UBS Operational Risk Framework

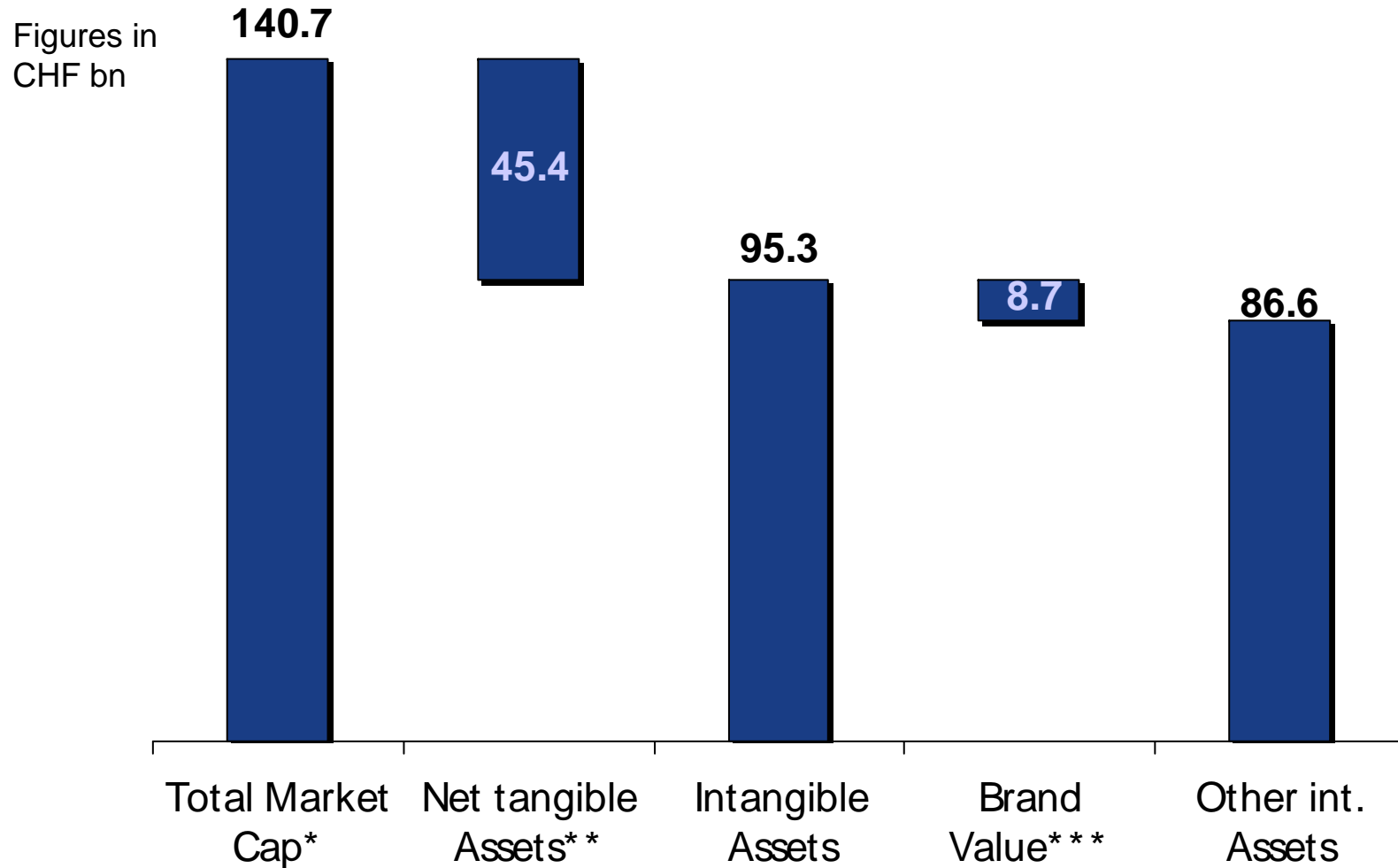# Judson Berkey, Group Operational Risk

BIS – 24 October 2006

Contents

- Design

- Implementation Status

- Examples (including Operational Risk Application)

- Integrating Qualitative and Quantitative

- Summary and Questions

Section 1

Design

The Business Imperative for the Approach

At current market-to-book ratios, UBS's market capitalization is mainly explained by intangible assets
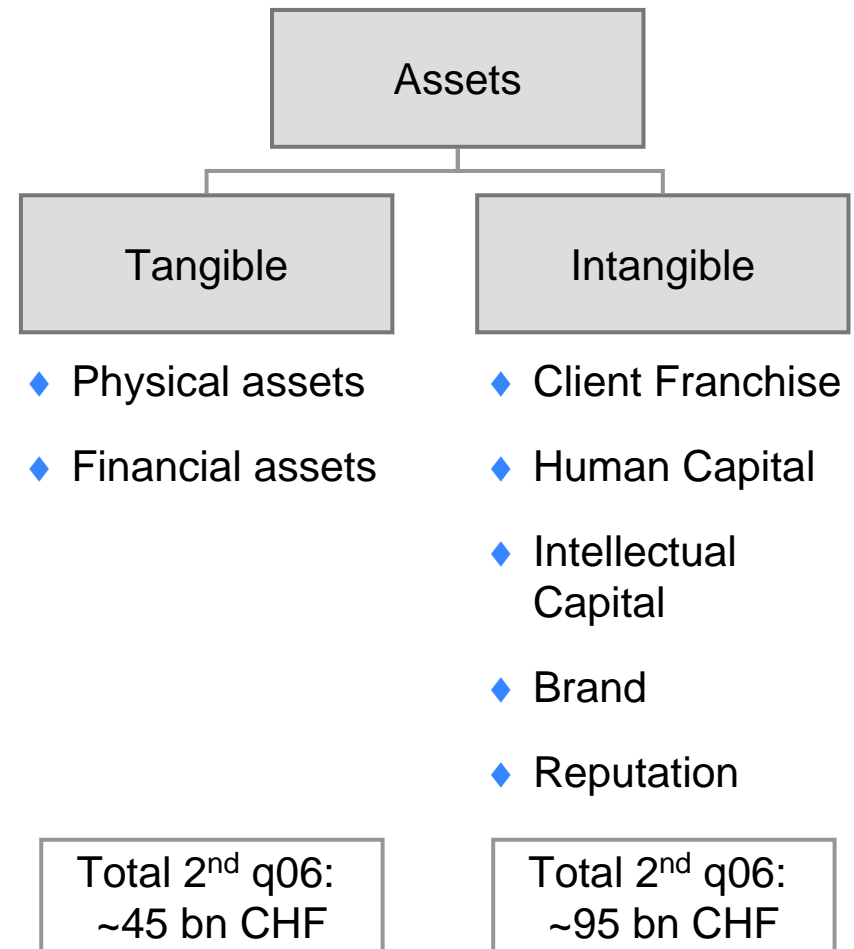
Figures in CHF bn

Total Market Cap*	Net tangible Assets**	Intangible Assets	Brand Value***	Other int. Assets
140.7	45.4	95.3	8.7	86.6

* Figures taken from UBS Financial Highlights; Second Quarter 2006 Report, 15 August 2006

** Equity attributable to UBS shareholders

*** According to Interbrand/Business Week Brand valuation, published in Business Week 7 August 2006

UBS

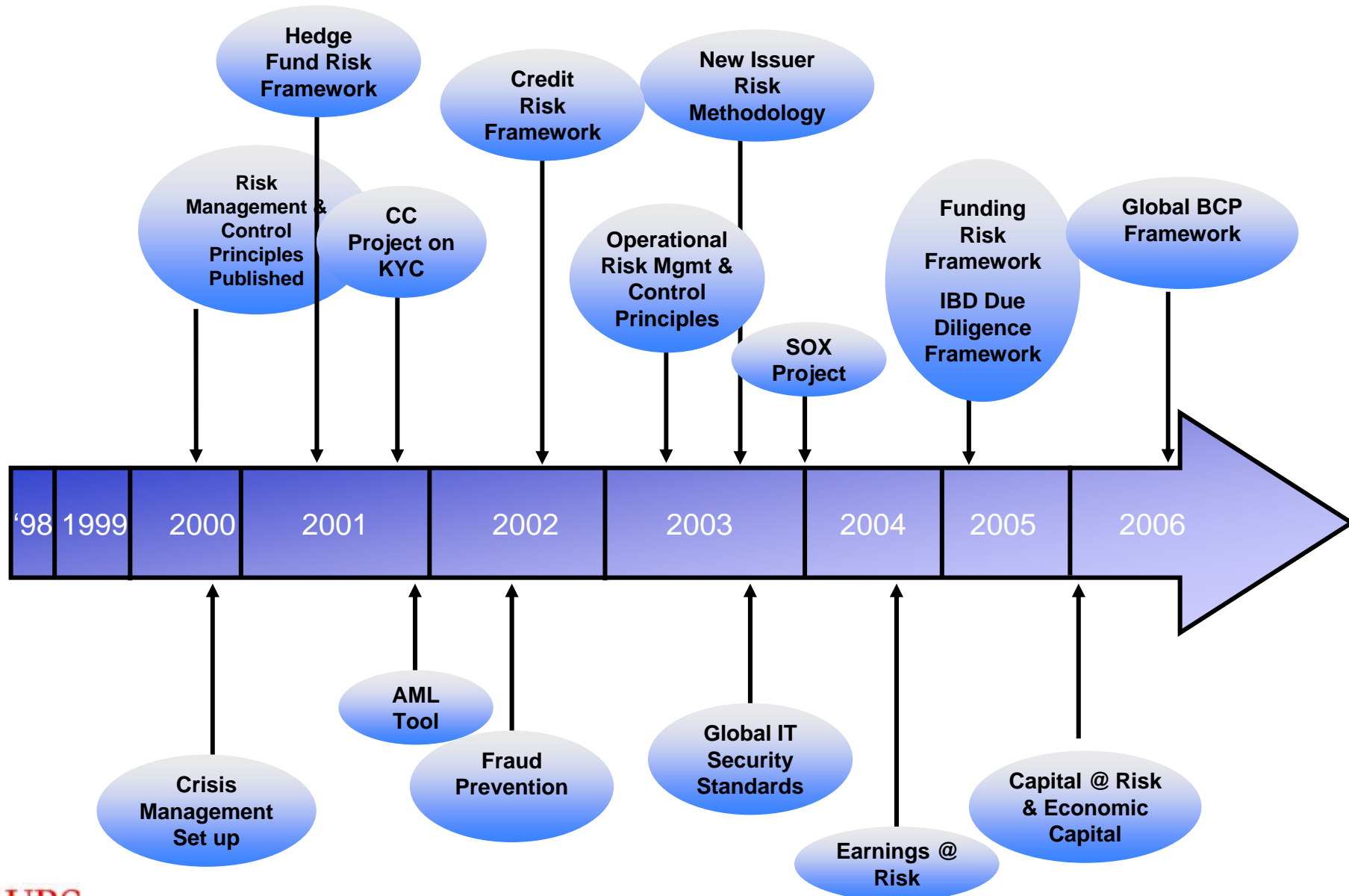# Assets and Assertions for Key Third Party Deliveries

