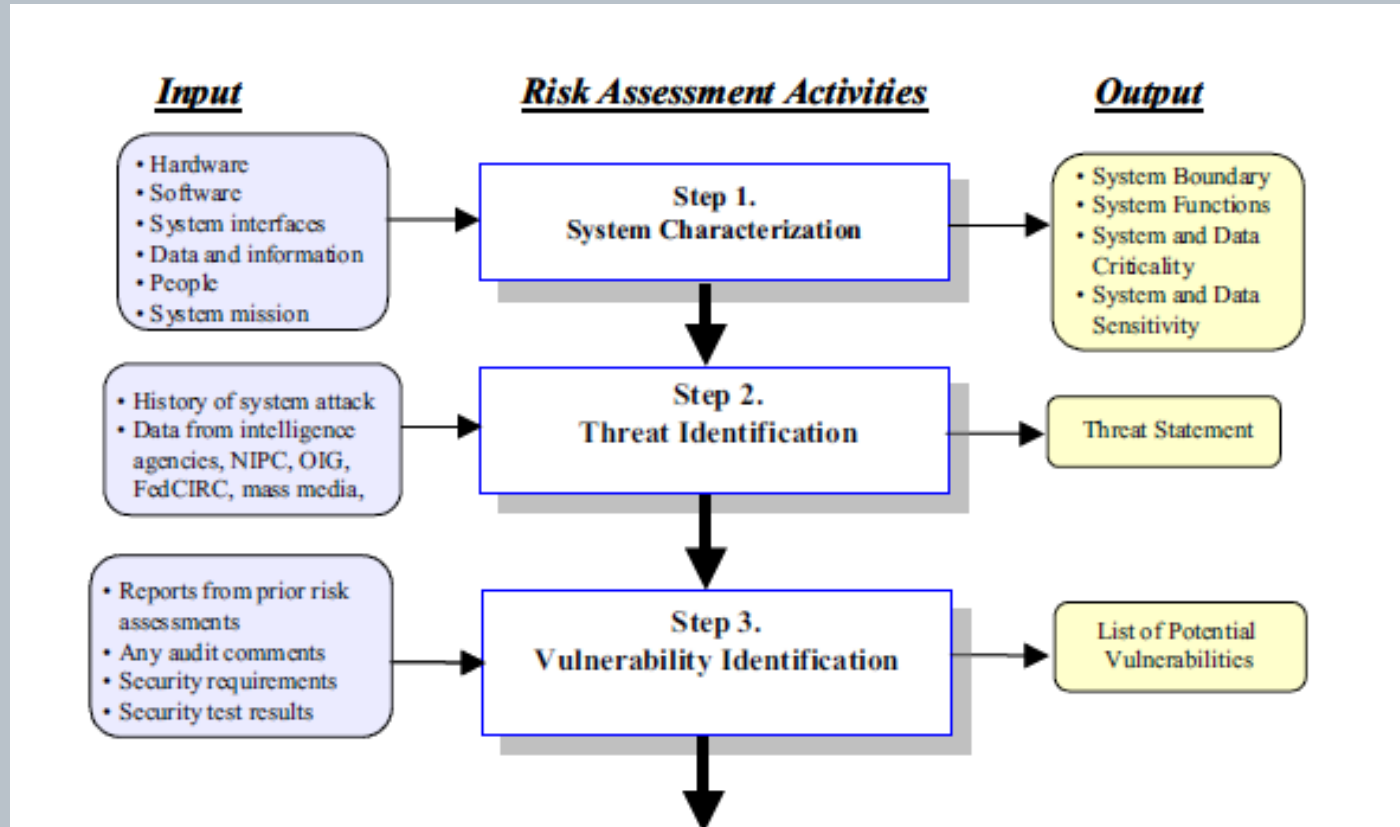
# Agenda

- Risk Management Trends
- Standardizing the Format
- The Control Self-Assessment

