

INTEGRATING COMPLIANCE RISK ASSESSMENTS INTO ENTERPRISE RISK MANAGEMENT

Catherine Jourdan, Euler Hermes - Paris

Heike Ottemann-Toyza, Allianz Asset Management - Munich

QUESTION 1

Who is responsible for the compliance risk assessment?



1. The chief compliance officer?
2. Several different compliance functions? (*Fraud & Corruption, Product Safety/Suitability, Data Privacy, other*)
3. Risk management?
4. Internal audit?
5. Other?

QUESTION 2

What is the scope of compliance in your organization?

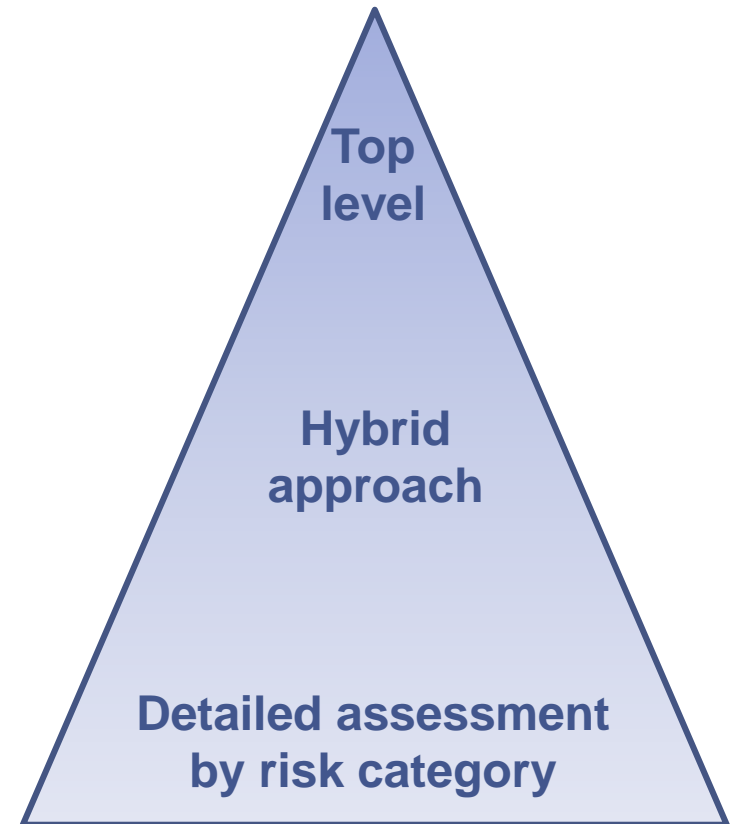
To the extent these risk categories are relevant to your organization, are they managed by compliance or another department, in particular those in blue?

1. Anti-fraud
2. Anti-corruption
3. Anti-money laundering
4. Economic sanctions
5. Conflicts of interest
6. Anti-harassment/discrimination
7. Environmental health & safety
8. Product safety/suitability
9. Antitrust
10. License/IP protection
11. Data privacy
12. Record retention
13. Cybercrime
14. Insider trading/capital markets rules
15. FATCA / Tax
16. Regulatory relations
17. Other?

