Integration of Risk Management and Internal Audit

Chartered Institute of Management Accountants, New Zealand
Contents

• Understanding the three lines of defense governance model
• What is “Risk”?  
  – Risk Management Framework  
  – Risk Assessment  
• What is “Internal Auditing”?  
  – Where does internal auditing fit into the risk management framework?  
• What is “Internal Control”?  
  – Where does internal control fit in with risk management and internal auditing?
Three Lines of Defense

First Line:
Sourcing, Supply Chain, Stores, Multi Channels, Financial Services, Customer Support

Second Line:
Operations, Finance, People, Information Systems, Risk

Third Line:
Internal Audit

Those creating risk (for reward) must also control it (Control Environment, Risk Assessment, Information & Communication, Control Activities and Monitoring)

Providing support and policy direction for the first line through procedures for managing risk, strategies, budgets, reporting, communication, and training

Providing assurance over the effectiveness of internal controls (both 1st and 2nd LOD), and SME risk and control support, advise and recommendations
What is Risk?

Uncertainty of Outcomes

Upright of Risk

Downside of Risk

Striving to Achieve

Strategy

Possible Opportunities

Possible Threats

1: borrowed from Bill Sharon of SORMs
What is Risk? Dimensions

Striving to Achieve

What should be:
(Defensive)
Compliance & Prevention:
Protect against threats & losses
Enhance Credit Ratings & Customer, Shareholder & Regulator Perceptions

What is:
(Offensive / Defensive)
Operating Performance
Ensure earning stability & business sustainability
Protect Shareholder Value

What could be:
(Offensive)
Strategic Objectives
Maximise Shareholder Value & Business Sustainability

Possible Threats

Possible Opportunities
What is Risk? Defensive Dimension

Striving to Achieve

What should be: (Defensive)

Compliance & Prevention: Protect against threats & losses
Enhance Credit Ratings & Customer, Shareholder & Regulator Perceptions
• Incident logging and reporting
• Protection of Directors & Officers liability
• Security, and privacy
• Business continuity and asset insurance
• Asset Protection/ Minimise Loss

Possible Threats

Possible Opportunities

Upside of Risk

Downside of Risk

1: borrowed from Bill Sharon of SORMs
What is Risk?

Offensive/ Defensive Dimension

Striving to Achieve

What is: (Offensive / Defensive)

Operating Performance
Ensure earning stability & business sustainability

Protect Shareholder Value

- Risk control analysis (management of risk)
- Sourcing, Merchandising, Supply Chain, Stock, Cash, Revenue, Financial and Store Management
- Making risk based decisions to compliment financial decisions
- Maintain relationship with all key stakeholders – directors, staff, customers, suppliers, regulators and public
- Constantly monitoring and remediating
- Understanding boundary risk between Strategic, Operational, Financial & Compliance Risks

Possible Threats

Possible Opportunities

Upside of Risk

Downside of Risk

1: borrowed from Bill Sharon of SORMs
What is Risk?

Offensive Dimension

Upside of Risk

Possible Opportunities

What could be:
(Offensive)

Strategic Objectives
Maximise Shareholder Value & Business Sustainability
• Positively influence Regulators & key Stakeholders
• Integrating Risk Management into Strategic Planning Process
• Support business exploitation of opportunities for growth, reward and sustainability
• Change Risk Management
• Realising & exceeding strategy

Downside of Risk

Possible Threats

Striving to Achieve

Strategy

1: borrowed from Bill Sharon of SORMs
What is Risk?

