Building a Risk Assessment Process from the Ground Up

David Fong, SVP – Audit Director
Bank of the West
Governance, Risk & Compliance – G12
Table of Contents

• Session Objectives
• Purpose for Risk Assessments
• Process Overview
  – Where to Start
  – Auditable Entities
  – Audit Universe
  – Risk Assessment
  – Annual Audit Planning
  – Audit Execution

• Questions
Session Objectives

• To walk through detailed steps for building a solid risk assessment process – from consideration for building the audit universe to audit execution
  – Risk assessments are the foundation to solid risk-based auditing
  – Not intended to tell you what to do, but, instead, how to start or what to consider

• For beginner, intermediate internal audit, senior, manager, director, VP interested in risk assessments and the annual audit planning process
About Me

• Director of Professional Practices at Bank of the West (BNP Paribas Group)
• CPA (inactive) and CISA
• Financial services experience (broker-dealer, asset management, banking, payment card, insurance)
• 17+ years external/internal audit experience
• 4+ years in vendor management
• 5+ years in accounting
About Bank of the West

• Founded in 1874
• $63.3 billion in assets
• Nearly 700 retail and commercial banking locations in 19 Western and Midwestern states
• Subsidiary of BNP Paribas, a top global financial institution
  – present in more than 85 countries
  – the company has more than 200,000 employees
A LITTLE ABOUT YOU
Why are You Here?

- Revisiting your current risk assessment process
- Preparing to start annual risk assessment process
- Wanting to learn about risk assessments
- Other reasons?
Your Interaction with Risk Assessments

• Preparer
• Reviewer
• User
Approximate Number of AEs at Your Organization

• 75 or less
• Between 76 and 150
• Over 150
Audit Cycles used at Your Organization

• 1/2/3 year
• 1/3/5 year
• None
• Something else
PURPOSE OF RISK ASSESSMENTS
The Basic Building Blocks

- Audit Cycle based on risk assessments
- Audit Plan
- Inherent Risk - Likelihood
- Quality of Control Factors
- Audit Universe
- Auditable Entities
- Risk Assessment Process
- Risk Factors
- Inherent Risk - Impact

2013 Fall Conference – “Sail to Success”
September 30 – October 2, 2013
Balance of Risk vs. Resources

Finite Assurance Resources

Dynamic Organizational Risk

2013 Fall Conference – “Sail to Success”
September 30 – October 2, 2013
Why Risk Assessments?

• Helps an Internal Audit function allocate a finite set of assurance resources against a set of dynamic set of risks
• Determine the relative risk for an organization’s long list of risks
• Plan multi-year assurance coverage based on that risk in order to determine resource needs
• Allocate assurance resources for audit planning
• Focus on higher areas of risk during an audit
Why Risk Assessments?

Using risk assessments to determine what to cover, when to cover, and why cover via a risk-attuned process

Higher risk entities
The Process

Auditable Entities

Audit Execution

Audit Universe

Annual Audit Plan

Risk Assessment
Decisions and Implications

• Before starting, key decisions must be made
• Use of Quantitative vs. Qualitative risk assessments
• What the auditable entity units will look like and the number of auditable entities in the universe
  – Granular vs. Non-granular
  – Organization vs. Functional vs. Thematic
• Rating levels and their respective definitions
Where to Start?

• Definitions, policies, and standards
  – Critical to have definitions, policies, and standards
  – Without them, the process WILL BE FLAWED

• Identify qualitative and quantitative risk factors relevant to your organization

• Risk assessments performed by other units will help validate your risk assessments
The Process

Auditable Entities

Audit Execution

Audit Universe

Annual Audit Plan

Risk Assessment
Auditable Entities

• Establishing related units of processes/businesses/products/investments/support infrastructure that is likely to be audited together
• Don’t be too high-level
  – Difficult to determine when the entity has been sufficiently audited for coverage purposes
• Don’t be too granular
  – Difficult to allocate resources and have meaningful results
Auditable Entity Types