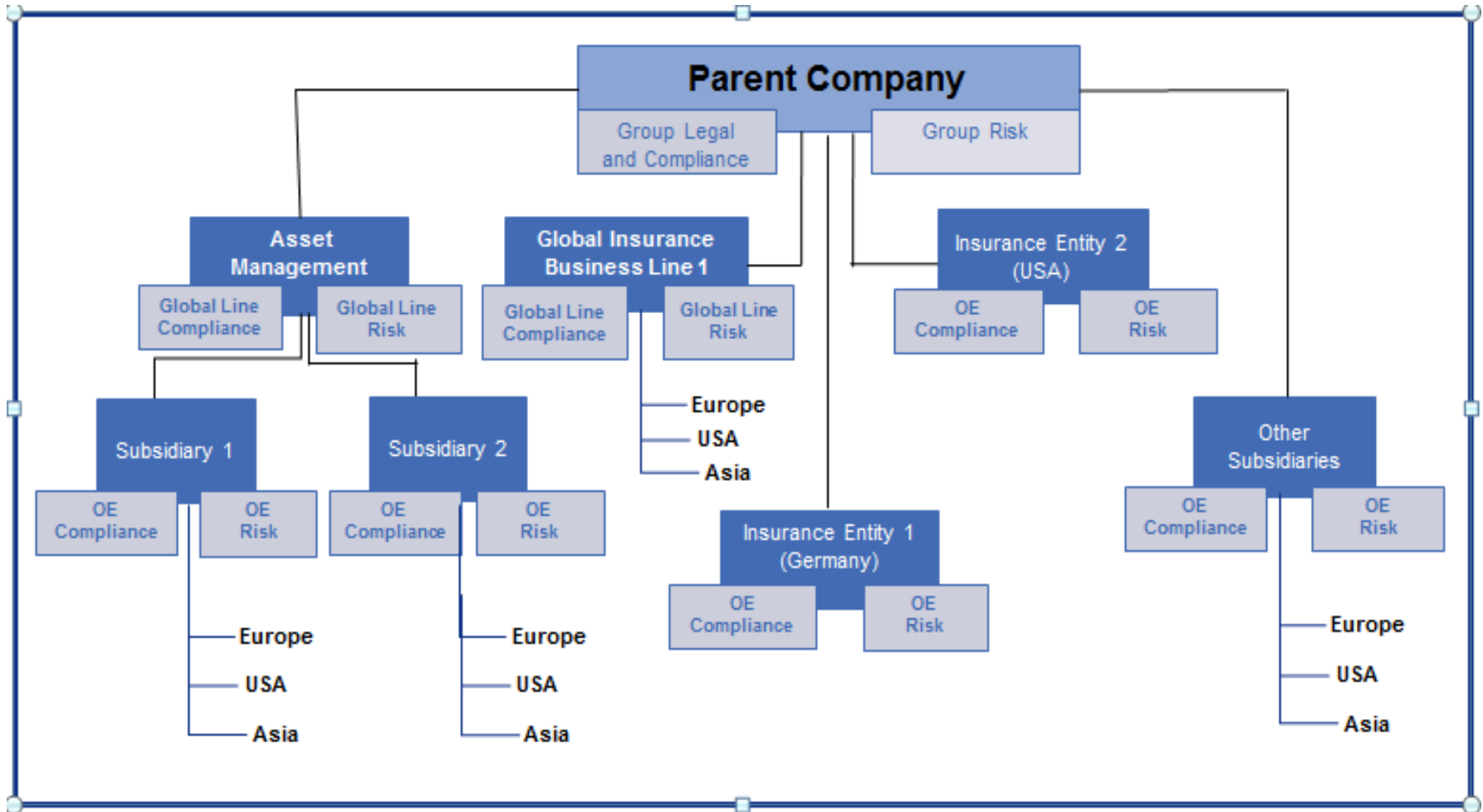
QUESTION 3

How granular is your compliance risk assessment?

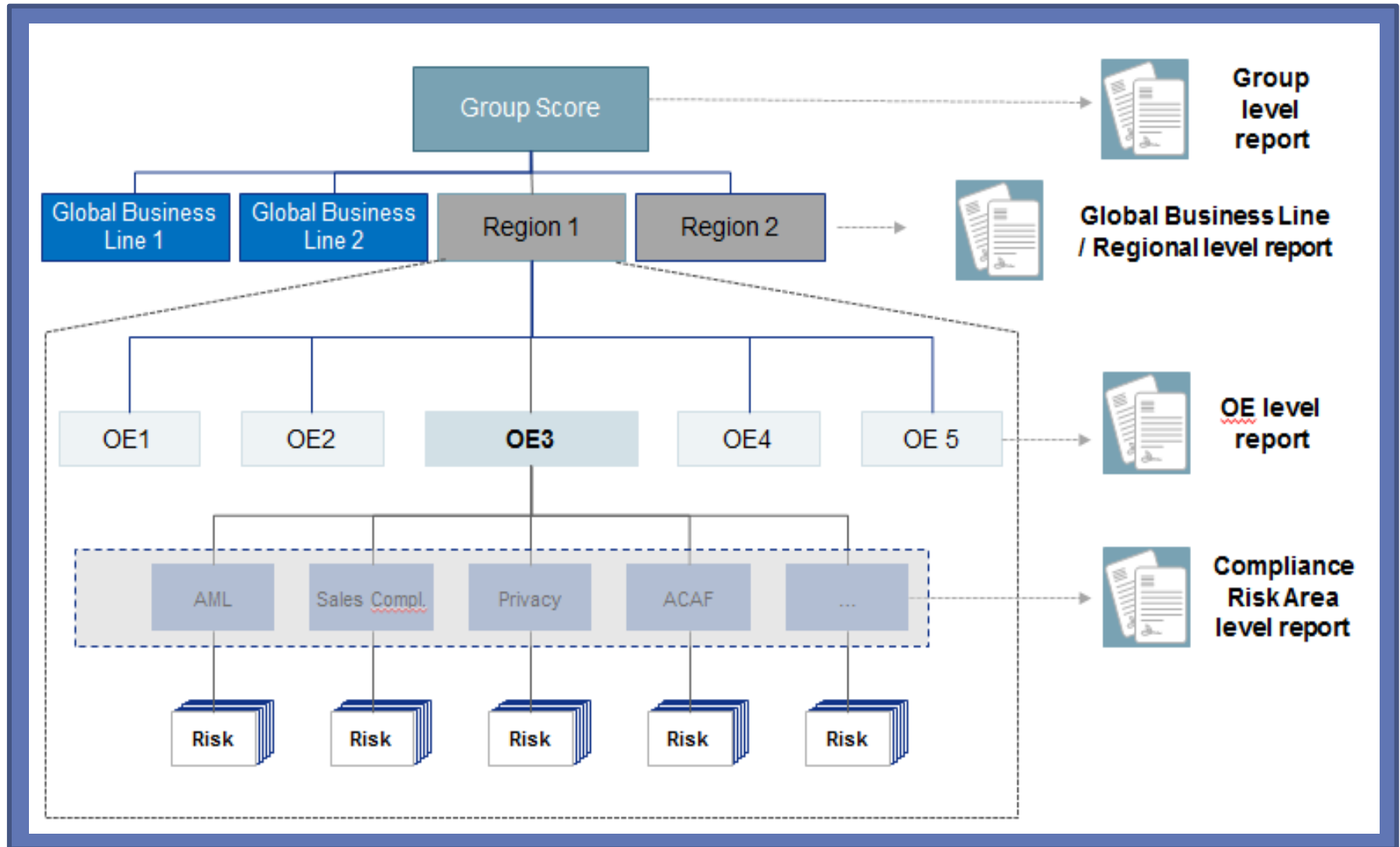
1. High-level picture for the board and other stakeholders
2. Varies by topic
3. Detailed matrices by compliance topic (SOX-like)