<table>
<thead>
<tr>
<th>Upside of Risk</th>
<th>Possible Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downside of Risk</td>
<td>Possible Threats</td>
</tr>
</tbody>
</table>

Striving to Achieve

**What should be:** (Defensive)

- Compliance & Prevention: Protect against threats & losses
- Enhance Credit Ratings & Customer, Shareholder & Regulator Perceptions
  - Incident logging and reporting
  - Protection of Directors & Officers liability
  - Security, and privacy
  - Business continuity and asset insurance
  - Asset Protection/ Minimise Loss

What is: (Offensive / Defensive)

- Operating Performance
  - Ensure earning stability & business sustainability
- Protect Shareholder Value
  - Risk control analysis (management of risk)
  - Sourcing, Merchandising, Supply Chain, Stock, Cash, Revenue, Financial and Store Management
  - Making risk based decisions to compliment financial decisions
  - Maintain relationship with all key stakeholders – directors, staff, customers, suppliers, regulators and public
  - Constantly monitoring and remediating
  - Understanding boundary risk between Strategic, Operational, Financial & Compliance Risks

What could be: (Offensive)

- Strategic Objectives
  - Maximise Shareholder Value & Business Sustainability
    - Positively influence Regulators & key Stakeholders
    - Integrating Risk Management into Strategic Planning Process
    - Support business exploitation of opportunities for growth, reward and sustainability
    - Change Risk Management
    - Realising & exceeding strategy

1: borrowed from Bill Sharon of SORMs
Top Down Risk Management Approach

- Strategy
- Risk Category
- Risk & Control Ownership and Location
- Risk Appetite Statements

Risk Assessment Criteria Matrix (Impact & Likelihood)

Risks (Risk Register)

Assessed Controls (Register)

Residual Risk Heat Map

Treatments (Updated Controls Register)

Target Risk Heat Map

By Strategy, Risk Category, Ownership and Location
<table>
<thead>
<tr>
<th>RISK UNIVERSE OR CATEGORIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Risk</strong></td>
</tr>
<tr>
<td>• Funding Risk</td>
</tr>
<tr>
<td>• Capital Risk</td>
</tr>
<tr>
<td>• Interest Rate Risk</td>
</tr>
<tr>
<td>• Foreign Exchange Risk</td>
</tr>
<tr>
<td>• Insurance Risk</td>
</tr>
<tr>
<td>• Investment Risk</td>
</tr>
<tr>
<td>• Credit Risk</td>
</tr>
<tr>
<td>• Counterparty Risk</td>
</tr>
<tr>
<td>• Liquidity Risk</td>
</tr>
<tr>
<td>• Solvency Risk</td>
</tr>
<tr>
<td><strong>Strategic Risk</strong></td>
</tr>
<tr>
<td>• Investor Risk</td>
</tr>
<tr>
<td>• Customer Risk</td>
</tr>
<tr>
<td>• Competitor Risk</td>
</tr>
<tr>
<td>• Supplier Risk</td>
</tr>
<tr>
<td>• Market and Economic Risk</td>
</tr>
<tr>
<td>• Strategic Initiatives and Projects</td>
</tr>
<tr>
<td>• Product Risk</td>
</tr>
<tr>
<td>• Environmental Risk</td>
</tr>
<tr>
<td>• Brand Risk</td>
</tr>
<tr>
<td>• Geopolitical Risk</td>
</tr>
<tr>
<td><strong>Operational Risk</strong></td>
</tr>
<tr>
<td>• People Risk</td>
</tr>
<tr>
<td>• Process Risk</td>
</tr>
<tr>
<td>• Systems and IT Security Risk</td>
</tr>
<tr>
<td>• External Events and Business Interruptions</td>
</tr>
<tr>
<td>• Fraud and Stock Shrinkage Risk</td>
</tr>
<tr>
<td>• Stock Management Risk</td>
</tr>
<tr>
<td>• Merchandising Risk</td>
</tr>
<tr>
<td>• Loss of Revenue Risk</td>
</tr>
<tr>
<td>• Stores Management Risk</td>
</tr>
<tr>
<td>• Sourcing and Logistics Risk</td>
</tr>
<tr>
<td><strong>Compliance Risk</strong></td>
</tr>
<tr>
<td>• NZX, Governance &amp; Financial Reporting Risk</td>
</tr>
<tr>
<td>• Health, Safety &amp; Environmental Law Risk</td>
</tr>
<tr>
<td>• Commercial Law Risk</td>
</tr>
<tr>
<td>• All Financial Services Laws and Regulations Risk</td>
</tr>
<tr>
<td>• Product Safety Risk</td>
</tr>
<tr>
<td>• Company Policies &amp; Procedures Risk</td>
</tr>
<tr>
<td>• Employment Law Risk</td>
</tr>
</tbody>
</table>