♦ Consider financial trading assets

    – A **rights and obligations** assertion

    – An **existence** assertion

    – A **completeness** assertion

    – A **valuation** assertion

    – A **presentation** assertion

♦ In all cases, the controls are shaped by third party expectations

```
                    ┌──────────────┐
                    │    Assets    │
                    └──────────────┘
              ┌───────────┴───────────┐
      ┌──────────────┐        ┌──────────────┐
      │   Tangible   │        │  Intangible  │
      └──────────────┘        └──────────────┘
```

Tangible	Intangible
♦ Physical assets	♦ Client Franchise
♦ Financial assets	♦ Human Capital
	♦ Intellectual Capital
	♦ Brand
	♦ Reputation

Total 2nd q06: ~45 bn CHF	Total 2nd q06: ~95 bn CHF

♦ The goal is to expand this concept to the remaining assets.

UBS

Evolution of Risk Control Framework
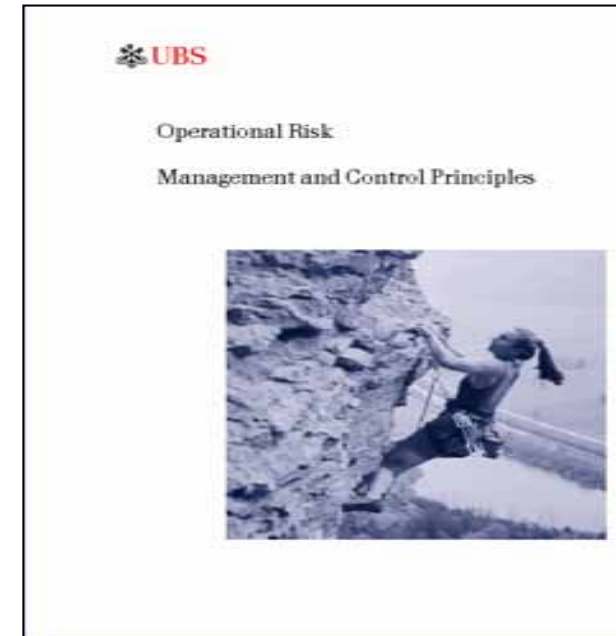
What is Operational Risk ?

◆ Operational Risk is defined by the UBS Management and Control Principles (approved by the Group Executive Board in July 2003) as:

"The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external causes (deliberate, accidental or natural). The losses may be direct financial losses, or indirect, in the form of revenue forgone as a result of business suspension. They may also result from damage to our reputation and our franchise, which have longer term financial consequences."

Operational Risk Management is the responsibility of every employee in the Bank throughout the performance of their day-to-day activities.

Operational Risk Management and Control Responsibilities

◆ We distinguish between risk managers and risk controllers

◆ Risk managers are held **primarily accountable** for managing risks, be they operational, market or credit risks

◆ Risk controllers exercise independent oversight to ensure risk is contained within the overall appetite of the organisation

◆ Risk control is not a police force, but does ensure that risk/reward decisions are taken at appropriate levels of management

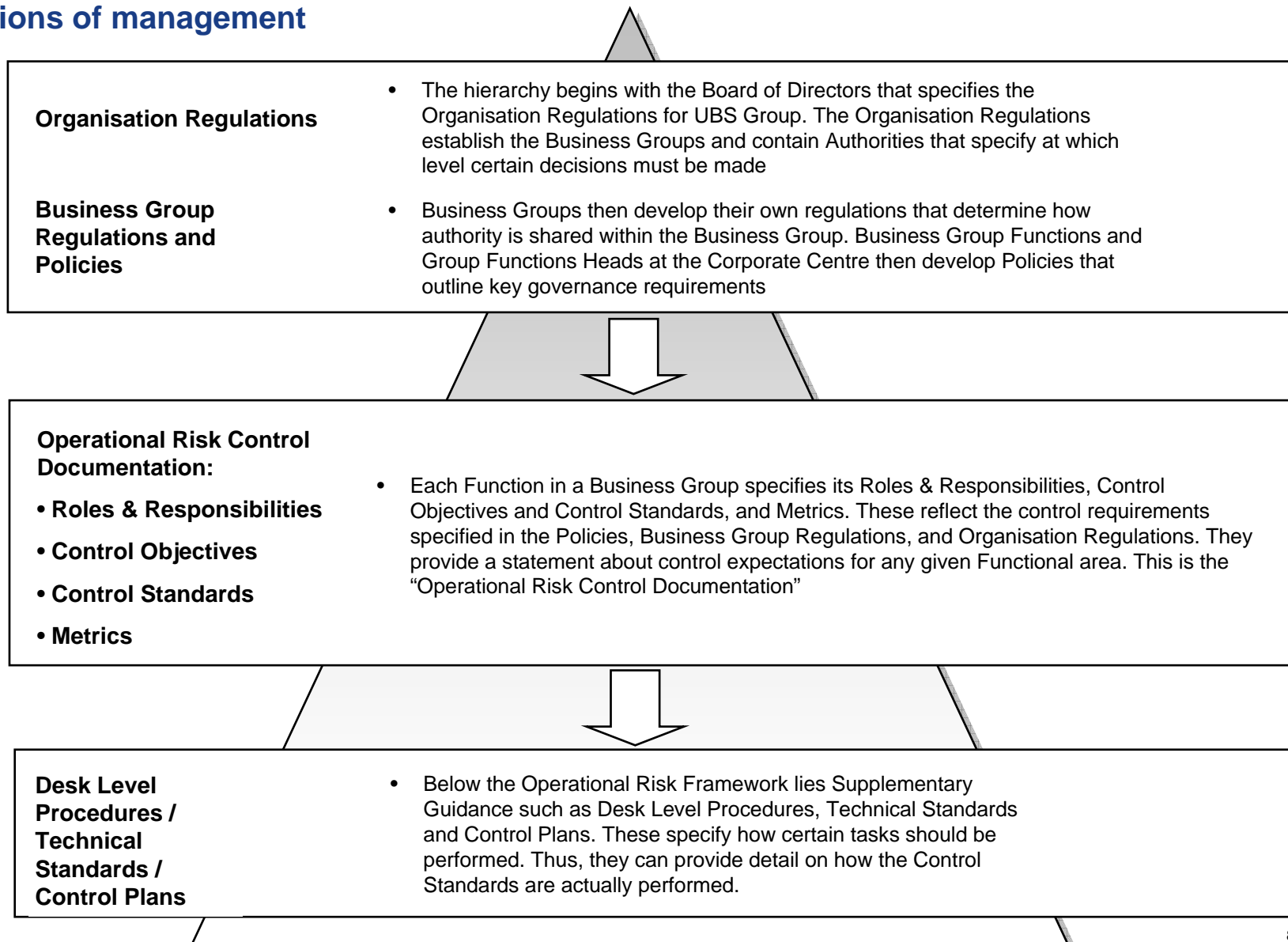◆ In order to fulfill this mandate, the key responsibilities of Operational Risk Control are the following:

> Independent verification of the identification, evaluation and response to operational risks as determined by management

