

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Project Structure and Methodology	<ul style="list-style-type: none"> <li>• Ability to consistently and efficiently develop guidance and approach</li> <li>• Ability to stay current on latest rules and thought leadership</li> <li>• Knowledge and experience with controls, accounting/financial reporting and applicable regulations</li> <li>• Ability to efficiently and effectively communicate guidance and approach enterprise wide</li> <li>• Proximity to project sponsor or steering committee</li> <li>• Consistent executive level and audit committee support and engagement</li> <li>• Central point of contact</li> </ul>	<ul style="list-style-type: none"> <li>• Generally, a centralized function (“SOX central”)</li> <li>• Currently led by a group headed by project sponsor</li> <li>• In most cases the function is in Finance (given the deliverable is a management assertion related to financial reporting), with close and heavy support from Internal Audit</li> <li>• Generally includes a dedicated project office, working group (with business unit and support functions, including IA, finance, legal, representation), steering committee and project sponsor</li> </ul>	<ul style="list-style-type: none"> <li>• Integrate with other risk management and compliance activities</li> <li>• Function reporting to either Chief Financial Officer or Chief Risk Officer with increasing ownership of execution by the business units (but with guidance and standardization from the central function)</li> <li>• Some companies are evaluating the role of “chief internal control officer”</li> <li>• Internal Audit continues to provide advice and input as part of “normal” audit activities</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Project Management	<ul style="list-style-type: none"> <li>• Ability to prepare an enterprise wide project plan and action plan</li> <li>• Ability to provide enterprise wide oversight, monitoring and reporting</li> <li>• Communicate enterprise wide methodology and standards and monitor adherence</li> <li>• Empowerment to initiate actions, and respect to get results</li> <li>• Ability to identify status and project issues</li> <li>• Access to executive management to elevate issues</li> </ul>	<ul style="list-style-type: none"> <li>• Centralized unit</li> <li>• Aligned with project sponsor</li> <li>• Support from project management specialists (e.g., IT)</li> <li>• Owns “the process” and execution</li> <li>• Documentation, testing, issue tracking and deficiency evaluation done using Excel spreadsheets and Word documents (some SOX specific technology tools)</li> </ul>	<ul style="list-style-type: none"> <li>• Continue to own “the process” (true project management roles, such as standards, deadlines, status reporting, deficiency evaluation, etc.)</li> <li>• Also own documentation format and standards, and changes to/design of test plans</li> <li>• But execution (updating the content of the documentation and executing test plan) transitioned to the business units</li> <li>• Use of an automated tool for documentation, testing, issue tracking and deficiency evaluation (and leveraging some other risk management tool – e.g., operational risk – rather than using a SOX specific tool)</li> </ul>

