



**Southern California Association for Financial Professionals
28th Annual EXPO L.A**

A 2x4 approach to payment product risk assessment

John Seddon

10:30am Friday, May 8th, 2009



DEKNATEL SEDDON & ASSOCIATES

SCAFP Risk 20090408.pptx

Today's Agenda

1 Acronym Soup

2 2 x 4

3 Great Expectations

4 Getting Down To Numbers

5 Practice, Practice, Practice

6 Decisions

Today's Agenda

1

History of Payment Products, Risks, Controls, and Guidance

2

Payment Product Risk Assessment

3

Stages of Improvement - A Maturity Model

4

Inherent Risk

5

Controls and Residual Risk

6

Next Steps – Prioritizing Improvements

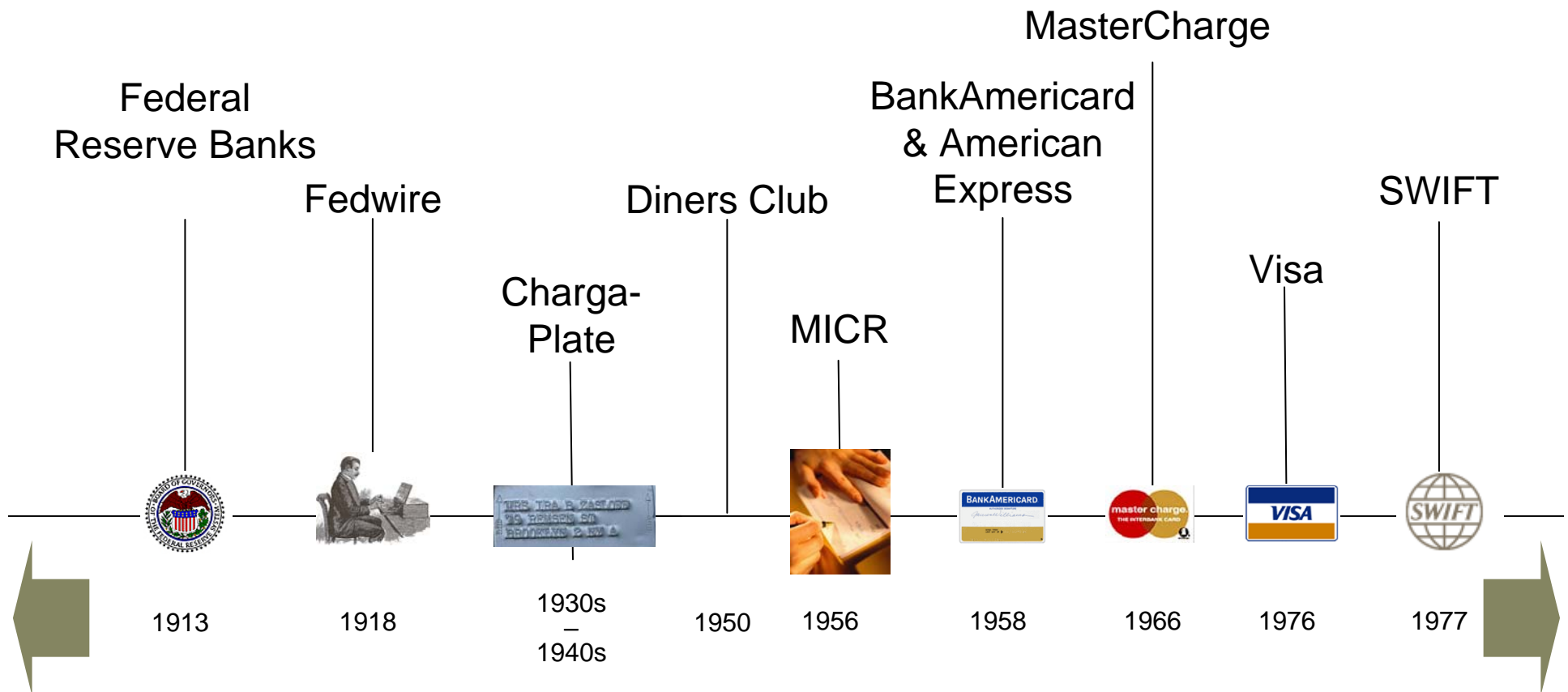
Today's Agenda

1

History of Payment Products, Risks, Controls, and Guidance

- Brief History of Payment Products, Risk, and Risk Measurement
- Acronym Soup: Overview of Regulatory, Other Guidance and Good Practice