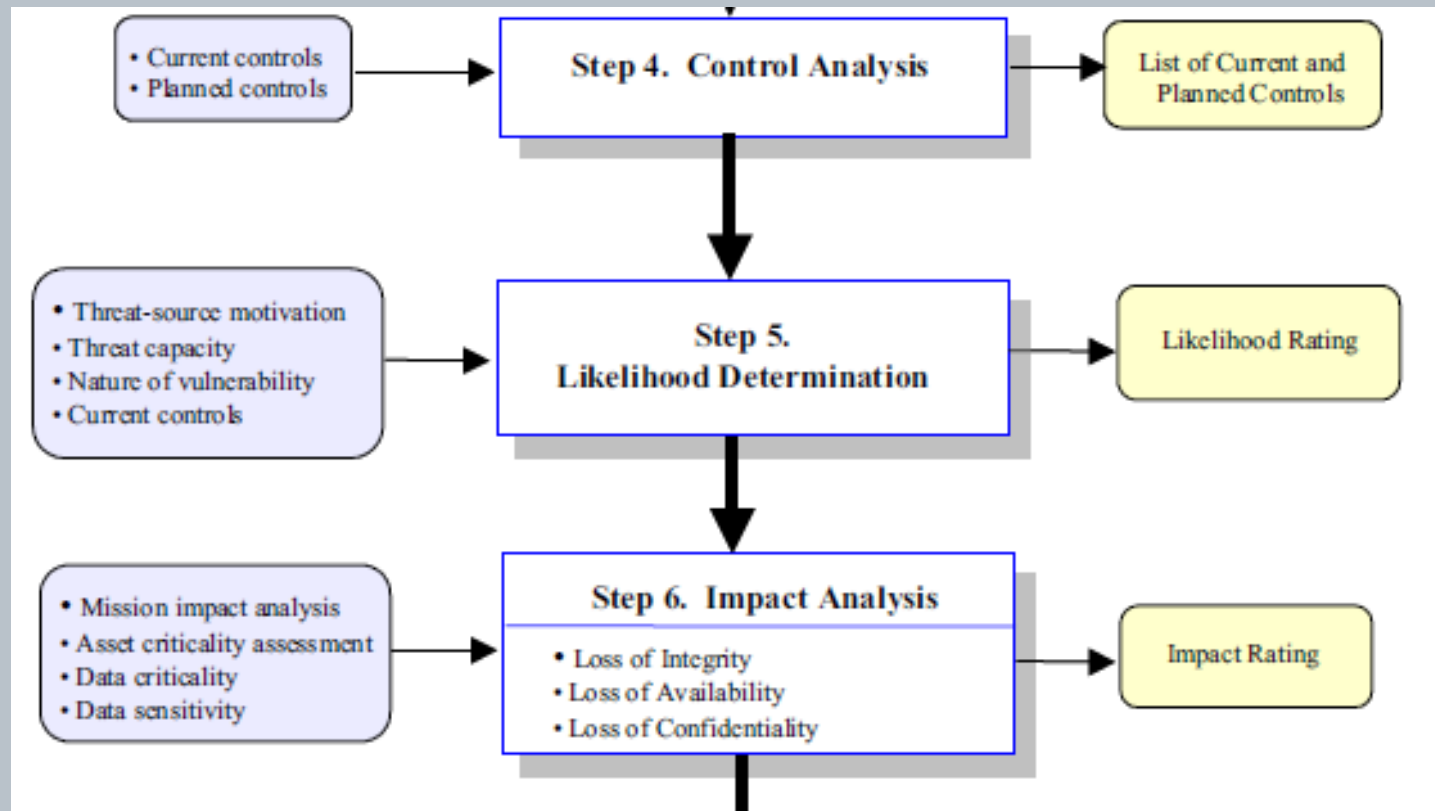
# The Risk Management Process

1. Risk Identification - Identify assets to be protected, or source of risk. To properly identify risks, a financial institution must recognize and understand existing risks or risks that may arise from new business initiatives. Risk identification should be a continuing process.
2. Risk Assessment - Identify threats and vulnerabilities to assets, evaluate the threat impact, & prioritize.
3. Risk Management - Apply controls designed to:
  1. Avoid/eliminate
  2. Reduce
  3. Transfer
  4. Retain (residual risk)
4. Test, train, re-evaluate.