- **Infrastructure**
  - Network
  - Databases
  - OS
  - Data Center

- **Thematic**
  - Transversal Risk
  - Emerging Risks
  - Regulations
  - Model governance
  - Projects

- **Business Units**
  - Sales
  - Marketing
  - Manufacturing
  - Accounting

- **Products**
  - Passenger Auto
  - Trucks
  - Marine
  - Consumer
  - Commercial

NOTE: Some thematic entities could be short-lived!
The Process

Auditable Entities

Audit Execution

Audit Universe

Annual Audit Plan

Risk Assessment
Audit Universe

- Complete listing of everything that could be and should be audited over a period of time

\[ \text{Audit Universe} = \sum \text{Auditable Entities} \]
Validate Audit Universe/Entities

• Validate the completeness of the audit universe/entities against
  – Organization charts
  – Management/Board view of the organization
  – Human Resource records
  – Legal Entities from Legal
  – Management Self-Assessments
  – Emerging risks
The Process

Auditable Entities

Audit Execution

Audit Universe

Annual Audit Plan

Risk Assessment

2013 Fall Conference – “Sail to Success”
September 30 – October 2, 2013
Purpose and Objective

- Risk Assessments (RA) provide the basis for the formulation of the annual audit plan and risk-based allocation of assurance resources.
Timing of Risk Assessments

Risk Assessments

- End of audit assignment
- Risk event
- New businesses formed
- At least, annually
- Organizational changes

Risk event

End of audit assignment

New businesses formed

At least, annually

Organizational changes

2013 Fall Conference – “Sail to Success”
September 30 – October 2, 2013
Basic Components

• Background information
  – Provides useful context information to determine which factors have the most impact for the entity and may need to be considered during next audit

• Risk assessment results
  – The assessment based on the applicable definitions

• Supporting rationale
  – The reason why a rating was chosen
  – Provides transparency so that others understand the drivers to the entity’s risk assessment
Some Different Approaches

- **Scorecard**
  - Assigning numeric scores to various factors
  - Using both quantitative and qualitative elements to assign scores

- **Quantitative**
  - Using objective measures

- **Qualitative**
  - Using subjective measures

- **Hybrid**
  - A combination of some or all of the above

IDEAL
## Risk Assessment Scorecard

### Application Development Team

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Score (1-10)</th>
<th>Weight</th>
<th>Weighted Score</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significance</td>
<td>10</td>
<td>25%</td>
<td>2.50</td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>9</td>
<td>10%</td>
<td>0.90</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>2</td>
<td>25%</td>
<td>0.50</td>
<td>Stable management team</td>
</tr>
<tr>
<td>:</td>
<td>2</td>
<td>5%</td>
<td>0.10</td>
<td></td>
</tr>
<tr>
<td>Date of last review</td>
<td>-</td>
<td>15%</td>
<td>-</td>
<td>in 2012</td>
</tr>
<tr>
<td>Prior audit findings</td>
<td>7</td>
<td>20%</td>
<td>1.40</td>
<td>Number of areas had findings</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td></td>
<td><strong>5.40</strong></td>
<td></td>
</tr>
</tbody>
</table>
# Simple Risk Assessment Summary

<table>
<thead>
<tr>
<th>Auditable Entity</th>
<th>Inherent Risk</th>
<th>Control Risk</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Line A</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Business Line B</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Marketing</td>
<td>L</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Accounting</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Human Resources</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Networks</td>
<td>H</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>User Access Management</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Databases</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>SDLC</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Change &amp; Problem Management</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Thematic-Privacy</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>
# Simple Risk Assessment Summary (2)