Brief History of Payment Products, Risk, and Risk Measurement



Risk Assessment Guidance - Payments

- FFIEC Wholesale Payment Systems July 2004:
 - “A financial institution’s information security program should include an effective **risk assessment** methodology that includes an evaluation of risks relating to performing high risk activities such as funds transfer and other payment-related activities.”
- FFIEC Retail Payment Systems March 2004:
 - “The privacy risk combined with the funds transfer capability should cause these systems to rank high in all institutions’ information security **risk assessments**.... The assessment should review the security of all third-party service providers as well.”

Risk Assessment Guidance – Payments / Banking

- Payment Card Industry (PCI) Data Security Standard, 2004 (previously CISP):
 - “Requirement 12: ...Establish, publish, maintain, and disseminate a security policy that includes an annual process that identifies threats and vulnerabilities, and results in a **formal risk assessment.**”
- Gramm Leach Bliley Act 1999:
 - “Institutions are required to: identify and **assess the risks** that may threaten customer information;”

IT Risk Assessment Guidance - Banking

- Federal Financial Institutions Examination Council, Information Security IT Examination Handbook 2006:
 - “The board should provide management with its expectations and requirements and hold management accountable for
 - Central oversight and coordination,
 - Assignment of responsibility,
 - **Risk assessment and measurement,**
 - Monitoring and testing,
 - Reporting, and
 - **Acceptable residual risk.”**
 - Includes multiple references to National Institute of Standards and Technology (NIST) as an information-security standard-setting group.

Today's Agenda

2 Payment Product Risk Assessment

- Risk Assessment Basics
- 4 Steps
- 2 Approaches

Risk Assessment Definitions

Threat

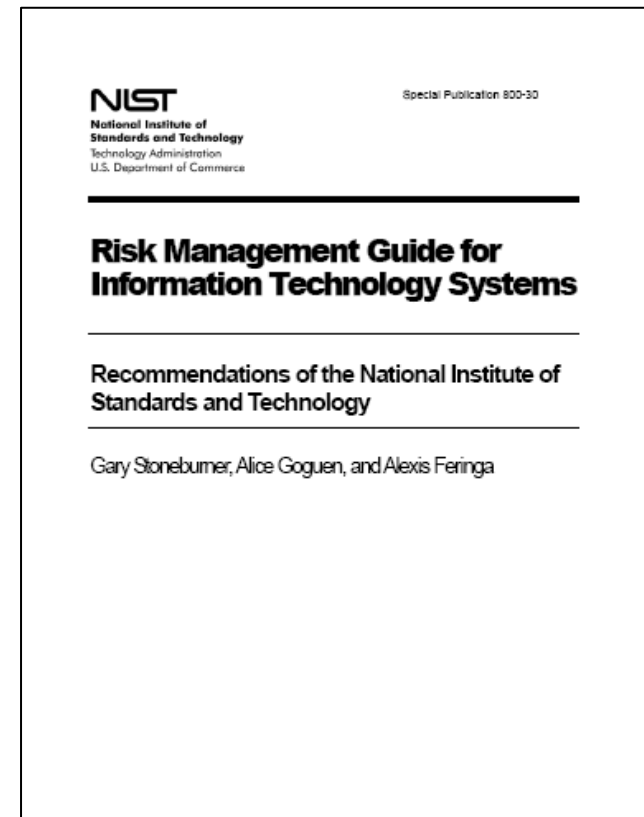
- A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability.

Vulnerability

- A vulnerability is a weakness that can be accidentally triggered or intentionally exploited.

Threat source

- A threat-source presents a risk when there is a vulnerability that can be exercised.