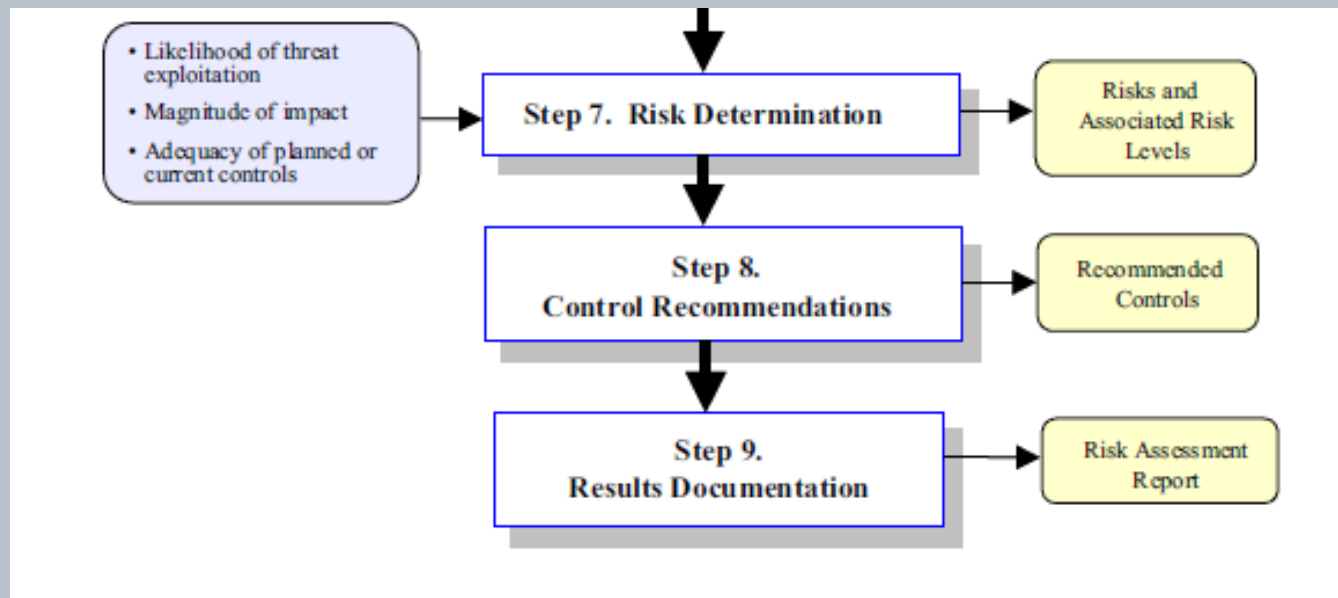
# Risk Assessment Process



# Risk Assessment Process



# Risk Assessment Process



# Risk Assessments

- GLBA Section 501(b), FIL-22-2001, FIL-81-2005, FFIEC IT Examination Handbook
  - *“Examiners must assess the quality of an institution’s risk assessment methodologies as part of the examination.”*
- The FFIEC agencies base their IT examination process on the concept of on-going, risk based supervision.

# Risk - Categories

- “The various FFIEC agencies have different names for the various categories of risk. The Federal Reserve includes six types of risk, which are credit, market, liquidity, **operational, legal, and reputational**. The OCC includes nine types of risk which are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, reputation, and strategic. This booklet uses the Federal Reserve categories with the addition of **strategic** risk and the assumption that market risk includes interest rate risk, price risk, and foreign exchange risk.”
  - *FFIEC IT Examination Handbook, Information Security Booklet*

# Risk - Categories

- Transactional/Operational
- Compliance/Regulatory/Legal
- Strategic
- Reputation

# Transactional Risk

- Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. **This risk exists in each product and service offered.**

# Transactional Risk

- Ex. 1: Remote Deposit Capture is implemented prior to an assessment of the risks of faulty equipment, inadequate procedures, or inadequate training of customers and their employees.
- Ex. 2: An improperly implemented IT upgrade.

# Compliance/Regulatory Risk

- Risk arising from inability to meet, or failure to comply with, statutory or regulatory obligations. Arises from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards.

# Compliance/Regulatory Risk

- Ex. 1: An ineffective DR strategy results in downtimes in excess of funds availability guidelines.
- Ex. 2: Not having an ID Theft policy in place after the deadline.

# Strategic Risk

- Arises from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. Can also stem from inaccurate information or analysis that causes management to make poor strategic decisions.

# Strategic Risk

- Ex. 1: Implementing new technology before evaluating against strategic plan.
- Ex. 2: Defining a target market demographic too narrowly, resulting in an overemphasis in that demographic.

# Strategic Planning

- IT management should have a corporate-wide view of technology. It should maintain an active role in corporate strategic planning to align technology with established business goals and strategies.