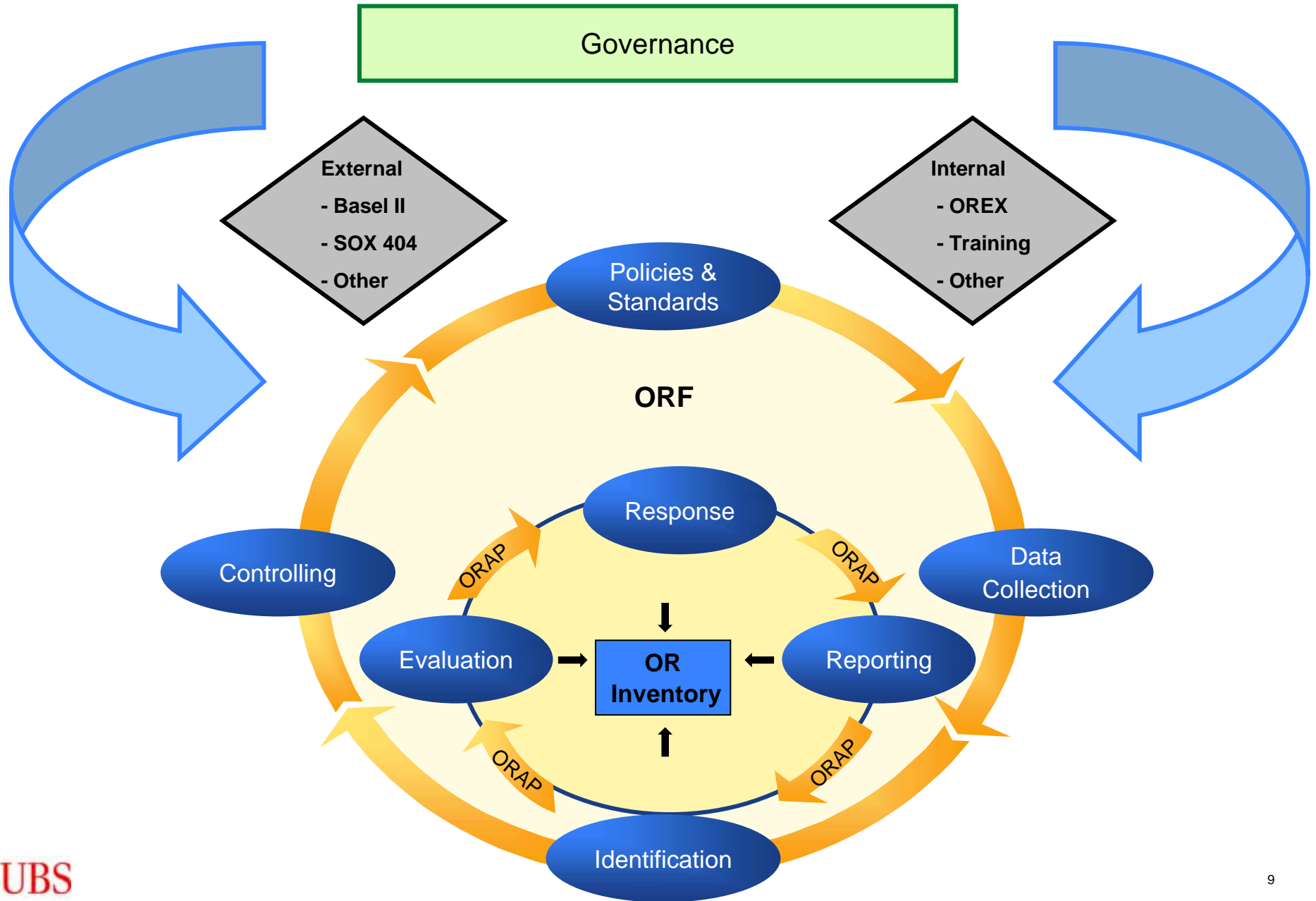> Reporting and monitoring of issues, including escalation, where appropriate

> Management of a cross-functional forum to discuss OR issues

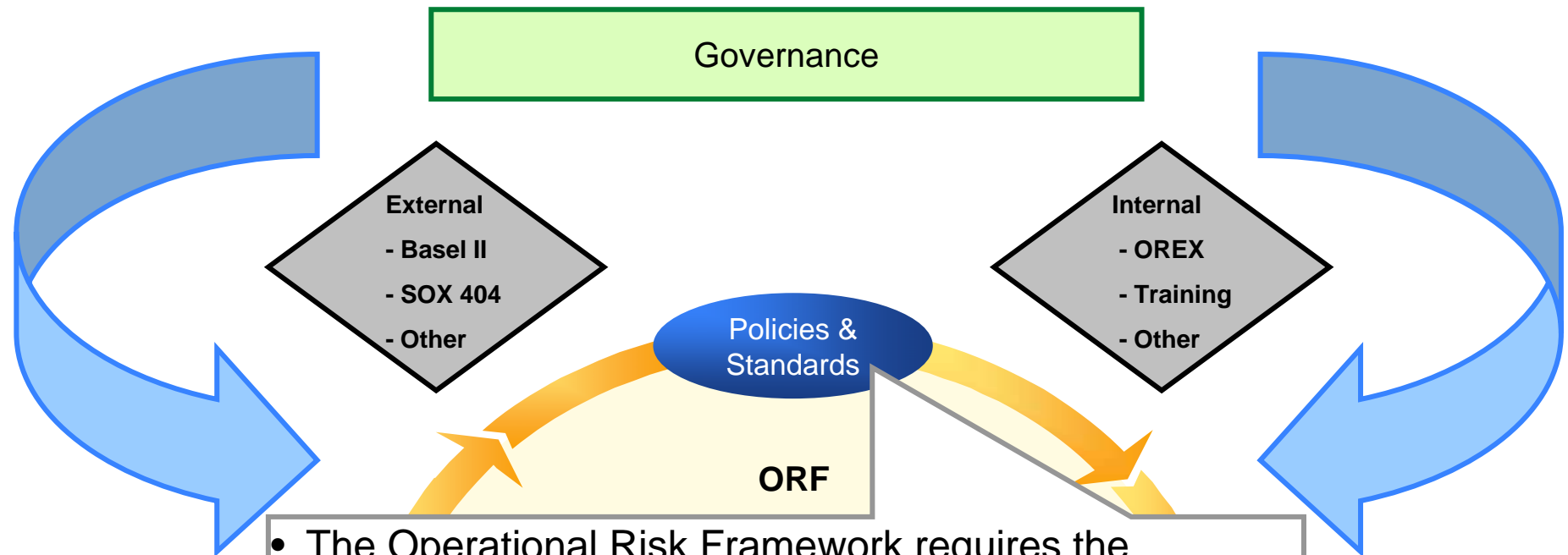# OR Control Documentation and Hierarchy of Control

A hierarchy specifies how authority is delegated within UBS Group and therefore how control is exercised. The OR Control Documentation is part of this and specifies the control expectations of management

Organisation Regulations

- The hierarchy begins with the Board of Directors that specifies the Organisation Regulations for UBS Group. The Organisation Regulations establish the Business Groups and contain Authorities that specify at which level certain decisions must be made

Business Group Regulations and Policies

- Business Groups then develop their own regulations that determine how authority is shared within the Business Group. Business Group Functions and Group Functions Heads at the Corporate Centre then develop Policies that outline key governance requirements

Operational Risk Control Documentation:

- **Roles & Responsibilities**
- **Control Objectives**
- **Control Standards**
- **Metrics**

- Each Function in a Business Group specifies its Roles & Responsibilities, Control Objectives and Control Standards, and Metrics. These reflect the control requirements specified in the Policies, Business Group Regulations, and Organisation Regulations. They provide a statement about control expectations for any given Functional area. This is the "Operational Risk Control Documentation"

Desk Level Procedures / Technical Standards / Control Plans

- Below the Operational Risk Framework lies Supplementary Guidance such as Desk Level Procedures, Technical Standards and Control Plans. These specify how certain tasks should be performed. Thus, they can provide detail on how the Control Standards are actually performed.

The UBS Operational Risk Framework

The UBS Operational Risk Framework

Governance

External
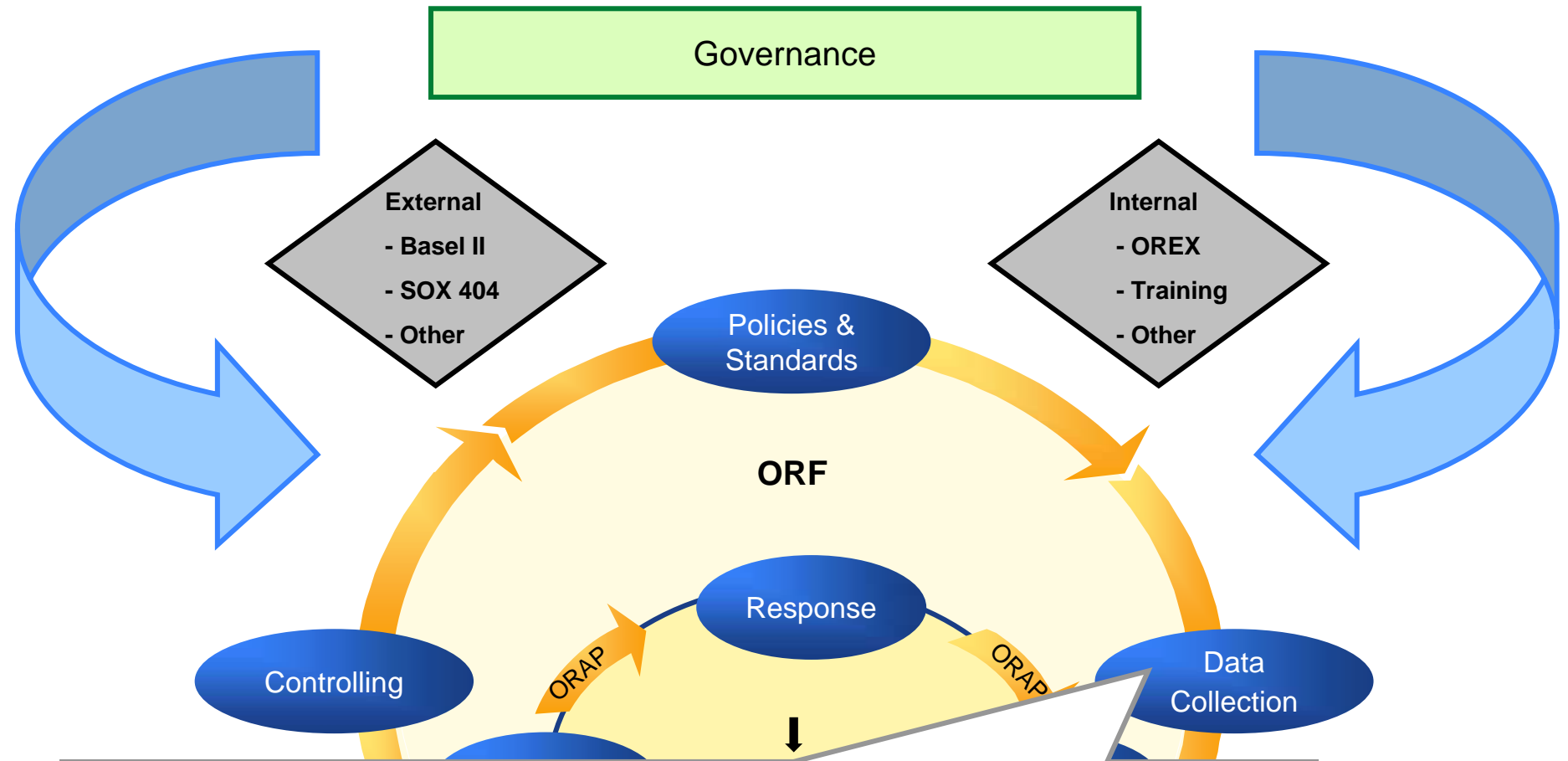- Basel II
- SOX 404
- Other

Internal
- OREX
- Training
- Other

Policies & Standards

ORF

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

- The results of the **Operational Risk Assessment Process** (ORAP) identify the current level of operational risk within the bank and help determine when changes to the Operational Risk Control Documentation are necessary.