**Sarbanes-Oxley Section 404**

**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**

**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
<p>Scoping and Risk Assessment</p>	<ul style="list-style-type: none"> <li>• Ability to consistently and efficiently apply quantitative and qualitative guidelines to financial statement line items/ footnotes and locations to determine scope</li> <li>• Ability to liaise with other groups to validate quantitative and qualitative assessments applied</li> <li>• Knowledge of financial reporting process and the accumulation of financial information</li> <li>• Knowledge of risks associated with financial transactions</li> <li>• Ability to conduct a periodic (i.e., quarterly) review to validate scoping and risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Generally led by Finance</li> <li>• Input from relevant business units and other functional units (e.g., Internal Audit, Risk Management, Compliance)</li> <li>• Risk assessment includes a high/medium/low rating scale determined subjectively</li> <li>• Some consideration and leverage of company level and general computer controls, with increased focus in Year 2</li> </ul>	<ul style="list-style-type: none"> <li>• Reconciliation of SOX risk assessment with other risk initiatives (Basel, Enterprise Risk Management, capital allocations)</li> <li>• Coordinated efforts of Finance and Risk Management</li> <li>• Risk assessment to be based on a quantitative scoring model leveraging other risk evaluation initiatives within the organization (e.g., operational risk, capital allocations, BASLE, Internal Audit, etc.)</li> <li>• Inclusion of “insignificant” accounts, locations and application systems on a rotational (but not pre-defined) basis for unpredictability</li> <li>• Substantive leverage of company level and general computer controls – significant impact on nature, timing and extent of detail testing</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Documentation	<ul style="list-style-type: none"> <li>• Knowledge of business processes and controls</li> <li>• Ability to identify changes (people, processes, systems, business activities, products, policies, etc.) and assess the impact on the internal control structure and related documentation</li> <li>• Ability to action any deficiencies and changes</li> <li>• Proximity to control ownership</li> </ul>	<ul style="list-style-type: none"> <li>• Year 1 completed by central group (e.g., SOX central, Internal Audit)</li> <li>• Year 2 saw some migration to updating documentation by business units</li> <li>• Reviewed and signed off by business units</li> <li>• Annual exercise</li> <li>• Standards and training provided by central group</li> </ul>	<ul style="list-style-type: none"> <li>• Documentation updates owned by the business units as they own the control and most knowledgeable of risks and any changes</li> <li>• Updated quarterly as part of the 302 process (to identify changes that may warrant a 302 or 404 response)</li> <li>• Standards and training continue to be provided by central group for standardization</li> <li>• Quality control review by the central group or Internal Audit</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Design Evaluation and Walkthrough	<ul style="list-style-type: none"> <li>• Knowledge of business processes, key risks, fraud risks, and related control points</li> <li>• Knowledge of outsourced processing</li> <li>• Determination of key controls and linkage to information processing objectives and financial statement assertions</li> <li>• Ability to identify intersections of business processes and controls</li> </ul>	<ul style="list-style-type: none"> <li>• Year 1 design evaluation completed jointly by central group and business units</li> <li>• Year 2 generally updated by business units with oversight from central group</li> <li>• Outsourced processing and receipt of vendor control reports done at the end of the process</li> <li>• Walkthroughs conducted by group conducting testing</li> <li>• Business process intersections and handoffs not as coordinated and therefore walkthroughs done for each process and generally without regard to intersections</li> </ul>	<ul style="list-style-type: none"> <li>• Design evaluation updated quarterly as part of documentation review (to reflect business process changes and/or refined controls)</li> <li>• Done by business units</li> <li>• Vendor agreements for outsourced processing renegotiated to require internal controls reports and earlier in the year (as well as audit rights)</li> <li>• Walkthroughs conducted by group conducting testing (transitioning to the business units)</li> <li>• Walkthroughs performed “seamlessly”, taking into consideration intersections and handoffs across multiple business processes</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
