

IT Governance and SOX

Dr. Stefan Friesenecker,
UBS Group CRO Program Management
November 29th, 2005

Agenda

- ◆ UBS Structure and Background
- ◆ IT Organization Structure
- ◆ UBS - Group IT Risk Control Reporting Structure
- ◆ Sarbanes Oxley Act 2002
- ◆ Hierarchy of Control within UBS
- ◆ The Operational Risk Framework
- ◆ OR Control Documentation and Self-Certification
- ◆ IT Control Framework
- ◆ Conclusions

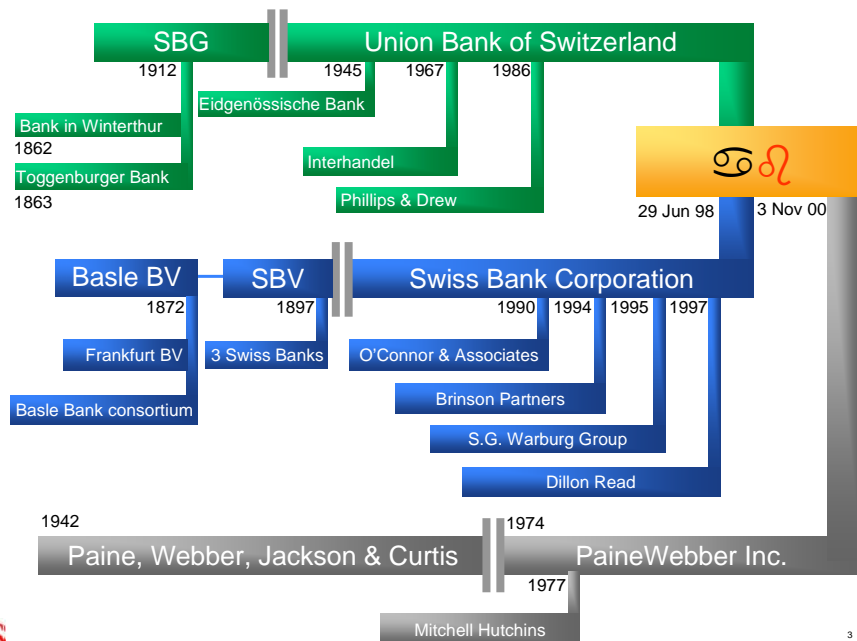
UBS - Key Figures

| | 30.09.2005 |
|---------------------------------|------------------|
| Market capitalization (CHF bn) | 116.7 |
| Total Assets (CHF bn) | 2'125 |
| Invested Assets (CHF bn) | 2'666 |
| Headcount | 70'502 |
| | 30.09.2005 (ytd) |
| Net Profit (CHF m) | 7'542 |
| Cost / Income ratio (%) | 69.3 |
| Return on Equity annualized (%) | 29.0 |