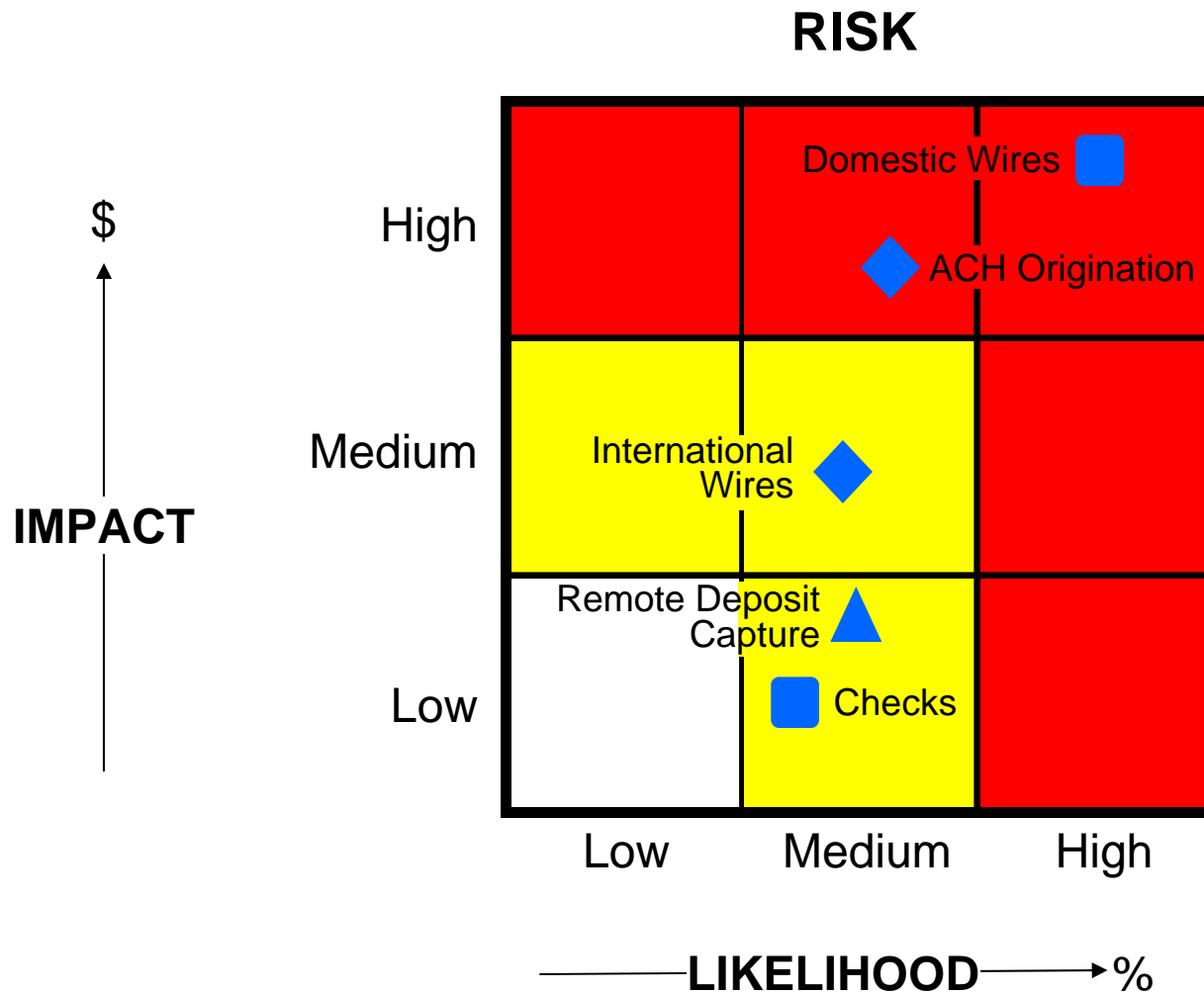
Source: National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems, SP800-30, July 2002.

Risk Assessment Definitions continued

- Risk Management
 - Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
- Likelihood
 - Annualized rate of occurrence (ARO) of the threat to the asset. The ARO is an estimate based on the data of how often a threat would be successful in exploiting a vulnerability.
- Impact
 - Single loss expectancy (SLE) of an asset. The single loss expectancy can be defined as the loss of value to asset based on a single security incident.