The UBS Operational Risk Framework

Governance

External
- Basel II
- SOX 404
- Other

Internal
- OREX
- Training
- Other

Policies & Standards

ORF

Response

Controlling

ORAP

ORAP

Data Collection

In order for risk issues to be identified, data must be collected from a number of sources, known as **Risk Identifiers**. These include **Self-Certification**, **Events** (Financial, Non-Financial, External), **Metrics** (Risk, Performance, or Process Indicators), **Audit Reports** (Internal and External), and **Top Down and Specialist Assessments**.

UB

Operational Risk Assessment Process (ORAP) Overview

The Operational Risk Assessment Process (ORAP) consists of four stages during which issues are assessed:

- **Identification**
- **Evaluation**
- **Response**
- **Reporting**
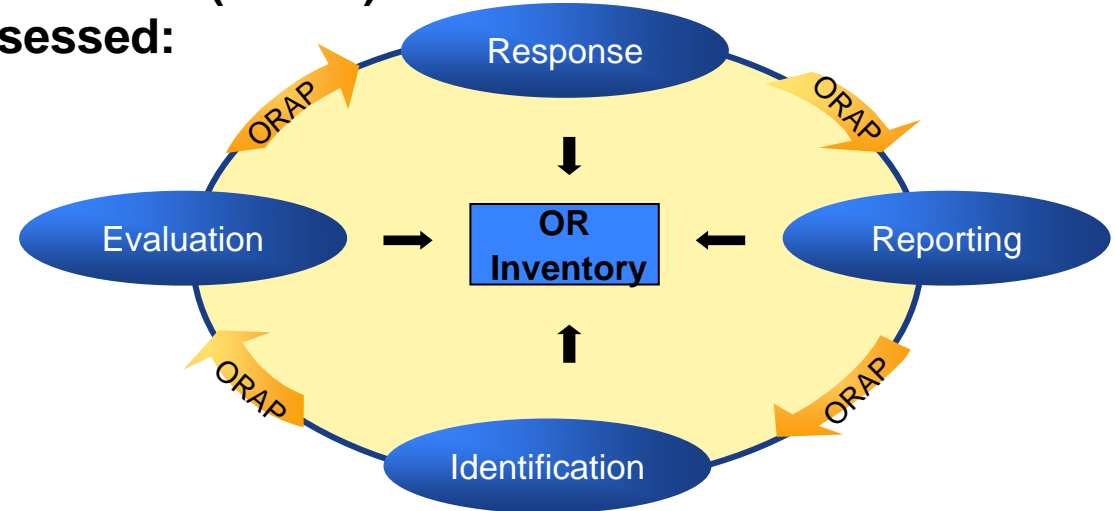
♦ In the first ORAP stage, potential Operational Risk issues are identified using data derived from the various risk identifiers.

♦ The second stage focuses on evaluation of the risk issues in terms of their potential impact on the Bank. Issues are rated red, amber or green.

♦ Based on the results of the evaluation stage, issues may be placed on the Risk Inventory. This requires determination of an appropriate response (e.g. action plan).

♦ In the final stage, risk issues are escalated and monitored periodically for progress.

Operational Risk Assessment Process

Risk Identifiers

Self-Certification (twice yearly)	Fin Events (monthly from G/L)	Non Financial/ Ext. Events (ad hoc)	Metrics (regular)	Audit Points (as issued)	Top-Down Assessment (quarterly)
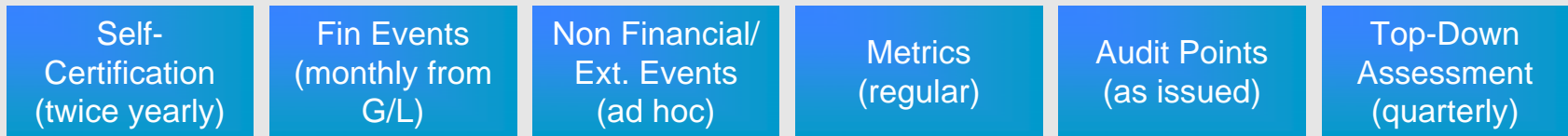
Identifiers are consolidated around Control Objective and assessed to identify OR issues. The issues are rated by operational risk managers on a Risk Inventory and action plans are agreed

Risk Inventory

1	...		X		SOX	...
2	...		-		-	...
4	...		X		=	...
5	...		X		-	...
6	...		-		SOX	...
7	...		-		=	...
8	...		X		SOX	...
...	...		-			...

Operational Risk Committee

Operational Risk Control administers the cross-functional OR Committee and performs an independent validation of the Risk Inventory as reported by the operational risk managers.

Operational Risk Reporting Process

Operational Risk Inventories and Reports proceed along defined escalation routes. This can be broadly illustrated as follows:

Business Groups

Group Executive Board

Quarterly Risk Reports

Group

Group Operational Risk Committee

Risk Inventory / Risk Reports

Management / Executive *or* Risk / Control Committee

Risk Reports

Note: Other Group-level specialized assessments (e.g. SOX 404) will have their own reporting and escalation structures.

Cross Functional Committees

Risk Inventory

Note: Each Business Group will have its own specific flow to integrate with its business governance

Individual Functions

Self-certification, event data, metrics etc.

Global Asset Management Global WM&BB Investment Bank Corporate Centre

UBS

Group Operational Risk Report

OVERVIEW

This Group Operational Risk Report identifies, based on the individual reports of the Business Groups, the most significant operational risk issues within UBS Group requiring Business Group or Group response. The issues have been grouped into subportfolios that in turn support four broad portfolios. The issues that were included in these subportfolios have been discussed with the Business Group Operational Risk Controllers, Group Legal and Compliance Risk Assessment, Group IT Risk Control, and Group Tax Risk Control.

- ◆ Report sent to the Group Executive Board based on the results of the ORAP.
  - General Overview to highlight themes and trends
  - Status of Business Group Risk Inventory Issues
  - Overview of Financial losses

- ◆ Portfolios of Risk Issues (each with their own subportfolios) and Group level action plans where appropriate for Group Inventory Issues
  - Business Process and IT Architecture
  - Corporate Governance
  - Legal, Regulatory, and Tax Obligations
  - Risk Representation and Financial Reporting

- ◆ Presents the board with information that allows them to understand the current operational risks and make decisions about where risk appetite has been exceeded.

Section 2

Implementation Status

UBS

Operational Risk Framework Implementation Status

♦ Principles – OR Man. & Control Principles ☑

♦ Structure – Bus. Group OR Controllers & Committees ☑

♦ Process – OR Assessment and Reporting Process ☑

♦ System – Operational Risk Application ☑

♦ Regulatory Compliance – Basel II and SOX 404 | 2006/ 2007 |

ORF Implementation – 2006

♦ 2,000+ Control Objectives

♦ 10,000+ Control Standards

♦ 6,500 Certifiers

♦ 3,000 Signatories

♦ > 175,000 Certification Items

♦ 10,000 Metrics being produced annually

♦ 70,000 Financial Events collected annually

UBS

Operational Risk Application

A modular, group-wide application supporting the ORF processes.

Reporting Tool
Reporting on Control Documentation,
Set-Up and Results of the Certification

Editor Tool
Storage and Maintenance of the
Control Documentation
(roles & responsibilities, control objectives & standards, etc.)

set-up process

Set-Up Tool
Preparation of the
Self-Certification
(certification items)

Certification Tool
Self-Assessment of the
Compliance to the Control
Standards for a specific "scope"
(entity, function, other dimension)

certification process

assessment process

Metrics Tool
Maintenance of the **Metrics Definitions** and
Collection/Reporting of the **Metrics Results**

Events Tool
Collection and Reporting of **OR Events / Losses**

Other Risk Identifiers
Audit Points, CLC, etc.

Governance

Basel SOX

OREX Train

Policy Stand

Respons e

Control

ORAP

Data

Evalu ation

OR Inventory

Repo rting

ORAP

ORAP

Identific ation

ORAP

Risk Inventory & Heatmap Tools

Identification, Assessment,
Monitoring and Reporting
of OR and SOX issues

Sarbanes Oxley Action Section 404

♦ Sarbanes Oxley Action Section 404 requires a process for assessing the design and operating effectiveness of internal controls over financial reporting.

♦ The U.S. SEC has provided rules implementing this act.

♦ Financial Reporting controls operate at both transaction and company levels.

♦ The Operational Risk Framework ensures control design effectiveness.

♦ The Operational Risk Assessment Process assesses operating effectiveness.

Internal Controls over Financial Reporting (ICOFR)

Controls at Process/Transaction Level

Operational Risk Framework

Front Office	IT	Finance	Operat-ions	Others

SOX 404 ⊠ ⊠ ⊠ ⊠ ⊠
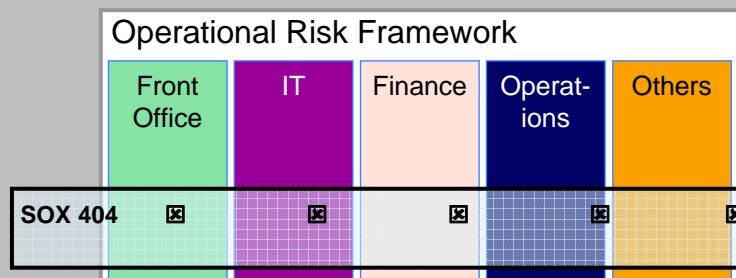
Controls at BG/Company (Entity) Level

• Governance Framework

• Policies and other standards

• Company level control survey

UBS Approach to SOX Design and Operating Effectiveness

OPERATING EFFECTIVENESS	DESIGN EFFECTIVENESS	

OPERATING EFFECTIVENESS

Function X
Function Y

Function A
Function B
Function ...