*Non-compliance or cost of over compliance*
Sources of and Identifying Risks & Opportunities – Risk Profiling

- Understanding what must go right and what must not go wrong relative to Strategy (at any level)
- External Loss Data, e.g. economic reports, industry reports
- Internal Loss Data, e.g. incident & near misses registers, internal audit reports
- Reference to the Risk Universe / Categories
- Interviews* with Management and Team Members and completion of the “Risk Profiling Questionnaire”
- Collating and analysing results* of the “Risk Profiling Questionnaire”
- Presentation of the Summarised results* of the Risk Profiling Questionnaire the Risk Profiling Workshop
- Facilitation* of Risk Profiling Workshops resulting in collective agreement on the list of risks and opportunities
# Risk Profiling - Questionnaire

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>#</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Your top 5 or so major concerns, i.e. relative to your business strategy, what must go right and what must not go wrong?</td>
<td>8.</td>
<td>Identify new and emerging risks that could have a serious impact on the achievement of your business strategies in the near or middle future?</td>
</tr>
<tr>
<td>2.</td>
<td>List the top 5 or so Major Projects relative to your business strategy, which will have a major impact on your business?</td>
<td>9.</td>
<td>List the regulatory requirements that you must comply with in your business area?</td>
</tr>
<tr>
<td>3.</td>
<td>List the top 5 or so critical business models and spreadsheets, i.e. those models or spreadsheets that help manage your business and which are used to make major business decisions?</td>
<td>10.</td>
<td>What are the key business strategies and initiatives that are top of mind at the moment?</td>
</tr>
<tr>
<td>4.</td>
<td>List the top 5 or Business Processes that support the achievement of your business strategies. Typically included would be key management controls that you relay upon to ensure achievement of your business strategies?</td>
<td>11.</td>
<td>Consider any Black Swan events that could come out of left field, but which are also very plausible (e.g. Christchurch Earthquakes, weather related impacts on business, etc.)?</td>
</tr>
<tr>
<td>5.</td>
<td>List the top or so Outsourced areas that at critical you’re your business?</td>
<td>12.</td>
<td>What are the key Value Drivers that create value to investors in your business and key stakeholders?</td>
</tr>
<tr>
<td>6.</td>
<td>List the Key Systems and software that support both your business strategies and are related to you key business processes (see question 4 above)?</td>
<td>13.</td>
<td>List recent loss areas and incidents including near misses?</td>
</tr>
<tr>
<td>7.</td>
<td>List the top 5 or so Key Contracts (both Supplier and Customer), which are key to achieving your business strategies?</td>
<td>14.</td>
<td>Looking at the Risk Universe, are there any other concerns or opportunities, not yet included in the questions above?</td>
</tr>
</tbody>
</table>
Assessing the individual Risks – derived from the Risk Profiling exercise

• Risks are measured for Likelihood using the RACM
• Risks are measured for Impact using the RACM
• Best done as a continuation of the Risk Profiling Workshop.
• A useful technique is the Bow Tie
Assessing the individual Risks – Workshop Outputs