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Risk Diagram Example

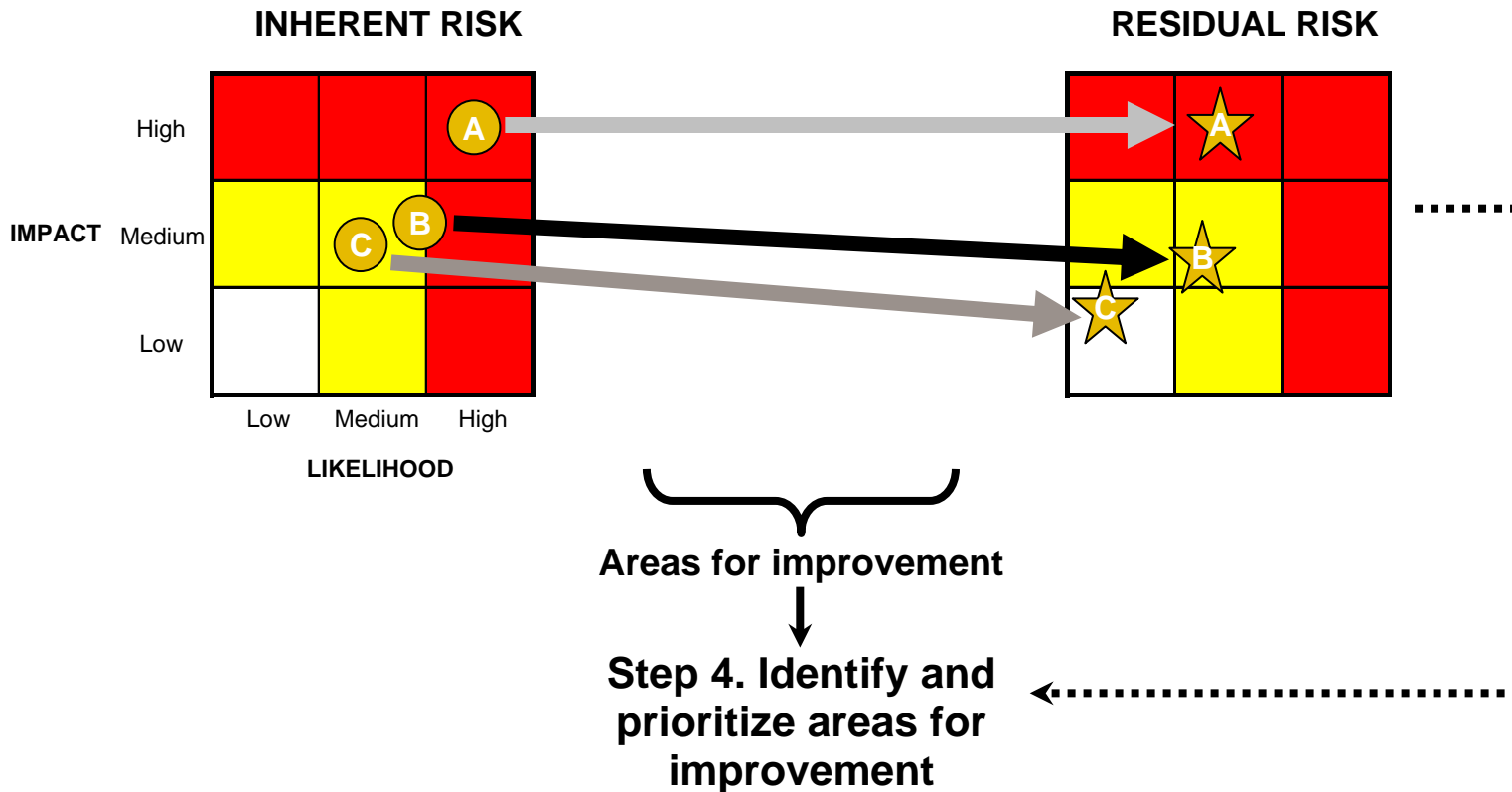


Four steps

Step 1. Assess inherent risk

Step 2. Assess controls

Step 3. Assess residual risk.



Inherent risk for area A, B, C etc.

Residual risk for area A, B, C, etc.



Mitigating control(s) for area, with high, medium, or low effectiveness

Two Approaches – Quantitative versus Qualitative

- Defining metrics, categorizing incidents and causes, and collecting data on a consistent basis, takes time and effort.
- Starting with a qualitative approach may be more feasible.

Quantitative	Qualitative
<ul style="list-style-type: none">• Prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.• The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner.• Requires data – and consistently collected data.	<ul style="list-style-type: none">• Subjective analysis of the components of inherent and residual risk does not lend itself to precise measurements.