2

UBS - Roots

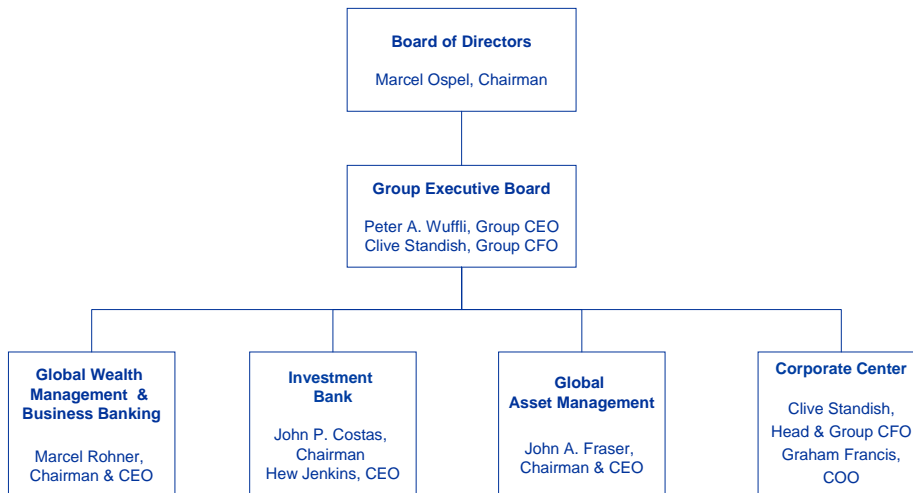


3

UBS - Global Locations

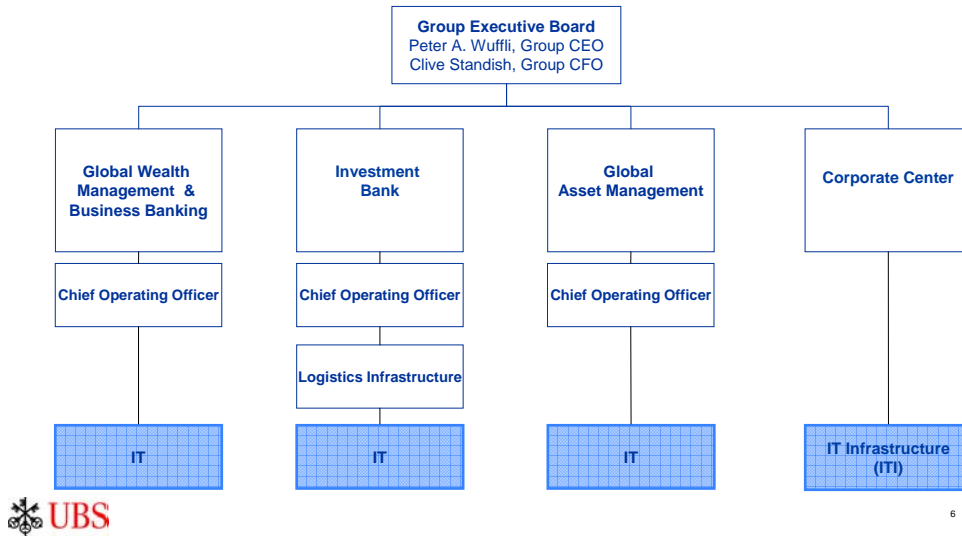


UBS - Structure

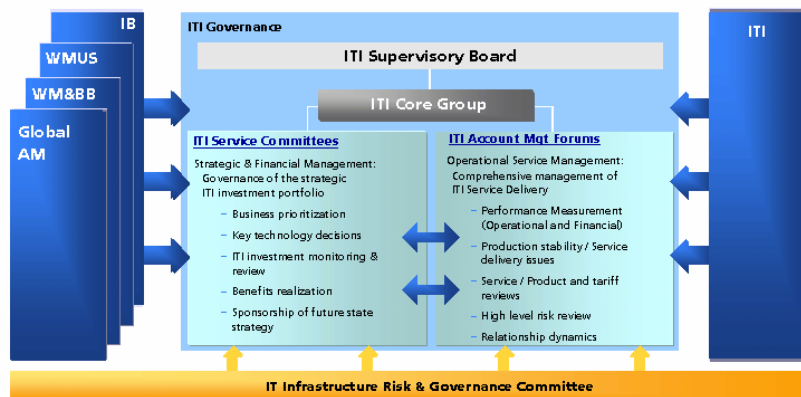


UBS – IT Organization Structure

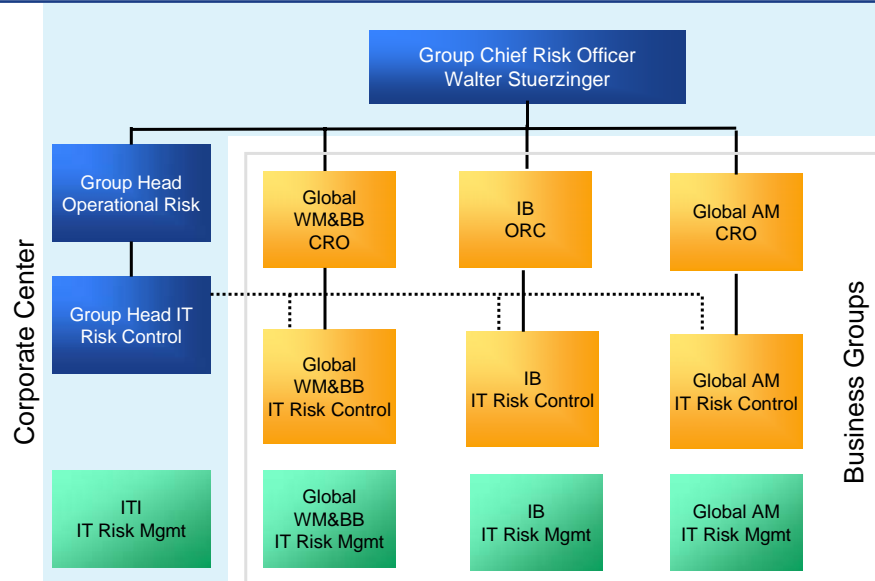
- ◆ Separation of IT infrastructure and IT development in 2004
- ◆ IT Infrastructure centralized at Group level
- ◆ IT development decentrally managed by each Business Group



UBS – IT Organization Structure - Governance



UBS - Group IT Risk Control Reporting Structure



NB: The dotted line above indicates that the divisional Risk Controllers have a functional reporting line into Group Head IT Risk Control. The IT Risk Management functions are displayed on this diagram for completeness. They do not report in to the Risk Control functions.