• Agreed Risk Appetite
• Completed Bow Ties
• RACM populated with Risks – Inherent, Residual and Target
• Risk & Control Register
• Top 10 or 20 Risk for immediate attention
• Further actions or treatments required.
<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Likelihood</th>
<th>Frequency</th>
<th>Financial Impact</th>
<th>Brand Impact</th>
<th>People Impact</th>
<th>Customer Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>Likely</td>
<td>Expected to happen more than once in the next year</td>
<td>&lt;5% of EBIT</td>
<td>Recoverable damage to Minor Earning Brands for more than 6 months</td>
<td>Minor Injuries</td>
<td>&lt;5% of Market Share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>10</td>
<td>Recoverable damage to Major Earning Brands for more than 6 months</td>
<td>Single Serious Injury</td>
<td>5-10% Loss of Market Share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>6</td>
<td>Irrecoverable damage to Minor Earning Brands</td>
<td>Multiple Serious Injuries</td>
<td>10-15% Loss of Market Share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>4</td>
<td>Irrecoverable damage to Major Earning Brands</td>
<td>Single Death</td>
<td>15-20% Loss of Market Share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>Irrecoverable damage to all Brands</td>
<td>Multiple Deaths</td>
<td>&gt;20% Loss of Market Share</td>
</tr>
<tr>
<td>Likely</td>
<td>Expected to happen at least once in the next year</td>
<td>4</td>
<td>8</td>
<td>Recoverable damage to Major Earning Brands for more than 6 months</td>
<td>Single Serious Injury</td>
<td>5-10% Loss of Market Share</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>Irrecoverable damage to Minor Earning Brands</td>
<td>Multiple Serious Injuries</td>
<td>10-15% Loss of Market Share</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Irrecoverable damage to Major Earning Brands</td>
<td>Single Death</td>
<td>15-20% Loss of Market share</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>Irrecoverable damage to all Brands</td>
<td>Multiple Deaths</td>
<td>&gt;20% Loss of Market Share</td>
</tr>
<tr>
<td>Possible</td>
<td>Expected to happen at least once in the next three years</td>
<td>3</td>
<td>6</td>
<td>Recoverable damage to Minor Earning Brands for more than 6 months</td>
<td>Single Serious Injury</td>
<td>&lt;5% of Market Share</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>12</td>
<td>Irrecoverable damage to Major Earning Brands for more than 6 months</td>
<td>Multiple Serious Injuries</td>
<td>5-10% Loss of Market Share</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>Irrecoverable damage to Minor Earning Brands</td>
<td>Single Death</td>
<td>10-15% Loss of Market Share</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Expected to happen at least once in the next 10 years</td>
<td>2</td>
<td>4</td>
<td>Recoverable damage to Minor Earning Brands for more than 6 months</td>
<td>Single Serious Injury</td>
<td>&lt;5% of Market Share</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>Irrecoverable damage to Major Earning Brands for more than 6 months</td>
<td>Multiple Serious Injuries</td>
<td>5-10% Loss of Market Share</td>
</tr>
<tr>
<td>Rare</td>
<td>Not expected to happen within the next 10 years</td>
<td>1</td>
<td>2</td>
<td>Recoverable damage to Minor Earning Brands for more than 6 months</td>
<td>Minor Injuries</td>
<td>&lt;5% of Market Share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>4</td>
<td>Irrecoverable damage to Major Earning Brands for more than 6 months</td>
<td>Single Serious Injury</td>
<td>5-10% Loss of Market Share</td>
</tr>
</tbody>
</table>

**Impact Risk Rating**

**Overall Risk Rating:**
- **High**: Executive Management and the Audit Committee
- **Medium & Low**: Senior and Operational Management

**Impact Risk Rating**

- **Financial**: 
  - <5% of EBIT
  - 5-10% of EBIT
  - 10-20% of EBIT
  - 20-30% of EBIT
  - >30% of EBIT

- **Brand**: 
  - Recoverable damage to Minor Earning Brands for more than 6 months
  - Recoverable damage to Major Earning Brands for more than 6 months
  - Irrecoverable damage to Minor Earning Brands
  - Irrecoverable damage to Major Earning Brands
  - Irrecoverable damage to all Brands

- **People**: 
  - Minor Injuries
  - Temporary Loss of Key Mgt/ Staff
  - Single Serious Injury
  - Loss of some Key Mgt/ Staff for up to 3 months
  - Multiple Serious Injuries
  - Loss of most Key Mgt/ Staff for up to 6 months
  - Single Death
  - Loss of all Key Mgt/ Staff for up to 1 year
  - Multiple Deaths
  - Loss of key Directors and Exec Mgt/ Mgt/ Staff for > 1 year