<p>Operating Effectiveness Testing</p>	<ul style="list-style-type: none"> <li>• Knowledge of controls and testing techniques (i.e., auditor knowledge/experience)</li> <li>• Understanding of how entity/company level controls impact activity level controls</li> <li>• Ability to develop appropriate tests to validate operational effectiveness</li> <li>• Ability to apply risk assessment to testing techniques to vary the nature, timing and extent of testing</li> </ul>	<ul style="list-style-type: none"> <li>• Generally conducted by Internal Audit or hired external consultants</li> <li>• Testing results reviewed by business unit</li> <li>• Entity/company level controls documented and tested at the end of the process</li> <li>• General computer controls tested and concluded upon at the end of the process</li> <li>• In Year 1, preponderance of the testing done using reperformance and later in the year, with more thoughtful migration towards other testing approaches in Year 2 (for all of nature, timing and extent)</li> </ul>	<ul style="list-style-type: none"> <li>• Integrate with existing business unit operational activities and existing/to be developed self-assessment processes</li> <li>• Integrate with “normal” Internal Audit plans versus separate SOX testing</li> <li>• Liaise testing strategy with external audit to optimize reliance model (nature, timing and extent)</li> <li>• Entity/company level controls documented and testing at the beginning of the process</li> <li>• General computer controls tested and concluded upon at the beginning of the process</li> <li>• More varied nature of testing with a more thoughtful and conscious mix of inquiry, observation, examination and reperformance, as well as interim versus yearend update testing</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Deficiency Analysis and Management	<ul style="list-style-type: none"> <li>• Knowledge of deficiency assessment framework</li> <li>• Knowledge of business process and related controls and interdependencies with other processes</li> <li>• Ability to consolidate deficiencies and assess enterprise wide reporting impact</li> <li>• Analytical skills and ability to recognize trends and themes across business units, locations, and accounts (with the current year and cumulatively)</li> <li>• Communicate deficiency to affected business units and enterprise wide deficiency management framework</li> <li>• Ability to develop and execute action plans to address identified deficiencies</li> <li>• Ability to monitor and report on action plans and status</li> </ul>	<ul style="list-style-type: none"> <li>• Conducted by central unit who labels deficiencies and leads the process of reaching conclusions</li> <li>• Determine remediation requirements, priority and timing</li> <li>• Tiered reporting at the working group, steering committee, executive management and audit committee levels</li> <li>• Tied into quarterly 302 disclosure review activities</li> <li>• Analysis of individual and aggregated deficiencies, with some use of the assessment framework</li> </ul>	<ul style="list-style-type: none"> <li>• Continue to be conducted by central group (the process) with business unit ownership of conclusions and remediation requirements</li> <li>• Coordinate with other regulatory and compliance issue management and risk activities (e.g., Basel, FDICIA)</li> <li>• Real time feedback loops to enterprise wide risk assessment activities</li> <li>• Calibration of “inconsequential deficiencies” to the original definition of the underlying control as a “key” control</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Reporting	<ul style="list-style-type: none"> <li>• Preparation of tiered levels of reporting depending on the recipient (status, challenges, deficiencies)</li> <li>• Message management, both internally and externally</li> </ul>	<ul style="list-style-type: none"> <li>• Business units report to central group or project oversight function on status</li> <li>• Presentation done by central unit to steering committee, executive management and audit committee</li> <li>• Deficiencies reported “at the end” versus early warning</li> <li>• 302 assessments and disclosures do not forewarn material weaknesses</li> </ul>	<ul style="list-style-type: none"> <li>• Business unit presentation to steering committee, executive management and audit committee (or as part of integrated risk/compliance/strategy presentations)</li> <li>• Early warning to all audiences to address the risk, manage the message and determine implications</li> <li>• 302 assessments and disclosures accurately forewarn a material weakness</li> </ul>

**Sarbanes-Oxley Section 404**  
**Banking Industry: Migration to Sustainability (from Year 2 to “Year 5”)**  
**Discussion Outline – April 2006**

Activity	Criteria/Characteristics	Current Industry Observations	Future Industry Direction
Sign off	<ul style="list-style-type: none"> <li>• Understanding of organization structure</li> <li>• Understanding of the “end game” – the final deliverable</li> <li>• Management of the overall project timeline to allow for thoughtful consideration of major decision and deficiencies throughout the project</li> </ul>	<ul style="list-style-type: none"> <li>• Annual two track tiered signoffs of the process and deficiencies: 1) from business units to executive management and 2) from central unit to working group to steering committee</li> <li>• Central unit prepares and maintains the overall documentation that includes documentation of all major decisions</li> <li>• Central unit maintains control documentation and testing results</li> </ul>	<ul style="list-style-type: none"> <li>• Quarterly signoffs leveraging the 302 process (using checklists and sub-certifications, modified to include internal control documentation)</li> <li>• Central unit prepares and maintains documentation of major decisions and final deficiency conclusions</li> <li>• Business units maintain control documentation and testing results, with central unit maintaining overall summaries and conclusions</li> </ul>