BG SOX 404 Reports

BG
BG
BG
BG

✓ SOX relevant

DESIGN EFFECTIVENESS

BG FUNCTIONAL REVIEWS

BG X-FUNCTIONAL REVIEWS (ORC/SRP)

GROUP REVIEWS

GROUP FCT REVIEW ITEMS	GROUP OR REVIEW ITEMS	GIA REVIEW ITEMS
123 IB	123 IB	123 IB
3423 WM-US	3423 WM-US	3423 WM-US
23123	23123	23123
123 IB	123 IB	123 IB
3423 WM-US	3423 WM-US	3423 WM-US
23123	23123	23123

Completeness Task Force

BG CFO and CEO SOX 404 Operating Effectiveness Assessment

YEAR-END BG DESIGN EFFECTIVENESS STATEMENT

BG CTF COMPLETENESS STATEMENT

Annual CTF report

SOX 404 Committee Assessment on **Operating Effectiveness (Group)**

SOX 404 Committee Assessment on **Design Effectiveness**

Basel II and the Operational Risk Framework

♦ The Basel Committee has developed specific rules for how banks must determine operational risk capital requirements. These rules contain three pillars.

Pillar 1: Minimum Capital Requirement to cover Operational Risk losses	**Pillar 2:** Supervisory Review of Capital Adequacy Assessment and Internal Processes	**Pillar 3:** Disclosure on Operational Risk Management and Control

♦ The Operational Risk Framework provides the processes to address each pillar.

– Internal financial event data and issues from the Group Operational Risk Report are quantified to provide both historical and forward-looking views of operational risk.

– The qualitative aspects of the ORF provide a basis for evaluating the capital requirement in light of the current level of and appetite for operational risk.

– Information collected during the assessment process is used for disclosure.

♦ This ensures that UBS is compliant with the rules as implemented by its primary supervisor, the Swiss Federal Banking Commission (EBK)

Eidgenössische Bankenkommission
Commission fédérale des banques
Commissione federale delle banche
Swiss Federal Banking Commission

UBS

Pillar 1 - Capital Charge Calculation

♦ UBS Group is composed of a number of different Legal Entities. The approach used to calculate the capital charge thus varies accordingly, as shown below.

Entity	Capital Charge Approach
UBS Consolidated Group	AMA
Parent Bank (UBS AG & Branches)	AMA
Foreign Banking Subsidiaries	Basic Indicator / Standardized Approach
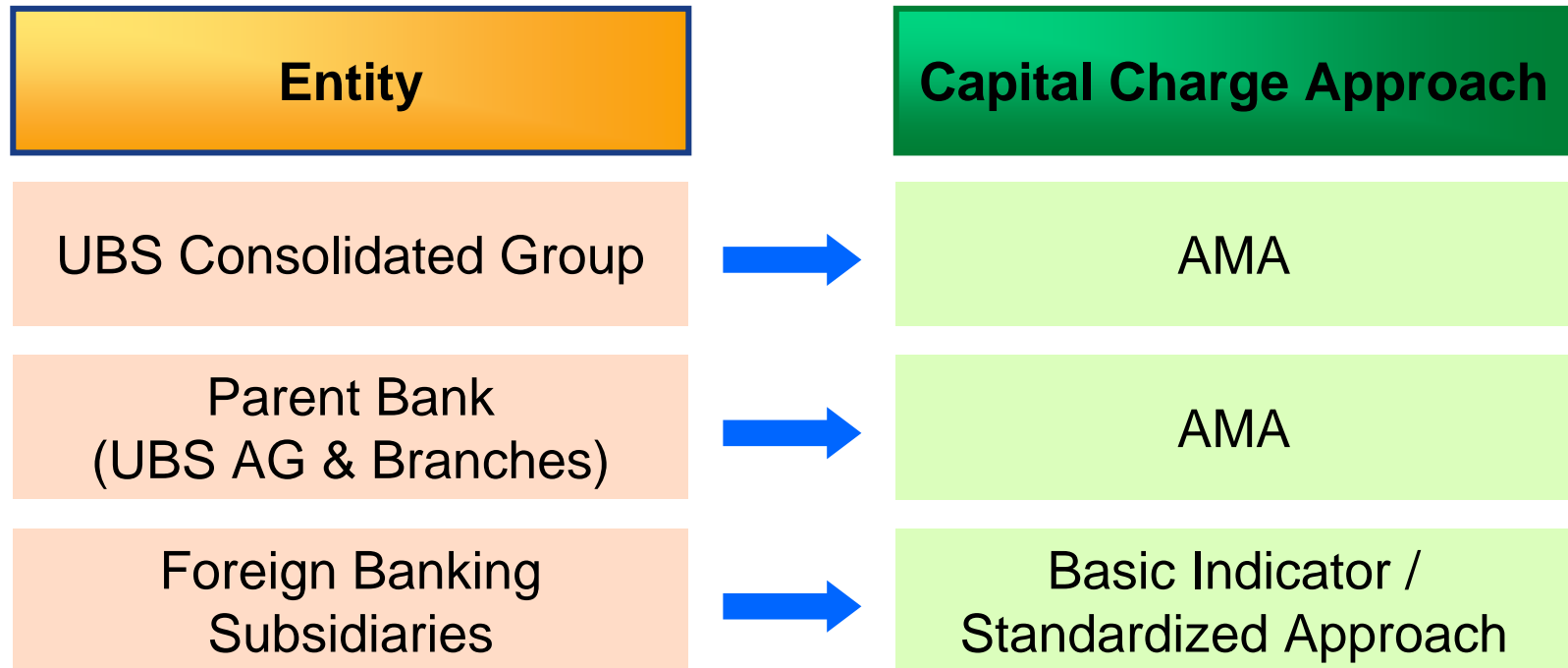
♦ The consolidated group-wide capital requirement and the Parent Bank requirements are calculated using the AMA. This is done at group level. Approval is required from the EBK.

♦ Local capital requirements are calculated using the Basic Indicator (or Standardized Approach). This is done by the local entity. Approval is required from the local regulator.

OREX: Operational Risk Excellence
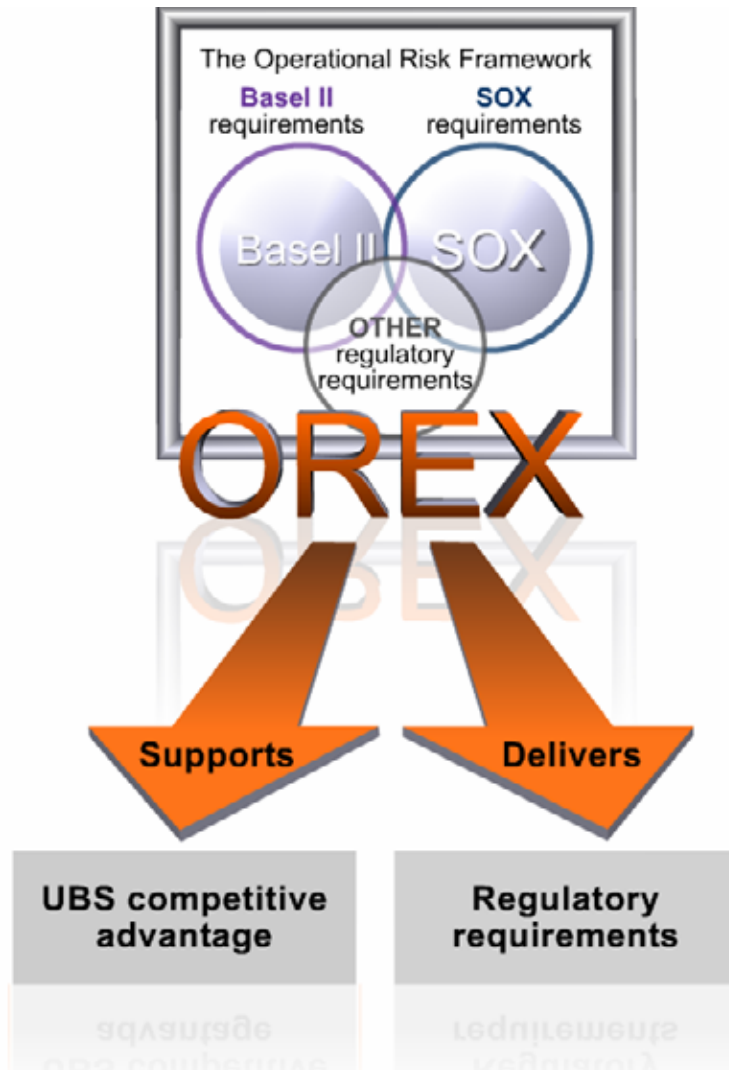
- ♦ 17 GEB sponsored initiatives to achieve excellence in operational risk management & control throughout UBS, reduce exposure to financial and reputational damage, contribute to 2010 growth agenda and establish and clarify responsibilities

- ♦ The Operational Risk Framework (ORF) and OREX enable UBS to meet SOX 404 and Basel II requirements

- ♦ While the ORF establishes a structure and a process for the management of Operational Risk, OREX is both more specific and larger since the initiatives go beyond the scope of the ORF

17 OREX Initiatives as Response to GEB Radar

STRATEGIC RESPONSE

- **Regulatory development**
- Target business process model
- Conflict of Interest (outside of OREX)
- **OR Communication and Education framework**

SHORT TERM RESPONSE

- Review Key Third Party Deliverables
- **Review of Legal Entity governance**
- **Top down alignment of Regulations, Policies and ORF Control Standards**
- **Realignment of IT Risk Management and IT Risk Control functions**
- Pricing and valuation of complex products
- Static data management
- Intercompany transactions
- (US Withholding) Tax

OTHER INITIATIVES

- Fraud global standards
- Group portfolio of projects and project management excellence
- **Standards for metrics (Key Risk Indicators)**
- Process for top down risk identification
- Factor key Operational Risks into business planning process
- HR OR Task Force