- **Customer**: 
  - <5% of Market Share
  - 5-10% Loss of Market Share
  - 10-15% Loss of Market Share
  - 15-20% Loss of Market Share
  - >20% Loss of Market Share
## Bow-Tie Risk Event

### Causes

<table>
<thead>
<tr>
<th>Item</th>
<th>Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Item 1</td>
</tr>
<tr>
<td>2.</td>
<td>Etc.</td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
</tbody>
</table>

**Preventative Controls**

**Control Owner**

**Control Effectiveness?**

- Not Effective
- Partially Effective
- Effective

### Effect

<table>
<thead>
<tr>
<th>Item</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Item 1</td>
</tr>
<tr>
<td>2.</td>
<td>Etc.</td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
</tbody>
</table>

**Detective/Corrective Controls**

**Control Owner**

**Control Effectiveness?**

- Not Effective
- Partially Effective
- Effective

### Inherent Likelihood Risk

**Existing Preventative Controls**

Linked to the Causes (to reduce causes)

<table>
<thead>
<tr>
<th>Item</th>
<th>Existing Preventative Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Item 1</td>
</tr>
<tr>
<td>2.</td>
<td>Etc.</td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
</tr>
</tbody>
</table>

**Control Owner**

**Control Effectiveness?**

- Not Effective
- Partially Effective
- Effective

### Inherent Consequence Risk

**Existing Detective & Corrective Controls**

Linked to the effects to reduce effects

<table>
<thead>
<tr>
<th>Item</th>
<th>Existing Detective &amp; Corrective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Item</td>
</tr>
<tr>
<td>2.</td>
<td>Etc.</td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
</tr>
</tbody>
</table>

**Control Owner**

**Control Effectiveness?**

- Not Effective
- Partially Effective
- Effective

### Residual Likelihood Risk

**Mitigations (future management actions)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Owner</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Item</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Etc.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rationale (why this action?)**

**Target Likelihood Risk**

### Residual Consequence Risk

**Mitigations (future management actions)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Owner</th>
<th>Date</th>
</tr>
</thead>
</table>

**Rationale (why this action?)**

**Target Consequence Risk**
What is Internal Audit?*

- Internal auditing is an independent, objective assurance and consulting activity
- Designed to add value and improve an Organization's operations
- It helps an Organisation accomplish its objectives
- By bringing a systematic, disciplined approach to evaluate and improve the
  - effectiveness of risk management
  - controls
  - and governance processes.

* Definition from the Institute of Internal Auditors Inc.
Internal Audit Activities

The internal audit activity evaluates the adequacy and effectiveness of controls in responding to risks within the an Organization's governance, operations, and information systems regarding the:

• Achievement of an Organization's strategic objectives;
• Reliability and integrity of financial and operational information;
• Effectiveness and efficiency of operations and projects;
• Safeguarding of assets; and
• Compliance with laws, regulations, company policies, procedures, and contracts.
Internal Audit Cycle

Align to Business Strategy

Act as Positive Change Agent by:
Influencing cost effective, useful and relevant improvements in PSRC,
Supporting in the achievement of Business Strategy

Understand PSRC:
Process, Systems, Risks, and Controls
as they relate to Business Strategy

Evaluate and comments on PSRC:
Efficiency of Processes & Systems,
Awareness of Risk,
Adequacy of Control Design, and
Operational Effectiveness of Controls
Internal Audit Principles
To be read with the Internal Audit Cycle Slide

• Alignment
• Integration
• Relevance
• Value Add
Alignment

• Assurance Provider to the Board Audit Committee and Risk & Control service provider to Management

• Audit Plan aligned to Business Strategy, Processes, Risks and Controls that matter
Integration

• Audit Plan integrated with Management’s efforts to control risk

• Evaluation of Control Design before implementation

• Evaluation of Operational Effectiveness of Management’s implemented Controls
Relevance

• Audit Plan in support of Business Strategies
• Understanding Process, Systems, Risk and Controls as they relate to Business Strategies
• Useful and relevant opinion and commentary on the Processes, Systems, Risk and Controls that matter to the Group
Value Add

