APPLICABILITY OF SELECTED SARBANES-OXLEY ACT REQUIREMENTS TO FINANCIAL INSTITUTIONS

Note: Institutions that meet more than one audit category should default to the first listed category (highest category in the hierarchy established in this chart.) For example, a public company that is also subject to FDICIA would be required to comply with all titles in Sarbanes-Oxley and default to the public company category.

Institution's Audit Category	Title II – Auditor Independence [1]	Title III – Corporate Responsibility [1]	Title IV – Enhanced Financial Disclosure [1]
Public companies [2]	Required [1]	Required [1]	Required [1]
FDICIA required audits [3]	Institutions are required to comply with Sections 201, 202, 203, and 206. Section 204 does not apply under the existing audit standards, but the FDIC may amend Part 363 to encompass standards that mirror Section 204. [6, 7]	Institutions are not required to comply with Section 301; however, they must have an audit committee that is independent of management. Institutions are not required to comply with Section 302. Institutions are not required to comply with Section 303 but it is an unsafe and unsound practice to exercise improper influence on the conduct of an audit. [7]	Institutions are not required to comply with Sections 401, 402, 404, and 406. However, the FDIC may amend Part 363 to require compliance with those sections. Institutions are not required to comply with 407; however, institutions with more than $3 billion in assets are required to have at least two members of the audit committee with banking or related financial management expertise. The audit committee must have access to its own outside counsel. [7] When subject to both Section 404 and FDICIA requirements, institutions may chose to prepare one report to meet both requirements or separate reports for the FDIC and SEC.[8]
OTS required audits [4]	Independent public accountants are required to meet the independence requirements and interpretations of the SEC and its staff. [9]	Institutions are encouraged to periodically review their policies and procedures relating to corporate governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. [10]	Institutions are encouraged to periodically review their policies and procedures relating to corporate governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. [10]

Footnotes are on page 6.
***Highlights of Selected Sarbanes-Oxley Act Requirements* are on pages 3-5.**

Institution's Audit Category	Title II – Auditor Independence [1]	Title III – Corporate Responsibility [1]	Title IV – Enhanced Financial Disclosure [1]
All other audits [5] - supervised by OTS, FRB, or OCC.	An institution may be required by another law or regulation, an order, or another supervisory action to have its financial statements audited by an independent public accountant. If warranted for safety and soundness reasons, the institution's primary federal regulator may require that the institution and its independent public accountant comply with the auditor independence requirements of Section 201. [6, 9]	Compliance may be required. If not so required, institutions are encouraged to periodically review their policies and procedures relating to corporate governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. [10]	Institutions are encouraged to periodically review their policies and procedures relating to corporate governance, internal controls, and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. [10]
All other audits [5] - supervised by FDIC.	Compliance not required. However, institutions are encouraged to follow the internal audit outsourcing prohibition in Section 201, audit partner rotation and "time out" periods similar to Section 203, institute auditor reporting practices similar to Section 204, and to comply with the conflicts of interest requirements in Section 206 given the institution's size, complexity, and risk profile. [7]	Compliance not required. However, institutions are encouraged to establish an audit committee consisting entirely of outside directors, similar to Section 301, asked to consider implementing Section 302, and strongly encouraged to comply with Section 303 (improper influence over external auditing work). [7]	Institutions are encouraged to implement to the extent feasible given the institution's size, complexity, and risk profile. Institutions are encouraged to implement Sections 401, 404, and 406, and continue to comply with Section 402 (Regulation O). [7]

Footnotes are on page 6.
***Highlights of Selected Sarbanes-Oxley Act Requirements* are on pages 3-5.**

HIGHLIGHTS OF SELECTED SARBANES-OXLEY ACT REQUIREMENTS

Title II – Auditor Independence

Section 201: Services outside the scope of practice of auditors

- Prohibits the external auditor from providing specified nonaudit services (impermissible nonaudit services) contemporaneously with the external audit. Impermissible nonaudit services include:
  1. Bookkeeping or other services.
  2. Systems design and implementation.
  3. Appraisal or valuation services.
  4. Actuarial services.
  5. Internal audit outsourcing services.
  6. Management functions or human resources.
  7. Broker/dealer, investment advisor or investment banking services.
  8. Legal services.
  9. Expert services unrelated to the audit.
  10. Other services, as the Board deems impermissible.

Section 202: Pre-approval requirements

- Audit committee must preapprove all services that are not prohibited that the external auditor provides, including audit, tax services, and other permissible nonaudit services. Some institutions may not have an audit committee, but would instead use the board of directors.

Section 203: Audit partner rotation

- The lead or coordinating audit partner and the reviewing partner rotate off the audit every five years with a five-year “time out.” Other significant partners subject to seven-year rotations with two-year “time outs.”

Section 204: Auditor reports to the audit committee

- The external auditor must report the following to the company’s audit committee:
  - — Critical accounting policies and practices;
  - — Alternative accounting treatments under GAAP for material items, including:
    - ♦ The ramifications of the use of alternative treatments, and
    - ♦ The treatment preferred by the auditors; and
  - — Other material communications between the auditor and management.