- Adding numerical elements for impact and likelihood

<table>
<thead>
<tr>
<th>Auditable Entity</th>
<th>Impact (1-5)</th>
<th>Likelihood (1-5)</th>
<th>Score</th>
<th>Inherent Risk</th>
<th>Control Risk</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Line A</td>
<td>5</td>
<td>5</td>
<td>25</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Business Line B</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Marketing</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>L</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Accounting</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Human Resources</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>4</td>
<td>5</td>
<td>20</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Networks</td>
<td>5</td>
<td>4</td>
<td>20</td>
<td>H</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>User Access Management</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Databases</td>
<td>3</td>
<td>5</td>
<td>15</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>SDLC</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Change &amp; Problem Management</td>
<td>4</td>
<td>5</td>
<td>20</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Thematic-Privacy</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>
Where to Divide the Audit Universe?

- Organizations can divide the auditable entities based on:
  - Relative risk scores (e.g., top X% are high)
  - Absolute risk scores (e.g., @ >59 then high)
  - Natural breaks

<table>
<thead>
<tr>
<th>Auditable Entity</th>
<th>Risk Score</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Line A</td>
<td>80</td>
<td>High</td>
</tr>
<tr>
<td>.</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>Thematic-Privacy</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>User Access Management</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Business Line B</td>
<td>55</td>
<td>Medium</td>
</tr>
<tr>
<td>.</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>Change &amp; Problem Mgmt</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Databases</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Accounting</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td>29</td>
<td>Low</td>
</tr>
<tr>
<td>SDLC</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>
Inherent Risk

• As defined by the IIA, **Inherent Risk** is:
  – the status of risk (measured through impact and likelihood) **without** taking account of any risk management activities (i.e., controls) that the organization may already have in place

• When assessing inherent risk, consider what could/has happened for the auditable entity or other similar institutions
  – “**It could not happen here because we are better controlled**” should never be part of the evaluation of inherent risk!
Another to Think About Inherent Risk

• Think of what happens when a bomb explodes (impact)

• Think of how often this is likely to happen (likelihood)
Inherent Risk Factors

- People
  - Client
  - Legal and Regulatory
  - Reputational
  - Significance
- Operational Complexity
  - Credit
  - Technology
  - Competitive Environment

Significance

2013 Fall Conference – “Sail to Success”
September 30 – October 2, 2013
Inherent Risk – Impact

• Each risk should be rated (e.g., High, Medium, Low) where relevant for the auditable entity

• When deemed not relevant, a rationale should be provided
  • Not all factors apply to all auditable entities, which should be explained within the risk assessment
Impact Criteria

**High**
Impact is considered severe, which adversely effects the auditable entity’s ability to meet its core objectives. Impact could be mid- to long-term.

**Medium**
Impact is considered moderate, which may have some effect on the auditable entity’s ability to meet its core objectives. Impact is short-term.

**Low**
Impact is minimal with little or no effect on the auditable entity’s core objectives.
Inherent Risk – Likelihood

• Each risk factor should be assessed for the likelihood of materializing (e.g., Likely, Probable, Remote) for the auditable entity

• When considering likelihood, consider experience at the entity/industry over the course of the last 5-7 years

• Remember that the quality of controls should not be considered at this point!
Inherent Risk - Likelihood

Likely

Has or likely to occur at least once a year

Probable

Has or likely to occur within a 1 to 7 year period

Remote

Has not occurred and unlikely to occur within the next 7 years

Start here...

1 When determining whether a recent occurrence indicates a likely vs. probable likelihood, look back at the last 7 years to determine the frequency of occurrence

2 Based on experience within the organization or within the industry

---

2013 Fall Conference – “Sail to Success”
September 30 – October 2, 2013

41
Determining Inherent Risks

Inherent Risk is a product of:

\[ \text{Impact} \times \text{Likelihood} = \text{Inherent Risk} \]

Results are depicted as follows:

<table>
<thead>
<tr>
<th>Inherent Risk</th>
<th>Likelihood</th>
<th>Likelihood</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Overview

BEFORE STARTING...
Not all Risk Factors are Alike!