- Providing insight, cost-effective and useful recommendations regarding:
  - Efficiency of Processes and Systems
  - Awareness of Risks that may impact on the achievement of Business Strategies and which management attention
  - Adequacy of Risk Control Design
  - Operational Effectiveness of Risk Controls
<table>
<thead>
<tr>
<th>Type</th>
<th>Nature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stores Audits</td>
<td>Risk based reviews Targeted Review or Spot checks.</td>
</tr>
<tr>
<td>Functional Audits</td>
<td>End to end process review (i.e. multiple processes) of a single function, division or brand; providing audit opinion on the effectiveness of controls within that function, division or brand.</td>
</tr>
<tr>
<td>Process Audits</td>
<td>Single process/ risk review over multiple functions/ divisions/ brands, providing audit opinion on the effectiveness of that single process across multiple functions/ divisions or brands</td>
</tr>
<tr>
<td>Risk and Control Review</td>
<td>Risk and control identification and assessment of brands, functions or processes, providing a risk opinion as to the adequacy of risk management/ internal controls using the TW Group risk management framework.</td>
</tr>
<tr>
<td>Project Audits</td>
<td>Formal review of the effectiveness of project management and the adequacy of control design build into the solution before going live. Provides an audit opinion on the effectiveness of project risk management and adequacy of control design and may include a post implementation review. Dual reporting to the Project Manager and to the Project Steering Committees.</td>
</tr>
<tr>
<td>Consultative Engagements</td>
<td>Informal participation in new initiatives or projects focusing mainly on the provision of business insight and adequacy of control design build into the solution before going live.</td>
</tr>
</tbody>
</table>
Integration with Risk Management -

- Strategy
  - See Slide
- Risk Category
  - See Slide
- Risk & Control
  - Ownership and Location
- Risk Appetite Statements

Risk Assessment Criteria Matrix
(Impact & Likelihood)
- See Slide 14

Internal Audit - Evaluation of Control Design and Effectiveness

Risk Heat Maps:
- Inherent Risk Heat Map
- Residual Risk Heat Map
- Target Risk Heat Map

Assessed Controls (Register)

Treatments (Updated Controls Register)

By Strategy, Risk Category, Ownership and Location
Internal Audit Methodology*  
Overview of Phases

1. Co-Develop Risk Areas  
2. Top-Down Risk Assessment  
3. Audit Plan  
4. Audit Project Execution & Reporting  
5. Exec. Mgt. & Audit Committee Reporting

Internal Audit Methodology within Internal Audit Framework

Understanding of Processes, Systems, Risk and Controls

Technology Support, Tools and Analysis
COSO defines internal control as having five components:

• Control Environment
• Risk Assessment
• Information and Communication
• Control Activities
• Monitoring
Control Activities (Examples)

- Segregation of Incompatible Duties
- Authorization of transactions
- Retention of records
- Supervision or monitoring of operations.
- Physical safeguards
- Top-level reviews-analysis
- IT general controls
- IT application controls
Nature of Controls

- **Preventative** – designed to mitigate the causes of risks, i.e. pre-risk event

- **Detective / Corrective** – designed to mitigate the effects of risk, i.e. post-risk event
Techniques to Evaluate Controls

• Walk-throughs
• Process Mapping with Risk and Controls Matrices
• Bow Ties
• Testing of Controls:
  – Inquiry
  – Observations
  – Re-performance
  – Detail Testing
• Analytical reviews using Computer Assisted Audit Techniques (CAATs)
Top Down Risk Management Approach

- Strategy
- Risk Category
- Risk & Control Ownership and Location
- Risk Appetite Statements

Risk Assessment Criteria Matrix (Impact & Likelihood)

Risks (Risk Register)

Inherent Risk Heat Map
Assessed Controls (Register)
Residual Risk Heat Map
Treatments (Updated Controls Register)
Target Risk Heat Map

By Strategy, Risk Category, Ownership and Location
Conclusion & Questions

• Three Lines of Defense
• Risk & Risk Management
• Internal Auditing
• Internal Controls
• Questions