Section 206: Conflicts of interest

- A registered public accounting firm may not perform an audit for an institution if a person in a financial oversight role of the issuer (e.g., CEO, controller, CFO, or chief accounting officer, etc.) was a member of the audit engagement team (> 10 hours) of the issuer during a one-year “cooling off” period prior to initiation of the new audit.

Section 208 Audit Disclosures

- Fee disclosures grouped into the following four categories:
  - Audit fees.
  - Audit-related fees (e.g. employee benefit plan audits, merger and acquisition due diligence, etc.).
  - Tax fees.
  - All other fees.
- Qualitative disclosure of services provided.

Title III - Corporate responsibility

Section 301: Public company audit committees

- Audit Committee vested with responsibility for the appointment, compensation, and oversight of the external audit firm.
- All members of the audit committee must be a member of the board of directors and be independent. The institution must fund the committee adequately and the committee must be able to hire independent counsel and other advisors.

Section 302: Certifications

- Each annual report and quarterly report must include various certifications by the CEO and CFO:
  - That the financial statements and information "fairly present in all material respects the financial condition and results of operations…"
  - That they are responsible for establishing and maintaining internal controls.

Section 303: Improper Influence on Conduct of Audits

- Prohibits any officer or director (or anyone under their direction) from taking any action to fraudulently mislead an auditor for the purpose of rendering a financial statement that is materially misleading.

Title IV - Enhanced financial disclosure

Section 401: Disclosures in periodic reports

- Financial reports must reflect all material correcting adjustments.
- Annual and quarterly reports must disclose material off-balance-sheet transactions and other relationships with unconsolidated entities.

Section 402: Enhanced Conflict of Interest Provisions

- Limits personal loans to directors and executive officers.

Section 404: Management assessment of internal controls

- Annual reports must contain an internal control report.
  - Must disclose material weakness(es)
  - Management **cannot** conclude internal controls are effective if material weakness(es) exist.
- Can issue one combined report or separate FDICIA and SOX §404 reports.
- Internal control report that meets Part 363 may in some instances be filed with the SEC. Part 363 (FDICIA) requires:
  - A statement of management's responsibility for preparing the institution's annual financial

statements, for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and for complying with designated laws and regulations relating to safety and soundness.

- — Management's assessments of:
  - ♦ The effectiveness of the institution's internal control structure and procedures for financial reporting as of the end of the fiscal year, and
  - ♦ The institution's compliance with the designated safety and soundness laws and regulations during the fiscal year.

Section 406: Code of ethics for senior financial officers

- Requires that period reports disclose whether the issuer has adopted a code of ethics for senior officers, and if not, why not.
- Requires disclosure of any changes or waivers of the code of ethics**.**

Section 407: Disclosure of audit committee financial expert

- Periodic reports must disclose whether the audit committee has at least one member who is a "financial expert" (and identify).

Section 906: Certifications

- Each annual report and quarterly report must include a certification by senior corporate officers:
  - — That the financial statements and information "fairly present in all material respects the financial condition and results of operations…"
- Note that this certification is in addition to the one required in Section 302. Section 906 is an amendment to the federal criminal law.

Footnotes

[1] Highlights of Selected Sarbanes-Oxley Act Requirements (Pages 3-5 of this document).

[2] Public companies: Banks, savings associations, and holding companies that have a class of securities registered with either the SEC or the federal banking agencies (including OTS) under Section 12 of the Securities Exchange Act of 1934 or are required to file reports with the SEC under Section 15(d) of that Act (commonly referred to as "public companies"); or, file with OTS pursuant to a reporting obligation under Section 563g.18, and, are required to have an external audit.

[3] FDICIA required audits: Banks and savings associations with assets of $500 million or more that are subject to the FDIC's external audit and reporting requirements under 12 CFR Part 363.

[4] OTS required audits: Savings associations and savings association holding companies required by OTS to have an audit pursuant to 12 CFR 562. Includes audits of:

- Savings associations with composite CAMELS rating of 3, 4, or 5;
- Savings association holding companies that control savings association subsidiary(ies) with aggregate consolidated assets of $500 million or more;
- *De novo* savings associations; and
- Other audits deemed necessary for safety and soundness reasons.

[5] All other audits include: Banks, savings associations, and holding companies that are (1) required to have an audit by another law or regulation, an order, or another supervisory action, warranted for safety and soundness reasons; and (2) not required to have an external audit, but do so.

[6] Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 17, 2003).

[7] FDIC Financial Institution Letter (FIL) – 17 – 2003, Corporate Governance, Audits and Reporting Requirements (March 5, 2003).

[8] SEC's Final Rule Discussing Reports on Internal Control That May Satisfy Both SEC Requirements and FDIC Part 363 Requirements, OTS CEO Letter No. 180 (August 21, 2003).

[9] Section 102 of the Sarbanes-Oxley Act requires audits of public companies to be performed by PCAOB "registered" accountants. This requirement does not apply to nonpublic companies. Auditors of nonpublic institutions must follow the independence standards identified in the AICPA Code of Professional Conduct.

[10] Joint Interagency (OTS, FRB, OCC) Statement on Application of Recent Corporate Governance Initiatives to Nonpublic Banking Organizations, OTS CEO Letter No. 174 (May 5, 2003).