Every auditable entity will have different drivers and sources of risk!

Risk factors with significant influence the overall inherent risk

Risk factors with immaterial influence on the overall inherent risk
Drivers of Primary Risk Factors

Every auditable entity will have different drivers and sources of risk!

- Regulated
- High Visibility
- Strategically important
- Client
- Nature of the Business
RISK FACTORS
Risk Factors

SIGNIFICANCE
Significance

Measures the relative financial significance of the entity to the organization as a whole. Depending on the nature of the entity, different financial benchmarks may be used.

Benchmarks to consider include: deposits, loans, revenues, expenses, net income, and/or expected losses.

When choosing the benchmark(s), careful consideration must be taken to understand why a chosen benchmark was the most suitable financial factor to use.

Answers the question of “why is this auditable entity financially significant for the organization?”
Significance: Impact Considerations

High
Revenue, deposits, loans, net income, expenses, and/or expected losses are material (>20%) for the Bank

Medium
Revenue, deposits, loans, net income, expenses, and/or expected losses are material (between 10-20%) of the Bank

Low
Revenue, deposits, loans, net income, expenses, and/or expected losses are material (<10%) of the Bank
Risk Factors

CLIENT
Client

Measures the relative impact to the organization’s ability serve its clients

Consider the number, type of clients, and nature services that could be affected from a realized risk event for the entity

Severe impact to client and services may also have an reputational impact as well

The larger the client base that is served through an auditable entity the greater the potential impact. As such, key operating functions, core systems, and infrastructure will likely have a largest potential impact to clients
Client: Impact Considerations

High
Severe service failure to all customers* or service types

Medium
Major service failure across a major customer* group or service type

Low
Operational failure impacts a number of clients* but is isolated

* Clients only and not employees
Risk Factors

REPUTATIONAL
Reputational

Measures potential reputational impact from activities of the entity

Consider the nature of the entity and the customers/activities that could give rise to reputational damage. The customers/geographies/business for the entity activities could affect the speed and dispersion of negative publicity

Would the reputational damage be covered by national, regional, or local media?

Who would care? Would the general public, regulators, or only a small group of interested parties care?
Reputational: Impact Considerations

High
Negative impact is nationwide and is widely public

Medium
Negative impact is regional with widespread publicity, but confined to a limited number of parties

Low
Negative impact is isolated with little or no publicity
Risk Factors

LEGAL AND REGULATORY
Legal and Regulatory

Measures the severity of regulatory and legal risks for the entity

Consideration should be given to the number, types, and complexity of regulations/contracts that the entity is subjected to and the nature/range penalties for non-compliance. This is sometimes tied to the reputational impact as well.

Regulatory issues from other financial institutions may also provide a barometer to measure potential outcomes for similar breaches.
Legal and Regulatory: Impact Considerations

- **High**
  - Public regulatory fines/censure or major litigation. **Significant** breach of rules, regulations, or contracts

- **Medium**
  - Regulatory censure or action. Breach of rules, regulations, or contracts

- **Low**
  - Isolated breach of regulatory or contractual obligations
Risk Factors

PEOPLE
Measures the impact that people (i.e., employees) have on the entities’ ability to achieve its business objectives (i.e., serve its clients, meet regulatory requirement, fulfill critical business functions)

Consider the nature of the tasks, required skillsets, transferability of skills, stability of the workforce, and ease of recruiting for the entity.
People: Impact Considerations

High

Key person risk. Specialized skillset that is not easily replaceable. Significant staff turnover >15%

Medium

Specialized skills are used, but can be replaced with some effort and time, or with existing resources from other areas. Staff turnover <15%

Low

Skillset is readily available in the market. Stable team environment
Risk Factors

OPERATIONAL COMPLEXITY
Operational Complexity

Measures the complexity of operations and its impact on the entities’ ability to achieve its business objectives (i.e., serve its clients, meet regulatory requirement, fulfill critical business functions).