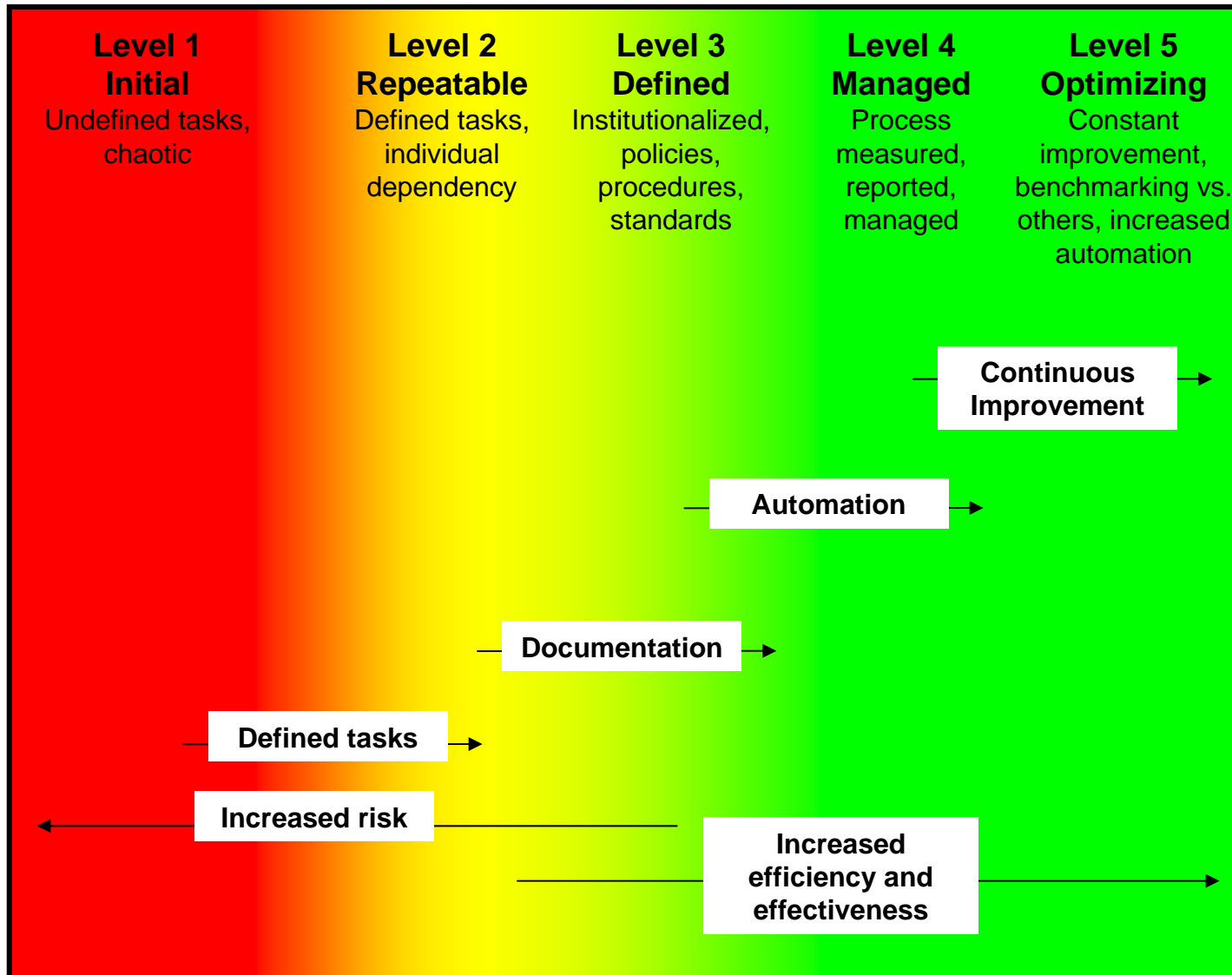
Today's Agenda

3

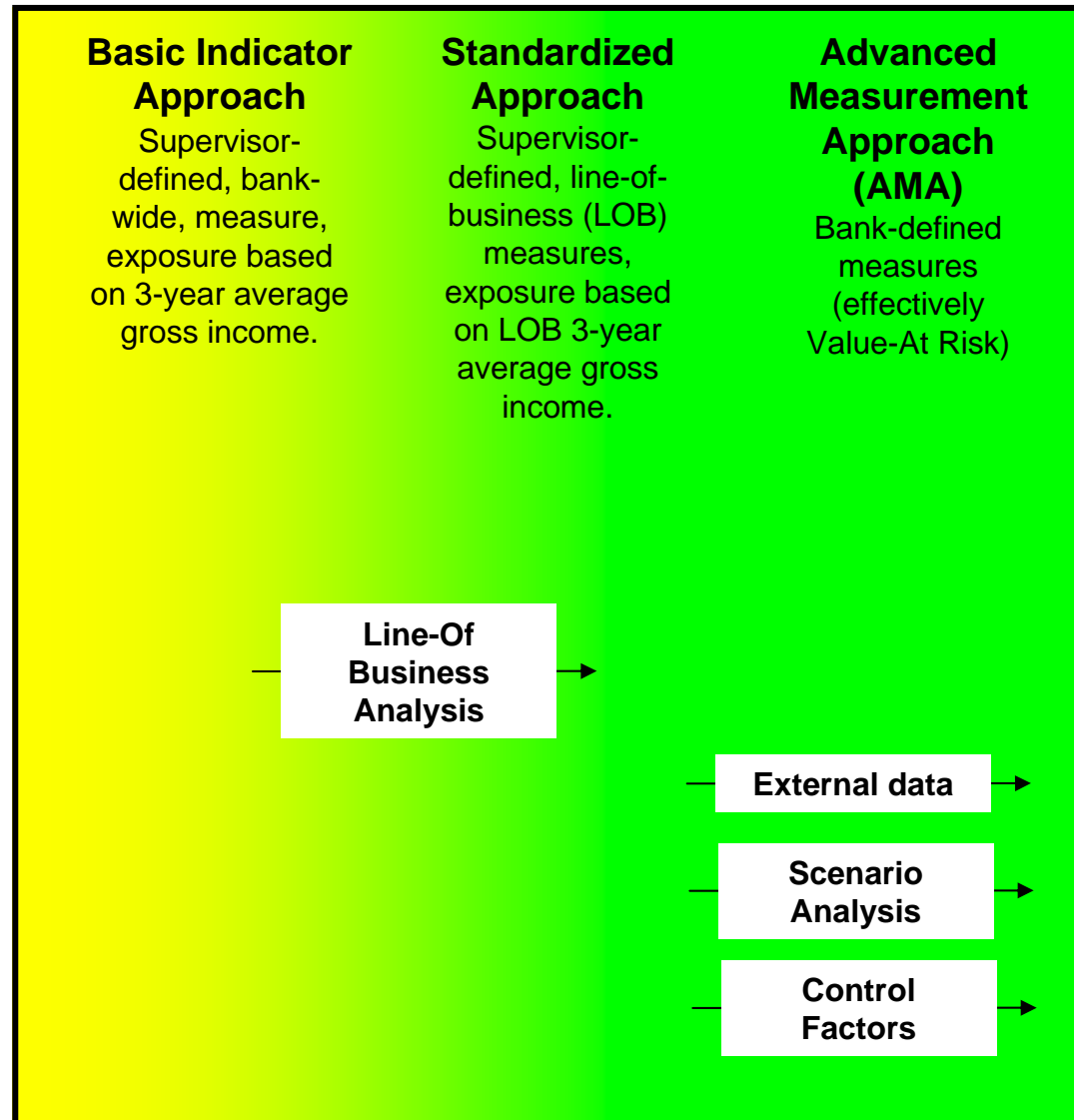
Stages of Improvement - A Maturity Model

- Capability Maturity Model
- BASEL II / U.S. BASEL II

Risk Assessment Maturity Models – CMM



Risk Assessment Maturity Models – BASEL II / U.S. BASEL II



Today's Agenda

4

Inherent Risk

- Data Sources
- Payment's Top 10 Frauds

Examples of Data Sources

Fraud / Robbery

- Los Angeles Police Department
- Federal Bureau of Investigation

Technology

- Symantec, McAfee, etc.
- Open Web Application Security Project (OWASP)
- NIST
- Department of Homeland Security

Fire / Earthquake / Public Health

- National Technical Information Service
- US Geological Survey



Data Sources for Financial Institutions

- FDIC 2004 Loss Data Capture Exercise (LDCE)
- Operational Risk Exchange (ORX)
- American Banker's Association Deposit Account Fraud Survey
- Cybersource Online Fraud Report



FDIC 2004 Loss Data Capture Exercise (LDCE 2004)

- Conducted in preparation for the U.S. implementation of the BASEL II capital framework
- Used seven operational risk event types defined by the Basel Committee:
 1. Internal Fraud
 2. External Fraud
 3. Employment practices & work place safety
 4. Clients, products, and business practices
 5. Disasters and public safety / Damage to physical assets
 6. Business disruption, technology and infrastructure failures
 7. Execution, delivery and process management.