# Strategic Planning

- Strategic IT planning focuses on a three to five year horizon and helps ensure the institution's technology plans are consistent or aligned with its business plans.
- Strategic planning should address long-term goals and the allocation of IT resources to achieve them.

# Reputation Risk

- Risk that negative publicity regarding an institution's business practices will affect the institution's ability to establish new relationships or services, as well as affect its ability to continue servicing its existing relationships.

# Reputation Risk

- Ex. 1: Remote Deposit customer PC is compromised due to inadequate security controls which in turn creates a negative image for the financial institution.
- Ex 2: Inadequate disaster recovery procedures result in unacceptable downtime, resulting in customers moving accounts to competitors.

# Risk

- **Inherent Risk** – Risks that exist before the application of controls.
- **Residual Risk** – Risks that exist after the application of controls.
- **Emerging Risk** – Anticipating changes in risk due to proposed changes in business process, offerings or vendors.

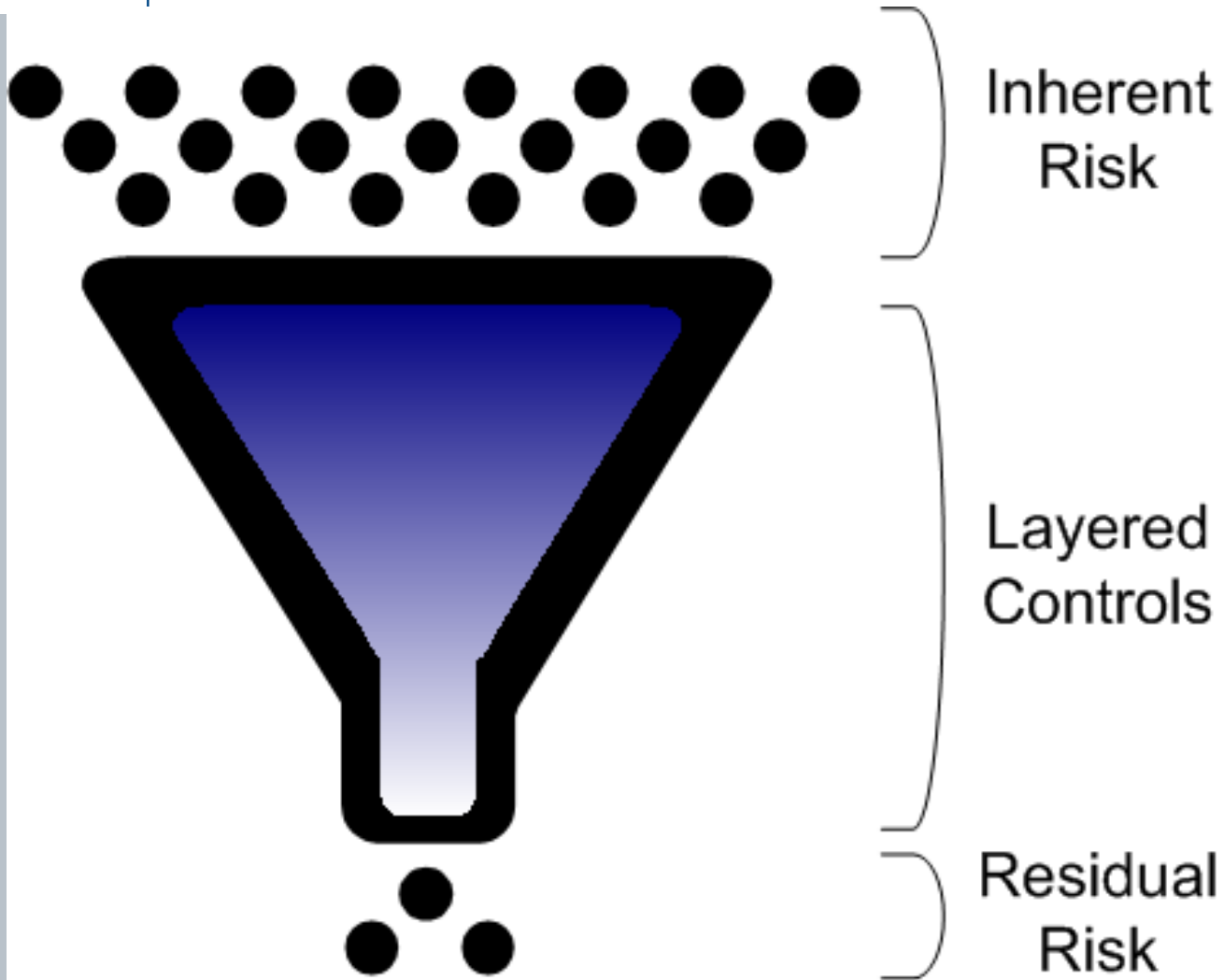
# Inherent Risk

- Risk existing prior to the application of controls.
- Must be established to determine scope and frequency of audits and independent reviews.
- Controls:
  - Avoid
  - Eliminate
  - Reduce
  - Transfer
  - Accept