Sarbanes-Oxley Act 2002 - Impact on UBS

| SARBANES-OXLEY ACT 2002 | |
|-------------------------|---|
| I | Public Company Accounting Oversight Board |
| II | Auditor Independence |
| III | Corporate Responsibility |
| IV | Enhanced Financial Disclosures |
| V | Analyst Conflicts of Interest |
| VI | Commission Resources and Authority |
| VII | Studies and Reports |
| VIII | Corporate and Criminal Fraud Accountability |
| IX | White Collar Crime Penalty Enhancements |
| X | Corporate Tax Returns |
| XI | Corporate Fraud and Accountability |

IMPACT ON UBS

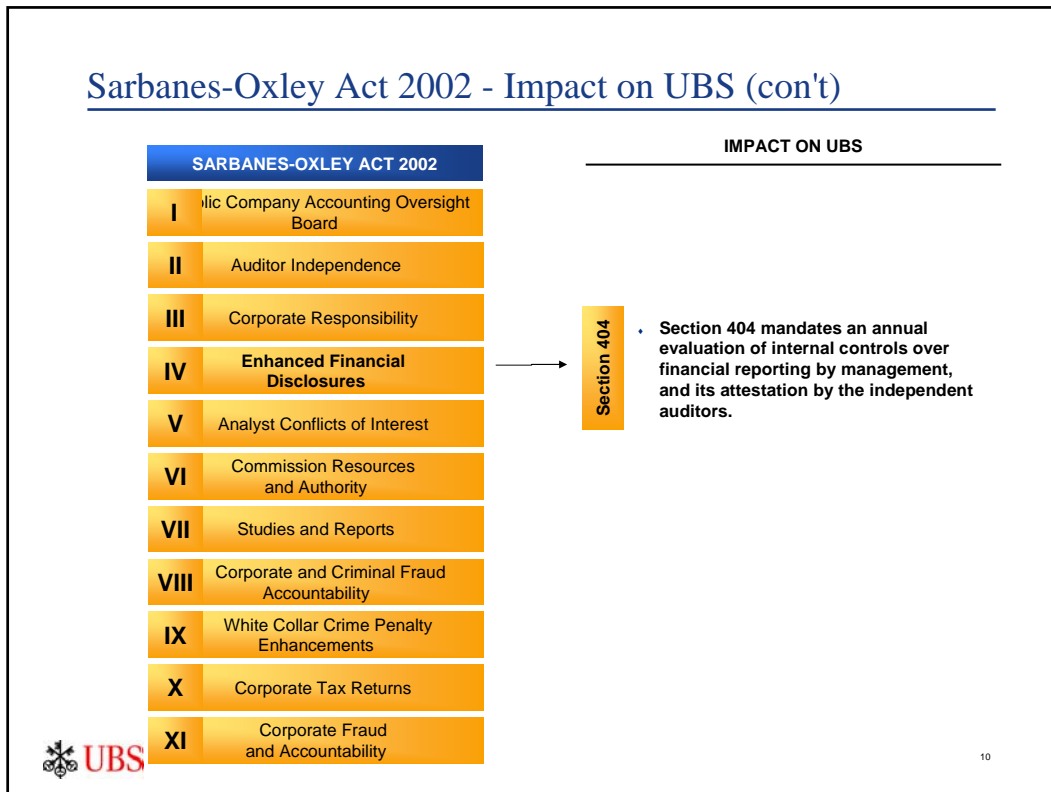
Applies to UBS annual report filed on Form 20-F and requires the following **CEO/CFO certifications and disclosures**:

- The UBS annual report does not contain any material misstatements or omissions and the **financial information fairly presents the financial conditions**, results of operations and cash flows of UBS as of, and for, the periods presented in the report
- CEO/CFO responsibility for establishment and maintenance of "**disclosure controls and procedures**" and "**internal control over financial reporting**"
- Conclusion on the **effectiveness** of UBS "disclosure control and procedures"
- Disclosure of any **material changes in the UBS' internal controls** over financial reporting
- CEO/CFO have **disclosed** to their audit committee and independent auditors any **significant control deficiencies**, material weaknesses, and acts of fraud.

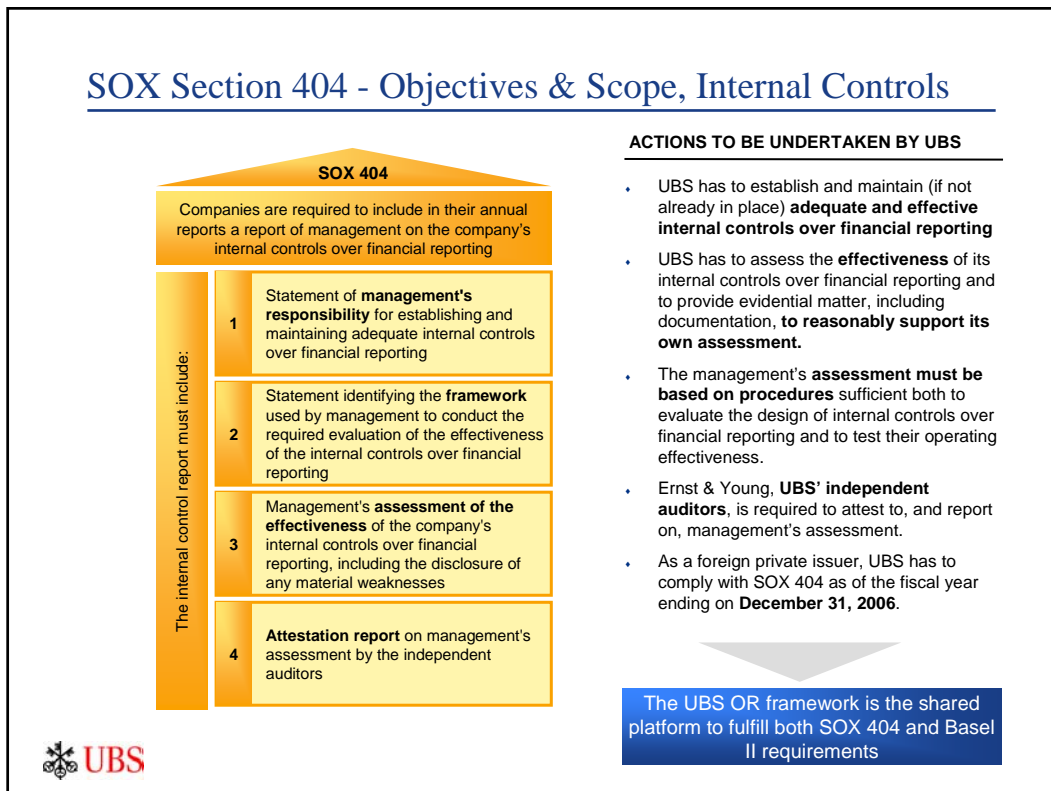
Section 302



Sarbanes-Oxley Act 2002 - Impact on UBS (con't)

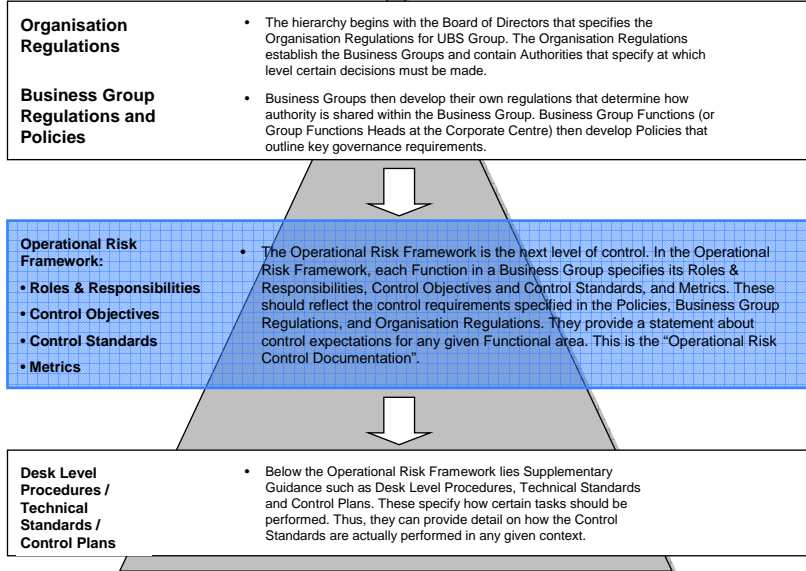


SOX Section 404 - Objectives & Scope, Internal Controls

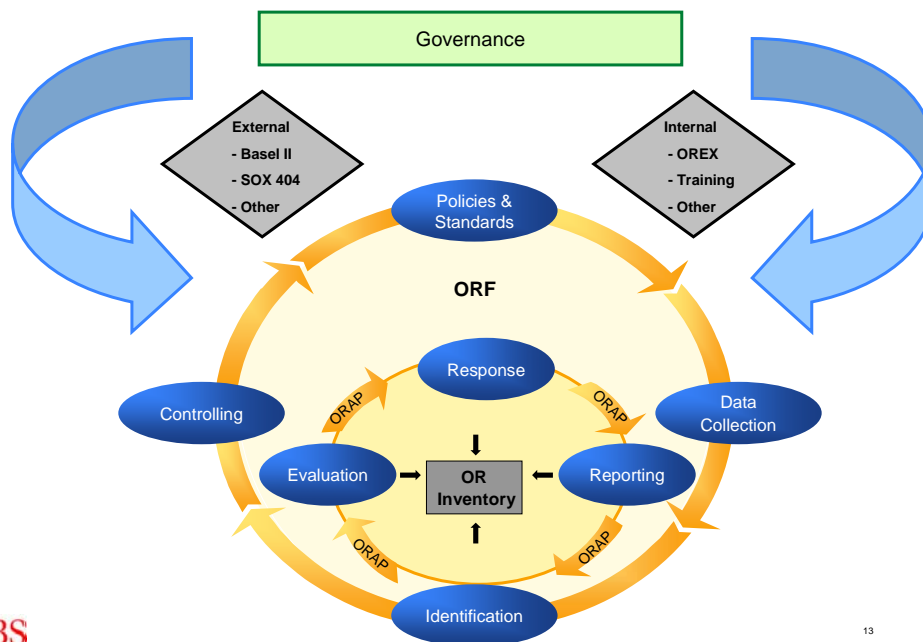


Hierarchy of Control within UBS

There is a hierarchy that specifies how authority is delegated within UBS Group and therefore how control is exercised.