� UBS

Section 3

Examples (including Operational Risk Application)

ORF in the organisation

Organisation Regulations & Risk Authorities

Implemented by

Business Group Regulations

Implemented by

Policies

Implemented by

OR Framework
- Roles and Responsibilities
- Control Objectives
- Control Standards
- Metrics

Technical Standards

- Control plans (& procedures)
- IT Build standards
- Accounting policy / standards

- Mandatory Group
  Operations Standards
- Optional Matrix (local)

ORF in the organisation – Roles and Responsibilities

Organisation Regulations & Risk Authorities

Implemented by

Business Group Regulations

Implemented by

Policies

Implemented by

OR Framework
- **Roles and Responsibilities**
- Control Objectives
- Control Standards
- Metrics

Technical Standards

- Control plans (& procedures)
- IT Build standards
- Accounting policy / standards

- Mandatory Group Operations Standards
- Optional Matrix (local)

Role and Responsibility:

♦ Operations have the stewardship responsibility for the financial assets of the organization and its clients. Stewardship includes protecting the asset of the organization and its clients from accidental or purposeful loss or damage

ORF in the organisation – Control Objectives

Organisation
Regulations
& Risk Authorities

Implemented by

Business Group
Regulations

Implemented by

Policies

Implemented by

OR Framework
- Roles and Responsibilities
- **Control Objectives**
- Control Standards
- Metrics

Control Objective:

♦ To validate the existence of the asset, the completeness and accuracy of the records by reconciliation with third parties and internal parties

Technical Standards

- Control plans (& procedures)
- IT Build standards
- Accounting policy / standards

- Mandatory Group
  Operations Standards
- Optional Matrix (local)

ORF in the organisation – Control Standards
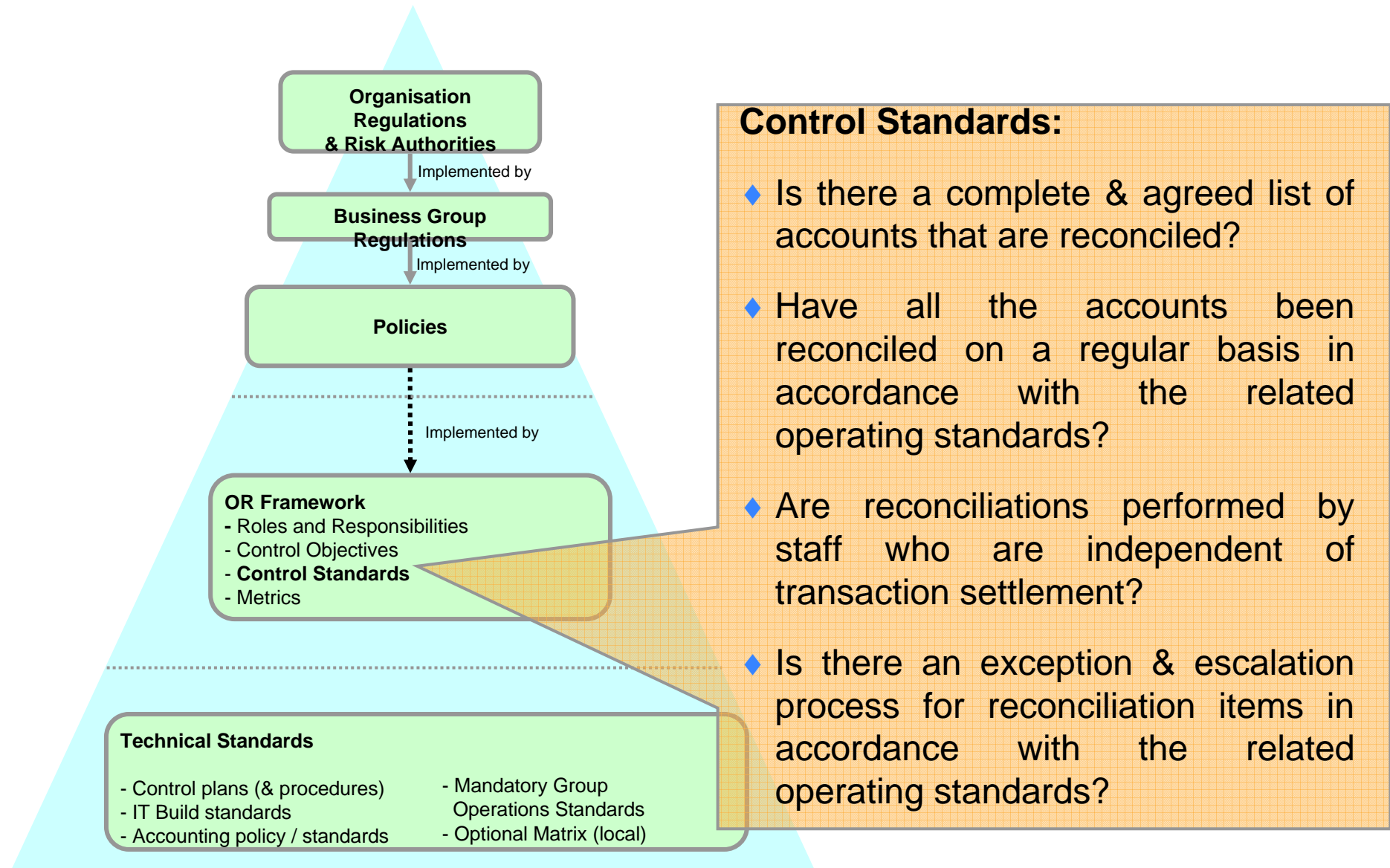
Organisation Regulations & Risk Authorities

Implemented by

Business Group Regulations

Implemented by

Policies

Implemented by

OR Framework
- Roles and Responsibilities
- Control Objectives
- **Control Standards**
- Metrics

Technical Standards

- Control plans (& procedures)
- IT Build standards
- Accounting policy / standards

- Mandatory Group Operations Standards
- Optional Matrix (local)

Control Standards:

♦ Is there a complete & agreed list of accounts that are reconciled?

♦ Have all the accounts been reconciled on a regular basis in accordance with the related operating standards?

♦ Are reconciliations performed by staff who are independent of transaction settlement?

♦ Is there an exception & escalation process for reconciliation items in accordance with the related operating standards?

Technical Standards – Account Reconciliations

Group Operations Standards

Group Operational Risk

Group Operational Risk
Bahnhofstrasse 102
Tel. +41-1-234 62 19

April 24, 2006

www.ubs.com

Standards for Account Reconciliations

Overview

This document describes control standards relating to reconciliation processes and must be read in conjunction with the following control standards.

- Is there a complete & agreed list of accounts that are reconciled?
- Have all the accounts been reconciled on a regular basis in accordance with the related operating standards?
- Are reconciliations performed by staff who are independent of transaction settlement?
- Is there an exception & escalation process for reconciliation items in accordance with the related operating standards?

The following defines the proper and comprehensive process lifecycle for reconciliation matching, exception handling and escalation:

- Match (reconcile) all relevant accounts on a transaction and position level. The differences identified at a transaction or individual account posting level must in value terms explain the differences in the two balances being reconciled including reconciling the balance brought forward equals the balance carried forward. The actual balances and the movement in the balances for the period must be reconciled.
- Investigate unmatched items/open breaks at a transaction/account posting level.
- Resolve unmatched items/open breaks.
- Monitor status of reconciliation.
- Reporting of open breaks.

A complete and proper reconciliation requires the following key processes to be followed:

1. **Activities within the reconciliation lifecycle**

1.1. Ensuring completeness and ownership of accounts
For all accounts transparency of ownership is essential. The person reconciling the account should be different from the person clearing the break.

1.2. Matching items
A reconciliation is primarily aimed at matching items to ensure that the records on one system, report or account and another (be it inside or outside the bank) are the same. Typically, this will involve matching pre-determined data fields, which will invariably include but not be limited to the value of the items. Reconciliation will result in unmatched items (also referred to as "breaks" or "open" items) that need to be investigated and resolved, the aim being to ensure that the two records are the same after clearance of the break.

2. **Reconciliation levels and matching criteria**
The activity of matching (reconciling) accounts must be performed on a transaction/account posting and position/balance level, that is, for all transactions collectively. Where applicable or mandated by local function management, it also can take place on a transaction level (for each transaction).

2.1. Position / balance level
The position/balance level reconciliation requires that total balances must match, for all accounts concerned[1]. This is important as it provides a proof that the items identified at a transaction/posting level as being unmatched are complete, i.e. that the sum of the individual items explains in total the difference between the balances.

2.2. Transaction/accounting entry/posting level
These are the individual items that need to be investigated and resolved.

A comprehensive exception and escalation process for handling reconciliation breaks requires the following:

3. **Activities within the reconciliation lifecycle**

The unmatched items need to be investigated and will result in a change to one or both of the systems or accounts being reconciled such that the difference is eliminated.

It is important that unmatched items are assigned to the correct area of responsibility and management authority for clearance, and that monitoring is performed to ensure clearance actually occurs on a timely basis.

As long as items remain unresolved and investigations are on-going the status is monitored. A break can be closed only when the transactions/account postings in question have been matched, and the overall position/balance difference resolved.

The status of the reconciliations must periodically be reported to management and other relevant parties. These reports will focus on the amount, number, and age of unmatched. Local management will determine the nature of this status reporting. Local management may also identify procedures for immediate escalation, typically when an unmatched item exceeds a certain value.

4. **Evidence of control performance**

In principle, evidence must be kept for the following aspects of the reconciliation process:

- Input controls: for example, the related sub-ledger, account statement and agent statement must be retained. Typically, this data is archived as part of a standard systems procedure.
- Control operation: for example, exception reporting must be documented; the report of the unmatched items must be retained.
- Control effectiveness: supervisory reviews must be documented at a minimum twice per month for a daily control[2]. For example, minutes of a supervisory review meeting should be kept.

Typically the specific evidence needed to meet this requirement is stated in the ORA tool.