# Residual Risk

- Risk management process is designed to identify residual risk.
- If residual risk is not within acceptable levels, additional controls must be implemented.
- To determine the extent of residual risk, FI's must understand the effectiveness of their existing controls.

# Risk Management



# Self-Assessments

- FFIEC
  - Mentioned 43 times, and in 7 of the 12 Handbooks
- COBIT
  - ME2 Monitor and Evaluate Internal Control
    - ME2.4 - Control Self-assessment
      - Evaluate the completeness and effectiveness of management's control over IT processes, policies and contracts through a continuing program of self-assessment.

# Self-Assessments

## COBIT

### Maturity Model for Internal Control

0. Non-existent
1. Initial
2. Repeatable, not documented
3. Documented
4. Managed and measurable
5. Optimized
  - ✓ Self-assessments

# Self-Assessments

## ISACA

- *CRSA is a technique that adds value by increasing an operating unit's involvement in designing and maintaining control and risk systems as well as identifying risk exposures and determining corrective action.*

# Self-Assessments

## IIA

- *CSA is a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met.*
- *CSA provides the framework to continually assess risk and develop an internal control environment to promote the achievement of objectives.*

# Self-Assessments

## FFIEC

- **OPERATIONS:**
  - Periodic **control self-assessments** allow management to gauge performance, as well as the criticality of systems and emerging risks.
- Does not eliminate the need for internal and external audits.
- Validate the adequacy and effectiveness of the control environment.
- Facilitate early identification of emerging or changing risks.

# Self-Assessments

## FFIEC

- **INFORMATION SECURITY**

- Condition monitoring tools include **self-assessments**, metrics, and independent tests.
- **Self-assessments**, metrics, and independent tests may address compliance with existing controls and the adequacy of those controls.
  - Provide a warning flag to line management so problems can be addressed before they arise in testing reports.
  - Uses tools and techniques similar to independently performed audits and penetration tests.

# Self-Assessments

## FFIEC

- **INFORMATION SECURITY**

- *“Senior management should require periodic self-assessments to provide an ongoing assessment of policy adequacy and compliance and ensure prompt corrective action of significant deficiencies.”*

# Self-Assessments

## FFIEC

- **MANAGEMENT**

- In addition to the traditional reliance upon internal and third party audit functions, financial institutions should perform **self-assessments** on a periodic basis. The scope and frequency of **self-assessments** will depend upon the scale and historical performance of the IT function. **Self-assessment** activities broaden management's perspective by involving a varied audience and by requiring acknowledgement of the results by those involved. The **self-assessment** process can help identify the need for policy changes and updates.

# Self Assessments In Practice

- Quarterly System Review now Quarterly Control Self-Assessment
- Committee setting, all functional units represented (Tech Steering ideal)
- Standardized agenda
- Assigning follow-up items and tracking to resolution

# Standardizing the Format New Technology

Risk Assessment Matrix		Technology is new, or change to existing	Technology is Software Hardware or Both	Customer Information Risk (GLBA)		Information Security Risk (FFIEC)			Enterprise-Wide Business Risk**				
				Privacy Exposure	Security Exposure	Confidentiality Risk	Integrity Risk	Availability Risk	Regulatory / Legal / Compliance	Strategic	Reputation	Operational / Transactional *	Credit / Interest Rate
Vendor name and description of Product/Service	Assessment Date	(N)ew, or (C)hange	(S)oftware (H)ardware or (B)oth	(H)igh, (M)edium, (L)ow	(H)igh, (M)edium, (L)ow	(H)igh, (M)edium, (L)ow	(H)igh, (M)edium, (L)ow	(H)igh, (M)edium, (L)ow	(H)igh, (M)edium, (L)ow, (N/A)	(H)igh, (M)edium, (L)ow, (N/A)	(H)igh, (M)edium, (L)ow, (N/A)	(H)igh, (M)edium, (L)ow, (N/A)	(H)igh, (M)edium, (L)ow, (N/A)