Operational Riskdata Exchange (ORX)

- Not-for-profit industry association, founded in 2002, in Zurich, Switzerland
- 51 members
- Database of 102,500 operational risk losses, each over €20,000 in value, to a total of €34.4 billion



- US bank members are:
 - Bank of America
 - JPMorgan Chase
 - National City Corporation
 - Northern Trust
 - State Street Corporation
 - US Bancorp
 - Wachovia Corporation
 - Wells Fargo & Co

American Banker's Association Deposit Account Fraud Survey Top 10

1. Identity Theft
2. On-Us Check Fraud
3. Wire Fraud
4. Credit-Card Bust-Out
5. ACH Fraud
6. Deposit or Payments Fraud
7. Debit Card Fraud
8. Online Account Takeover
9. Cross-Channel Fraud
10. Organized Fraud Rings



Today's Agenda

5

Controls and Residual Risk

- Incident Examples
- Controls and Good Practices
- Residual Risk

Web-based Threats

- Symantec observed Web attacks from 808,000 unique domains, many of which are mainstream websites.
- 600 million browsers are estimated to be insecure.
- Over 23 million machines were infected with misleading applications.
- The Attack Bar is low: off the shelf software toolkits allow any person to automatically exploit hundreds of thousands of systems.



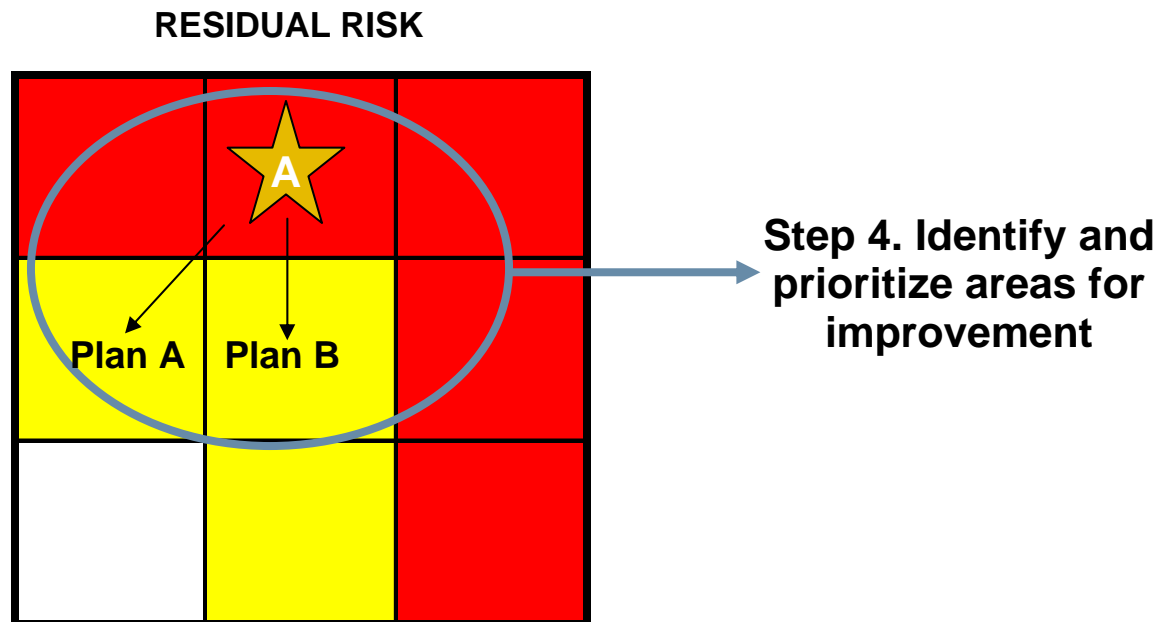
Today's Agenda

6 Next Steps – Prioritizing Improvements

- Return on Control Investment
- Priorities, Prerequisites, Plan

Return on Control Investment

- Evaluate control investments and remediation alternatives based on risk reduction:
 - Reduction in risk provides return on investment
 - Qualitative approach provides relative return.



Thank You!

John Seddon

john@dekseddon.com