Consider the number of interdependencies (i.e., mutual reliance on processing between this entity and other entities) and handoffs (i.e., passing processing control to/from this entity and other entities).

Also, consider the effect and ability for the business processes to be handed-off in the event of a business disruption.

The greater the number of interdependencies and handoffs the greater the impact.
Operational Complexity: Impact Considerations

**High**

High-degree of interdependencies and hand-offs with many different areas. Key processes cannot be easily performed at alternate locations.

**Medium**

High-degree of interdependencies or hand-offs with a few different areas. High degree of automation of key processes.

**Low**

Limited hand-offs and interdependencies. Processing not constrained to a single location.
Risk Factors

CREDIT
Credit

Measures the impact of credit exposure relative to the organization as a whole

Consideration is given to:

- the significance of the auditable entity’s Risk Based Capital, calculated as a percentage of Total Bank Risk based Capital
- the significance of the year over year change in the amount of Risk Based Capital of the auditable entity
Credit: Impact Considerations

High
Risk based capital (RBC) >20% of total RBC or annual change of >20% in amount of RBC

Medium
Risk based capital (RBC) between 10-20% of total RBC or annual change between 15-20% in amount of RBC

Low
Risk based capital (RBC) between 0-10% of total RBC or annual change between 0-15% in amount of RBC
Overall Inherent Risk

Inherent risk factor(s) → Relevant risk factor(s) → Overall inherent risk
Overall Inherent Risk

• From the various risk factors rated, identify those factor(s) which should drive the overall rating
• The rating should not be an average or simply based on the most severe rating
• Based on your assessment of the inherent risk factors, select the most relevant drivers and based
QUALITY OF CONTROLS
# Quality of Control Indicators

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Control Indicators</th>
</tr>
</thead>
</table>
| Do Not Know         | ➢ New entity (rather than an entity separated out from an existing entity)  
                      ➢ No recent assessments with the last 4 year  
                      ➢ Used in very limited situations                                                                                                               |
| Unsatisfactory      | ➢ Recent internal reviews or external examinations rated as “Unsatisfactory” with a number of critical rated findings still unresolved  
                      ➢ High error rate (>10%) or significant (>1MM) actual losses  
                      ➢ Known, significant control gaps exist  
                      ➢ General management disregard over risks/controls                                                                                             |
| Marginally Satisfactory | ➢ Recent internal reviews or external examinations rated as “Marginally Satisfactory” or worse with a number of critical findings still unresolved  
                      ➢ Moderate error rate (<10%) or moderate (between $500K and $1MM) actual losses  
                      ➢ Number of refused recommendations  
                      ➢ Known control gaps exist, but does not significantly impact the entities ability to achieve its objectives  
                      ➢ Lack of proactivity over management of risk/control                                                                                         |
| Generally Satisfactory | ➢ Recent internal reviews or external examinations rated as “Generally Satisfactory” or worse with most critical findings resolved  
                      ➢ Negligible error rate (<5%) or insignificant (<$500K) actual losses  
                      ➢ Findings show general proactivity in the management of risk/controls  
                      ➢ No known control gaps exist                                                                                                                   |
| Satisfactory        | ➢ Recent internal reviews and external examinations rated as “Satisfactory”  
                      ➢ Findings from all previous internal reviews and external examinations have been remediated  
                      ➢ Proactive management of risk/controls.  
                      ➢ No known control gaps and minimal actual operating losses                                                                                   |
Overview

RESIDUAL RISK
Residual Risk

• As defined by the IIA, **Residual Risk** is
  – “the *remaining risks* after management takes action to reduce the impact and adverse event, including control activities in responding to a risk.”

\[
IR \geq RR
\]
## Residual Risk

<table>
<thead>
<tr>
<th>Inherent Risks</th>
<th>Residual Risk</th>
<th>Quality of Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>DNK</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Validation of Results