\* Never "N/A" when service is outsourced

# Standardizing the Format New Technology

Overall Inherent Risk	CONTROLS							Residual Risk	
	Service/Technology fits organization's strategic plan?	Documented Procedures Exist?	Vendor DR Capability Verified?	Recovery documented in our DR/BCP?	Vendor Oversight - Financials Reviewed?	Vendor Oversight - 3rd Party Assessments Reviewed?	Vendor Oversight - Contracts & SLAs reviewed?		
(H)igh (M)edium (L)ow	(Y)es or (N)o	(Y)es or (N)o	(Y)es or (N)o	(Y)es or (N)o	(Y)es or (N)o	(Y)es or (N)o	(Y)es or (N)o	(H)igh (M)edium (L)ow	Notes: (If residual risk other than low, describe additional controls)
H								H	

# Standardizing the Format IT Asset

Asset Description (data, applications, systems, HW and physical media)/Data Type	Reasonably Foreseeable Internal and External Threats and Vulnerabilities	Data Type		Likelihood of Occurrence	Potential Damage to the Bank	Overall Risk	Description of Security Controls (A) Administrative (T) Technical/logical (P) Physical  & disposal/retention procedures	Residual Risk	Testing Methods, Frequency, Control Issues	Recommendations/ Strategy to Mitigate Residual Risk
		Physical	Electronic							
(NPI) in printed or written form	Unauthorized disclosure due to files/NPI left in area (not filed, or properly destroyed). Items left on fax machine.	X	X	Medium	Moderate	Medium	(A) Branch/Departmental standards are covered in periodic employee training. Acknowledgement forms signed by every employee. (A) documents in process are stored in locked desk drawers or cabinets. (A) Employees trained on record retention schedules.	Not Acceptable	- Area Owner periodically reviews area and trash/shred bins to confirm NPI is properly handled according to defined standards. ISO non-scheduled walk throughs. Unsecured Fax machine in lobby area.	Consider moving the fax machine to a room/closet that can be locked (included in <i>Residual Risk Report</i> dated 8/7/07). Confirm that "in-process" documents for all areas are stored in fire proof, locked desk drawers or cabinets.



# Standardizing the Format IT Asset

## Informational Asset Inventory with Risk Assessment and Compensating Controls

### SAMPLE LISTING

#### Information Supplied by the Financial Institution

Functional Areas	Information and/or Systems Asset	Asset Name or Vendor (if Applicable)	Location(s)	Electronic, Paper, Both, or N/A	In-House, Outsourced, or N/A	Reasonably Foreseeable Internal and External Threats	Probability of Occurrence	Potential Damage	Inherent Risk Value	Inherent Risk Rating	Controls	Exposure Factor	Residual Risk Value	Residual Risk Rating
All	Files - Unsecured Areas	N/A	Various areas at each branch location	Both	In-House	Unauthorized access to sensitive/confidential information in paper and electronic forms. <b>Internal:</b> Employees without a need-to-know, fire and/or water damage, and lack of proper security measures/practices (i.e., handling, transmission, disposal, storage). <b>External:</b> Vendors, customers, and malicious individuals (i.e., hackers and social engineering schemes).	High	High	8	High	Employee training program, "Clean-Desk" policy, shred procedures, desk locks, vendor supervision, screensaver passwords, complex password-protected computers	Minimal Mitigation	4.25	High
All	Files - Secured Areas	N/A	Various areas at each branch location	Both	In-House	Unauthorized access to sensitive/confidential information in paper and electronic forms. <b>Internal:</b> Employees without a need-to-know, fire and/or water damage, and improper security measures and/or practices (i.e., handling and disposal). <b>External:</b> Vendors and malicious individuals (i.e., hackers and social engineering schemes).	Low	Medium	2	Mid-Low	Fire-resistant cabinets, employee training program, limited employee access to file vaults, vendor supervision	Intensive Mitigation	0.1	Low
Cust. Serv.	Loan Applications (Commercial, Installment, & Mortgage)	N/A	Loan personnel desks, loan storage area at the Main Office. Loan Origination and document imaging systems.	Both	In-House	Unauthorized access to paper and/or electronic documentation. <b>Internal:</b> Employees without a need-to-know, improper disposal, and lack of vendor oversight. <b>External:</b> Vendors, customers, malicious individuals (i.e., hackers and dumpster diving).	Medium	High	4	Mid-High	Shred procedures, limited access to loan file cabinets, employee training program, limited access to loan origination application	Some Mitigation	2.6	Medium
HR	Payroll	N/A	HR office at Main Office. HR share on the network server.	Both	In-House	Unauthorized access to paper and electronic payroll documents. <b>Internal:</b> Employees without a need-to-know and improper access controls <b>External:</b> Vendors and malicious individuals (i.e., hackers and dumpster diving).	Low	Medium	2	Mid-Low	Limited access to HR files, payroll information is encrypted on the servers	Moderate Mitigation	0.9	Low
IT	Data (Storage)	N/A	Network server, backup tapes, employee computers	Electronic	In-House	Unauthorized access of data or loss of data. <b>Internal:</b> No and/or weak encryption methods, encryption keys not properly secured, fire and/or water damage, employees without a need-to-know. <b>External:</b> Disaster, hackers, janitors, vendors, malicious individuals.	Medium	High	4	Mid-High	File permissions set to minimal rights that are required, complex password-protected computer access, dry-charge fire system in server rooms, limited access to server rooms, encryption on certain highly sensitive server folders, mirrored servers at backup site, laptop encryption	Elevated Mitigation	1	Low
Operations	Internet Banking System	ACME Internet Banking	Server housed at ACME Corporation's Operations	Electronic	Outsourced	Unauthorized access to sensitive and/or confidential information. <b>Internal:</b> Weak password standards, session time-out, lack	Medium	High	4	Mid-High	MFA, 180 day password expiration, complex password requirements, SAS-70 and pen	Intensive	0.2	Low