---

[1] If applicable, appropriate guidelines for how to deal with global systems need to be set by the relevant functional management.

[2] According to IB experiences, E&Y requires 25-50 supervisory reviews p.a. for a daily control. If auditor's requirements can be met with a lower frequency of control, this lower frequency may be applied.

Operational Risk Application

A modular, group-wide application supporting the ORF processes.

Reporting Tool
Reporting on Control Documentation,
Set-Up and Results of the Certification

Editor Tool
Storage and Maintenance of the
Control Documentation
(roles & responsibilities, control objectives & standards, etc.)

set-up process

Set-Up Tool
Preparation of the
Self-Certification
(certification items)

Certification Tool
Self-Assessment of the
Compliance to the Control
Standards for a specific "scope"
(entity, function, other dimension)

certification process

Metrics Tool
Maintenance of the **Metrics Definitions** and
Collection/Reporting of the **Metrics Results**

Events Tool
Collection and Reporting of **OR Events / Losses**

Other Risk Identifiers
Audit Points, CLC, etc.

assessment process

Governance

Basel SOX

OREX Train

Policy Stand

Response

Control

Evaluation

ORAP

ORAP

OR Inventory

Data

Reporting

Identification

ORAP

ORAP

Risk Inventory & Heatmap Tools

Identification, Assessment,
Monitoring and Reporting
of OR and SOX issues

UBS

Editor: Clicking through to control standard 04.26.023.s001

Editor: 04.26.023.s001 : Details

Control Standard Details

Title	Is the client asset, invested asset and net new money reporting on BA level in I ...		
Reference Number	04.26.023.s001	Parent	023 (3.0.0. approved) Client asset reporting and Net New Money
Version	9.0.0	Status	approved

Details | SOX | CTF | Reporting Lines | Status | History

Description *

Is the client asset, invested asset and net new money reporting on BA level in line with the expectations of the Business Area Controllers?

Explanatory Notes

Description of Evidence Requirements (*)

Control Input: Market movement report, analysis from C/C Asset Reporting concerning Net New Money
Control Operation: A plausibility check has to be performed. The development of the relevant markets (FX, stock market, etc.) as well as the movements (Net New Money, Invested Assets as a whole) in absolute and relative terms have to be taken into account.

Technical Standards

Frequency of Execution

Level of Person Performing the Control

Editor: 04.26.023.s001 : SOX

Control Standard Details

Title	Is the client asset, invested asset and net new money reporting on BA level in I ...		
Reference Number	04.26.023.s001	Parent	023 (3.0.0. approved) Client asset reporting and Net New Money
Version	9.0.0	Status	approved

| Details | SOX | CTF | Reporting Lines | Status | History |

☑ **Mappings to GCoRs/Processes**
☐ Invested Assets: 163 - Analytical Review

Remove   Select

Check Out

Control Standard Details

Title	Is the client asset, invested asset and net new money reporting on BA level in I ...		
Reference Number	04.26.023.s001	Parent	023 (3.0.0. approved) Client asset reporting and Net New Money
Version	9.0.0	Status	approved

| Details | SOX | CTF | Reporting Lines | Status | History |

☑ **Reporting Lines**
☐ [IA7000] Invested assets - Note 36 Invested assets and Net new money
☐ [PS703Y] Net new money - Note 36 Invested Assets and Net new money

Remove   Select ...

Check Out

Workflow tool: 04.26.023.s001: Certification item

Metrics Tool: login

Metrics Tool: Metrics item detail

Loss Event Database : Events Overview

Loss Event Database: Event Detail

Core Event Details

Export Close

Event Details | Audit History

Transaction ID	Metrics GT Sell Down April
Risk Category	Transaction Processing Risk
Record Date	31.05.2006
Error Date	30.04.2006
Orig. Amount	1,560,891 [CHF]
USD Amount	1,280,552.46
CHF Amount	1,560,891
Region	Switzerland (CH)
Country	UBS AG - Corporate Center
Location	UBS AG - Corporate Center
Business Group	Corporate Center
Business Unit	Operating CC
Business Area	Group Functions
Business Sector	Group Treasury
Business Segment	Group Treasury Management
Business Function	Group Treasury (GT)
Account	51400.0
Accounting System	GCRS
Linkage Type	Non-Linked
Submission Date	28.06.2006 14:33:13
Comment	The operational risk concept, which has been implemented in light of the Basle II framework, views the p/l estimate proc inherent volume uncertainty as an operational risk, since inaccurate p/l estimates can lead to substantial FX losses. The therefore requesting an appropriate measurement and accountability of operational risk involved in the monthly FX sell c

Risk Inventory : Login

Risk Issues Included in the Quarterly Board Report

1.1 Capacity and Obsolescence

BG Issue	IB AMTRACS Vendor Risk		Risk tracker ref: A 929 Q2 Q005
Description	There are vendor support and technology obsolescence issues for the AMTRACS (settlement engine for US Dollar payments) application. Specifically, there are (a) One "very high" risk gap for contract management. UBS is the last remaining bank using AMTRACS and the vendor (IntraNet) will not support the product past Sept 2007. (b) One "high" risk gap for the lack of contingency for supplier failure (IntraNet owns the code) (c) Major changes in the core code over the years which affects supportability of the system. (d)One "high" risk gap for the non-bank-strategic VAX/VMS platform though this is presently still supported by the bank. HP can sunset support with 18 months notice though this is deemed unlikely for the following reasons: HP has signed an agreement with the Department Of Defense in US to continue to develop and support VMS for the next 15 years. AMTRACS currently runs on the Open VMS 6.2 operating system (8.2 is the latest). HP currently supports Open VMS back to version 5.2. There is no confirmation from HP as to when they will discontinue support for the 6.2 operating system however there are still many clients on this platform. Note: Risk Rated per MORCS risk rating guidelines		
Action Plan	Bank has undertaken mitigating controls (such as program fixes) to close or minimise the gaps. In the long term, this will be replaced by the GCU system in end 2006. (RFP in progress and the timeframes and dates TBD once vendor selection been completed). Until the system is replaced, a number of residual risks remains and will become critical if the GCU program is delayed. Interim Measures are as follows: a)Committment from hardware as well as software vendors to ensure continued support till system is replaced. b) Provide Backup/Training for vendor as well as bank staff to avoid reliance on key staff and improve quality of support c) Consider Outages/Recovery scenarios/improvements against application requirements; including the implementation of Tolerant Clustering Services (DTCS) allowing recovery to NY data centre to be reduced from 8 hrs to less than 2 hrs (Q1 2005).	Owner	Gordon J. Elliot
		Deadline	31 Dec 2006

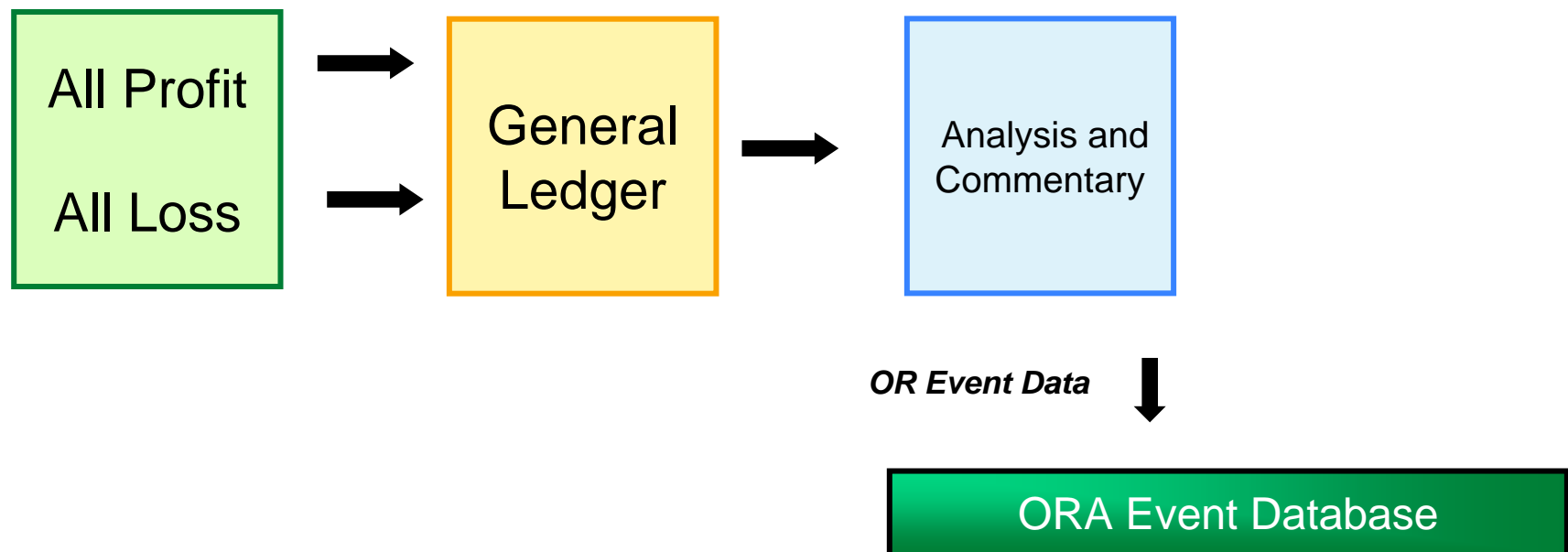Section 4

Integrating Qualitative and Quantitative

The Quantitative and Qualitative are Included in the AMA

♦ UBS's quantification of operational risk consists of **two components**:

   1. Historical event analysis

     – Based on historical information about UBS-specific events.

     – Uses an objective set of definitions and categorizations.

   2. Scenario analysis

     – Generated from UBS's Operational Risk Assessment Process.

     – Relies primarily on expert judgement of hypothetical events.

♦ Key principle - **risk described as a distribution of possible outcomes.**

   – Each of the two components output is a loss distribution

   – For each component, **capital = expected + unexpected loss** (UL).