• Review the distribution of the residual risk ratings for reasonableness
  – Lack of distribution may result in inefficient allocation of assurance resources

• Compare internal audit RAs with results from other assessments
  – Identify any differences
  – Understand driver for these differences

• Discuss with executive management to affirm the results
The Process

Auditable Entities

Audit Execution

Audit Universe

Annual Audit Plan

Risk Assessment
Annual Audit Planning

• Once the RAs have been updated for all entities in the universe, compare the date of last audit to the results from the risk assessment
• Audit those entities requiring audits based on risk and the associated cycle
• Actual time allocated should be correlated to the residual risk
  – Spending 1,200 hours on a low risk entity vs. 400 hours on a high risk entity may need some explanation
## Annual Audit Planning: Step 1

- **Start with the risk assessment results**

<table>
<thead>
<tr>
<th>Auditable Entity</th>
<th>Inherent Risk</th>
<th>Control Risk</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Line A</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Business Line B</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Marketing</td>
<td>L</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Accounting</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Human Resources</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Networks</td>
<td>H</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>User Access Management</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Databases</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>SDLC</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Change &amp; Problem Management</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Thematic-Privacy</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>
### Annual Audit Planning: Step 2

- **Determine the date of the last audit**

<table>
<thead>
<tr>
<th>Auditable Entity</th>
<th>Inherent Risk</th>
<th>Control Risk</th>
<th>Residual Risk</th>
<th>Date of Last Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Line A</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Oct-2011</td>
</tr>
<tr>
<td>Business Line B</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>Sep-2011</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>Accounting</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>Human Resources</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>Feb-2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Systems</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Jun-2010</td>
</tr>
<tr>
<td>Networks</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>User Access Management</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>Mar-2012</td>
</tr>
<tr>
<td>Databases</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>Jun-2010</td>
</tr>
<tr>
<td>SDLC</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>May-2012</td>
</tr>
<tr>
<td>Change &amp; Problem Management</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Jul-2012</td>
</tr>
<tr>
<td>Thematic-Privacy</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>Aug-2012</td>
</tr>
</tbody>
</table>
Annual Audit Planning: Step 3

- Based on target audit cycle and date of last audit, determine which entities to audit

<table>
<thead>
<tr>
<th>Auditable Entity</th>
<th>Inherent Risk</th>
<th>Control Risk</th>
<th>Residual Risk</th>
<th>Date of Last Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Line A</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Oct-2011</td>
</tr>
<tr>
<td>Business Line B</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>Marketing</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>Accounting</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>Human Resources</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>Feb-2012</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Jun-2010</td>
</tr>
<tr>
<td>Networks</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>Sep-2011</td>
</tr>
<tr>
<td>User Access Management</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>Mar-2012</td>
</tr>
<tr>
<td>Databases</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>Jun-2010</td>
</tr>
<tr>
<td>SDLC</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>May-2012</td>
</tr>
<tr>
<td>Change &amp; Problem Management</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Jul-2012</td>
</tr>
<tr>
<td>Thematic-Privacy</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>Aug-2012</td>
</tr>
</tbody>
</table>

- The targeted audit cycle assumes 1/2/3 year for H/M/L, respectively
Resource Allocation

Assuming that the risk assessments were prepared accurately

Risk assessments should drive depth and breadth of audit coverage

Higher the risk, the greater the focus and effort!
The Process

Auditable Entities

Audit Execution

Audit Universe

Annual Audit Plan

Risk Assessment
Audit Execution

Review RAs
Understand the risk drivers for the entity

Confirm
Risk drivers and the previous assessments

Focus
Areas of higher risks

Update RAs
Reflect updated understanding
Summary

• A quality risk assessment process needed to balance and allocate finite assurance resources against dynamic risks

• Quality of the process requires
  – Definitions and standards
  – Meaningful auditable entities
  – Understanding risk drivers
  – Sensible coverage cycle of the risks
QUESTIONS?