# Standardizing the Format

## AS/NZS 4360

<b>Impact</b>	<b>Extreme</b>	<b>Significant</b> 5	<b>Major</b> 10	<b>High</b> 15	<b>Severe</b> 20	<b>Severe</b> 25
	<b>Very High</b>	<b>Moderate</b> 4	<b>Significant</b> 8	<b>Major</b>	<b>High</b> 16	<b>Severe</b> 20
	<b>Medium</b>	<b>Low</b> 3	<b>Moderate</b> 6	<b>Significant</b> 9	<b>Major</b> 12	<b>High</b> 15
	<b>Low</b>	<b>Trivial</b> 2	<b>Low</b> 4	<b>Moderate</b> 6	<b>Significant</b> 8	<b>Major</b> 10
	<b>Negligible</b>	<b>Trivial</b> 1	<b>Trivial</b> 2	<b>Low</b> 3	<b>Moderate</b> 4	<b>Significant</b> 5
		<b>Rare</b>	<b>Unlikely</b>	<b>Moderate</b>	<b>Likely</b>	<b>Almost Certain</b>
		<b>Probability</b>				

# Standardizing the Format Prouty Approach

	Malicious Activity				Natural Disasters						Technical Disasters							
	Fraud, Theft, Blackmail	Sabotage	Vandalism & Looting	Terrorism	Fire	Flood, Water Damage	Severe Weather	Air Contaminants	Hazardous Spills	Pandemic	Communications Failure				Power Failure	Equipment & Software Failure	Trans. System Disruptions	Water System Disruptions
<b>Impact</b>	-1	1	0	3	3	3	3	3	2	3	2	3	4	5	3	4	-2	-3
<b>Probability</b>	2	-1	2	1	1	-1	2	-3	-2	-1	-1	-3	2	1	4	2	1	2
<b>Threat</b>	2.8	2.4	3.5	4.8	4.8	3.2	5.6	1.6	2.1	3.2	2.8	1.6	6.3	6	7.2	6.3	1.8	1.4

**Probability**

<= -3	Almost nil (extremely Unlikely)
-2 to 1	Slight (has not happened, but could)
2 to 3	Moderate (happens once in a while)
4 to 5	Definate (happens regularly)

**Impact**

<= -2	Slight
-1 to 2	Moderate to Significant
3 to 5	Severe

# Questions?



[www.FFIECguru.com](http://www.FFIECguru.com)  
[www.safesystems.com](http://www.safesystems.com)

Tom Hinkel, CISA, CRISC - Director  
of Compliance, Safe Systems, Inc.  
[tom@safesystems.com](mailto:tom@safesystems.com)