♦ **UL is set at the 1-year, 95% level** for both AMA components

   – Results are more stable and consistent.

   – 99.9% equivalence is achieved by

     – Simulation of losses well in excess of actual losses in the historical component.

     – An upward bias in the scenario component.

     – Using a weighted average of the two components

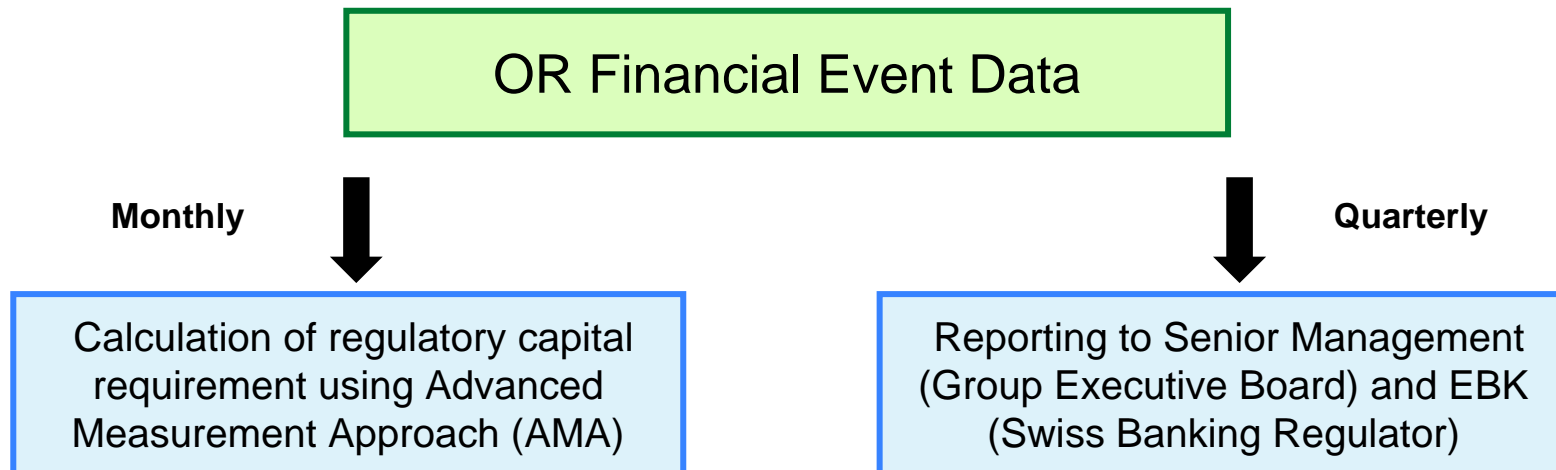   **(Note: weighting factor to be determined by EBK).**

OR Financial Events – Collection Process

♦ All OR profits and losses within the Bank are booked into the general ledger in the appropriate OR account as defined per accounting policy.

♦ Events are then analysed and commentary is added (where required), before being uploaded into the Group-wide ORA Event Database.

♦ Reconciliation to the general ledger is required before upload. Comments may be added before or after upload.

Purposes for Data Collection

♦ OR Financial Event is a risk identifier within the Operational Risk Assessment Process. Thus, it helps identify potential operational risk issues.

♦ In addition, the collection of data serves two further important functions.

OR Financial Event Data

Monthly → **Quarterly** →

Calculation of regulatory capital requirement using Advanced Measurement Approach (AMA)	Reporting to Senior Management (Group Executive Board) and EBK (Swiss Banking Regulator)

♦ The OR Financial Event data is incorporated into the UBS internal AMA model that determines the OR capital reserve required by Basel II.

♦ The OR Financial Event data is reported on a quarterly basis in the Group Risk Report to the Group Executive Board as well as to the EBK.

Risk Assessment is Primarily Qualitative

♦ Risk issues are identified from the review of the risk identifiers (certifications, metrics, events, audit reports, etc) by senior functional management.

♦ While the risk identifiers may often confirm their pre-existing views they do provide a level of objectivity to the process.

♦ Once risk issues are identified they are rated according to a defined scale that helps ensure a consistent rating of the issue.

♦ This distinguishes between the materiality of an issue based on a Red, Amber, Green scale.

♦ The risk assessment is guided by quantitative concepts.

Group Operational Risk Assessment Matrix

Risk Appetite

Risk Appetite	Group Risk Appetite Expected Loss Range (CHF m)	
	From	To
Green	0	5
Amber	5	25
Red	25	100
Red*	100	

Expected Loss (m CHF)

Financial Scale (CHF)

Frequency (Probability p.a.)	<5k	5k to 15k	15k to 50k	50k to 100k	100k to 500k	500k to 1m	1m to 5m	5m to 10m	10m to 25m	25m to 50m	50m to 150m	>150m
More than 12 times a year	0.03	0.12	0.39	0.90	3.60	9.00	36.00	90.00	210.00	450.00	1'200.00	2'400.00
4 to 12 times a year	0.02	0.08	0.26	0.60	2.40	6.00	24.00	60.00	140.00	300.00	800.00	1'600.00
2 to 4 times a year	0.01	0.03	0.10	0.23	0.90	2.25	9.00	22.50	52.50	112.50	300.00	600.00
1 to 2 times a year	0.00	0.02	0.05	0.11	0.45	1.13	4.50	11.25	26.25	56.25	150.00	300.00
Once between 1 and 2 years	0.00	0.01	0.02	0.06	0.23	0.56	2.25	5.63	13.13	28.13	75.00	150.00
Once between 2 and 5 years	0.00	0.00	0.01	0.03	0.11	0.26	1.05	2.63	6.13	13.13	35.00	70.00
Once between 5 and 10 years	0.00	0.00	0.00	0.01	0.05	0.11	0.45	1.13	2.63	5.63	15.00	30.00
Less than every 10 years	0.00	0.00	0.00	0.01	0.02	0.06	0.23	0.56	1.31	2.81	7.50	15.00

Non-Significant	Minor	Moderate	Signifi-cant	Major
No significant reputational impact	Minor reputational impact	Possible coverage in the press or market rumour that cannot be used easily by competitors to impact on client relationships	Unpleasant coverage in the press with moderate damage	Reputation badly damaged
No significant regulatory impact	Minor impact on regulators	Repeated inspections or private warnings	Regulators made aware of serious incidents. Potential for public warnings / significant fines.	Intensive inspection by regulators triggered by serious and repeated market malfunctions with high visibility.

UBS

47

Use of Scenarios in the AMA – Q2 2006 summary

1.1 Capacity and Obsolescence

BG Issue	IB AMTRACS Vendor Risk		Risk tracker ref: A 929 Q2 Q005
Description	There are vendor support and technology obsolescence issues for the AMTRACS (settlement engine for US Dollar payments) application. Specifically, there are (a) One "very high" risk gap for contract management. UBS is the last remaining bank using AMTRACS and the vendor (IntraNet) will not support the product past Sept 2007. (b) One "high" risk gap for the lack of contingency for supplier failure (IntraNet owns the code) (c) Major changes in the core code over the years which affects supportability of the system. (d)One "high" risk gap for the non-bank-strategic VAX/VMS platform though this is presently still supported by the bank. HP can sunset support with 18 months notice though this is deemed unlikely for the following reasons: HP has signed an agreement with the Department Of Defense in US to continue to develop and support VMS for the next 15 years. AMTRACS currently runs on the Open VMS 6.2 operating system (8.2 is the latest). HP currently supports Open VMS back to version 5.2. There is no confirmation from HP as to when they will discontinue support for the 6.2 operating system however there are still many clients on this platform. Note: Risk Rated per MORCS risk rating guidelines		
Action Plan	Bank has undertaken mitigating controls (such as program fixes) to close or minimise the gaps. In the long term, this will be replaced by the GCU system in end 2006. (RFP in progress and the timeframes and dates TBD once vendor selection been completed). Until the system is replaced, a number of residual risks remains and will become critical if the GCU program is delayed. Interim Measures are as follows: a)Committment from hardware as well as software vendors to ensure continued support till system is replaced. b) Provide Backup/Training for vendor as well as bank staff to avoid reliance on key staff and improve quality of support c) Consider Outages/Recovery scenarios/improvements against application requirements; including the implementation of Tolerant Clustering Services (DTCS) allowing recovery to NY data centre to be reduced from 8 hrs to less than 2 hrs (Q1 2005).	Owner	Gordon J. Elliot
		Deadline	31 Dec 2006

Financial Scale: Once between 5 and 10 years; 50 m to 150 m CHF

Risk Appetite and Tolerance Occurs at Multiple Points

◆ Risk appetite is expressed through the initial development of the control documentation. The specification of Control Objectives and Control Standards and the tolerance bands around metrics express the risk appetite of functional management.

◆ Risk appetite is also expressed during the assessment process by setting bands for the rating of the risk issues.

◆ Finally, risk appetite is determined when action plans are developed for risk issues. The due date of the action plan is a qualitative expression of the appetite or tolerance for the current risk exposure.

Section 5

Summary and Questions

Lessons Learned

- ◆ Senior management buy-in is critical
  - – Consistency and Quality vs. Buy-in
    - – Ownership of control documentation ensures its sustainability
    - – However consistency may need to be addressed over time

- ◆ Structure and culture must be aligned
  - – Functional versus process views
  - – Open versus blame culture

- ◆ Business not regulatory focus
  - – Know your organization and how this can fit in
  - – Integrate and consolidate other regulatory requirements

- ◆ Management focus
  - – This is not an audit framework
  - – It should be part of the management supervisory process

- ◆ Education and Training
  - – Operational Risk should be integrated into new joiner programs
  - – Control documentation can be a training tool itself

Ongoing Communication and Education

Key Points

- UBS Approach to Operational Risk
  - Business focused
  - An integrated framework used by management and control
  - Combines the qualitative and the quantitative
  - Risk appetite is ex-ante and ex-post

- Scalability
  - The framework can be applied by any institution
  - Must respect the organisation structure and culture

- This is about cultural changes as much as anything else

- Questions?