The Operational Risk Framework - Overview



OR Control Documentation – Basic Elements

The Operational Risk Framework requires the existence of comprehensive underlying Control Documentation, designed to ensure that the Bank's processes operate correctly and effectively. The **Operational Risk Control Documentation** encompasses the following:



OR Control Documentation –Example

Roles and Responsibilities

A shortlist of distinct tasks for which a function is responsible

Example:

Information Technology - System Managers

System Manager has the responsibility to ensure the secure operation and administration of a given system. Regarding information security he has to authorize requests for privileged access to specific systems and he has to implement, maintain and document appropriate security measures for each information system. He has to document suitable IT contingency plans and he also has to ensure that critical or sensitive business information processing facilities are to be housed in secure areas and protected.

Control Objectives

- ◆ Derived by identifying "what could go wrong" within a Role & Responsibility
- ◆ Provide a brief description ensuring that the Operational Risks within any given Role & Responsibility are identified and addressed through the application of specific controls.

Example:

Capacity and Performance Management

To achieve the required service level (with respect to availability, response time, execution time, and stability) by assuring that, at all times, sufficient IT resources (CPU power and main memory, disk and tape capacity, network bandwidth, I/O bandwidth) are available to all systems that support business operations. This includes spare resources to cover unforeseen application growth as well as losses in case of hardware failures and disaster situations as defined in the service level agreement.

OR Control Documentation – Example (con't)

Explanatory Notes

- ◆ Where necessary, attached to Control Objectives.
- ◆ Provide context as to why a given Control Objective is deemed necessary for addressing a specific Operational Risk.
- ◆ Indicate how Controls relate to underlying transaction processes.

Example:

Capacity management is responsible for calculating the IT resources that are necessary in order to deliver the IT service levels agreed by service management with the IT Customer. It supports the software development teams in the design and engineering phase in order to use IT resources efficiently. Capacity management plans and manages all IT resources including CPU power, disk and tape capacity and network capacity.

Performance management provides capacity management with actual performance and utilisation figures in order to adjust their planning task and enable recalculation for IT services in operation. All business critical applications are monitored end to end and trend analysis is conducted in order to detect potential resource shortages at all times.

The definition and approval of standardised hardware models (hardware vendor selection, security approval of hardware and base software) is dealt with in section 2.2 Supply Management. Capacity management only defines the need for resources; supply management does the actual purchasing. Furthermore, storage management (assignment of application objects such as database files to available resources such as disk space) is not a capacity management issue and is dealt with in section 1.2 Data Backup and Recovery.

OR Control Documentation – Example (con't)

Control Standards

- ◆ Specific expectations that should be met in the performance of a function's activities with regard to Operational Risk Control.
- ◆ Represent the actions required in order to address the risks identified in the Control Objective.

Example:

Does the SLA specifically define the requirements for recoverability testing? Is recoverability testing performed in accordance with the SLA?

Metrics

- ◆ Supplement the self certification process by measuring the quality of controls that have been performed
- ◆ Indicate when Operational Risk levels may be deviating from the intended risk limit.

Example:

- Metrics Name: **SLA shortfalls regarding core IT applications**
- Metrics Description: Number of cases where the availability SLA target for the core IT applications cannot be met in relation to the number of TOP IT Services
- Calculation Methodology: Percentage = Average of (Numbers of SLA shortfalls per week / Number of controlled services/applications)
- Threshold: green: <=4%; amber: 4%-5%; red: > 5%
- Metrics Type: Quantitative
- Frequency: Quarterly

Self Certification

- ◆ The Self Certification Process is the first process that provides information for the Operational Risk Assessment and the SOX 404 Assessment
- ◆ Business Groups need to assign the Control Standards to named **Individuals**, who will be responsible for applying the Control Standard and completing the self-certification process. Afterward, First and Further Signatories must review the response.

| | |
|--|---------|
| Number of Control Standards: | 9'746 |
| Number of involved people (Certifiers, Signatories): | 8'536 |
| Number of Certification Item: | 171'377 |

Figures as of 1st quarter 2005



18

OR Control Documentation - Where?