COMPLEX GROUP STRUCTURES MAKE COMPLIANCE RISK ASSESSMENT AND INTEGRATED ERM A CHALLENGE



COMPLIANCE RISK ASSESSMENT (CORA) PROCESS



OUR CHALLENGE

Integrating compliance risk assessments
into enterprise risk management

Within a complex and diverse
financial conglomerate

Requires:

A common understanding
of compliance risks and a
sufficiently **uniform handling** group-wide

WHAT VALUE SHOULD COMPLIANCE RISK MANAGEMENT DELIVER?

Compliance =
Managing Compliance Risks

Purpose of compliance risk management =

To build stakeholders trust and a sustainable competitive advantage
by **fully integrating compliance risk management** into
the **daily business activities** and the **strategic planning process**

THE BIG PICTURE → ACHIEVING AN INTEGRATED RISK MANAGEMENT PROGRAM



COSO Enterprise Risk Management – Integrated Framework, 2003

- How do we identify and assess Compliance risk, recognizing the other parts of the bigger picture?



TWO KINDS OF COMPLIANCE RISK ASSESSMENTS

Compliance
Function

Annual Risk Assessment:

Comprehensive assessment
of all potentially relevant risks and related documentation

Strategic
Planning



Business
Functions

Daily Risk Assessments

Supporting each business decision;
typically required of the front-line business managers

Daily
Business
Activities

INTEGRATION: A CONTINUOUS JOURNEY

Integrating compliance risk assessments into the **daily business activities** and the **strategic planning process**

Requires:

Appropriate governance structures enabling the compliance and other support functions to continuously support the relevant risk assessments

COMPLIANCE GOVERNANCE CHALLENGES & OPPORTUNITIES AS SEEN FROM ONE ORGANIZATION

Euler Hermes

- Full integration into operational processes
- Involvement in strategy discussions, as appropriate
- Combined approach with operational risk and other support functions
- Visibility of risks by topic and geographic area
- Continuous awareness and training

COMPLIANCE GOVERNANCE CHALLENGES & OPPORTUNITIES AS SEEN FROM ANOTHER ORGANIZATION

Allianz Asset Management

- Globally aligned methodology for annual assessment of all relevant compliance risks; integration into global ERM
- Local / regional / global compliance programs following a risk based approach; closely aligned to the results of the risk assessment
- Specific risk assessments for certain high risk areas performed closely together with relevant business functions
- Certain compliance risks become part of the risk control self-assessment, which is feeding into the Top Risk Assessment (CoRA → RCSA → TRA)

THANK YOU

We want your feedback! Use the conference app or visit the Registration Desk.

Be sure to join the Twitter conversation: @CWEurope