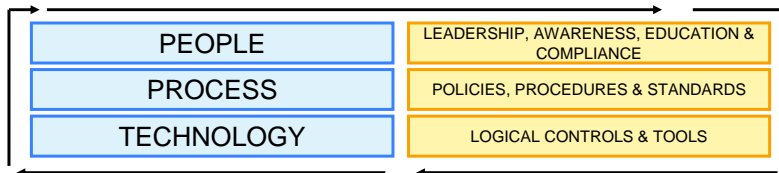
All OR Control Documentation (except Metrics) may be viewed by any employee in the Bank via the ORA Editor Tool.



19

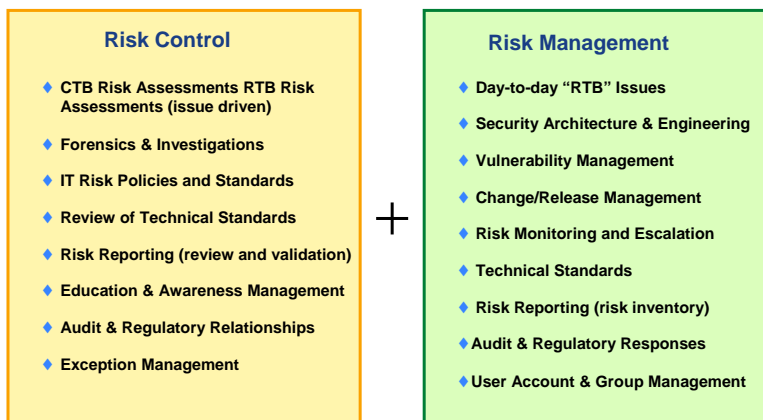
IT Control Framework - UBS Strategy for IT Risk

UBS uses a three-tiered strategy to control and manage IT Risk



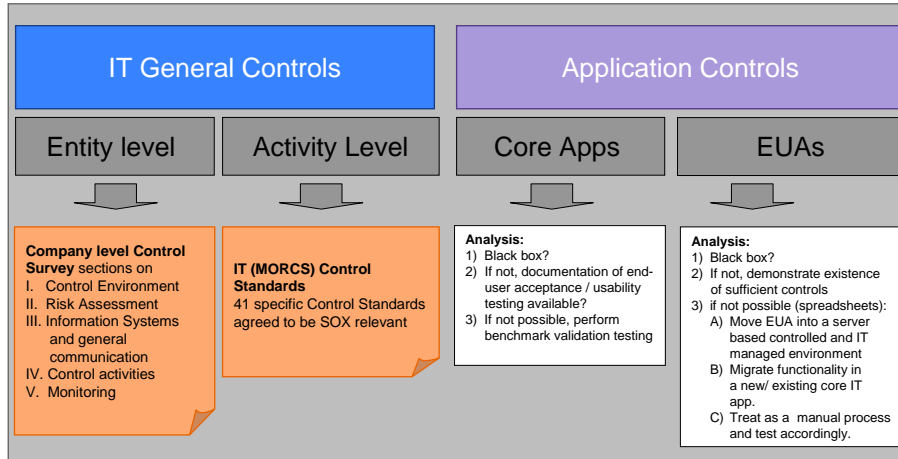
IT Control Framework – IT Risk Management vs. IT Risk Control

Clear delineation of roles and responsibilities, examples:



≡ Working together as effective partners, IT Risk Control and IT Risk Management work to reduce the Bank's overall IT Risk profile.

IT Control Framework in relation to SOX 404 Compliance



Conclusions