



Enterprise Wide Risk & Assurance Management

IRM Risk Forum
20th September 2004



What is risk?

- “Risicare” – old Italian
- “To dare”
- Threats to objectives
- Missed opportunities
- Uncertainties in achieving objectives
- Management of the business



Uncertainty

“Reports that say that something hasn’t happened are always interesting to me, because, as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don’t know we don’t know”

Donald Rumsfeld
US Defence Secretary



Lessons Learned

- UKPS 1999
- CRB
- Business Processes rather than IT?
- Difficulties recognised on the ground
- Initial price rather than long term VFM
- Manageable implementation steps
- Complexity of change
- Inadequate resources
- Testing & contingency



Stage 4
Predictive – integrated approach:
the business thinks risk.

Stage 3
Proactive –
• risk analysis
• spot trends in KRIs by monitoring against triggers

Stage 2
Reactive – investigate & review control

Stage 1
Band aid – compliance only



Management by risk

- Risk focused
 - Targeting resources & effort on risks to key objectives
 - Supporting achievement of business objectives
- Rigorous in examination of costs & other impacts of risks & mitigation
- Integrated into
 - Regular business activity
 - Business planning & reporting
 - Performance management
- Designed to improve assurance whilst containing costs of compliance



Enterprise Wide Risk & Assurance Management

Objectives

- Help manage the business better
- Increase probability of achieving objectives
- Avoid/minimise unnecessary loss/disruption
- Informed decision making
- Take advantage of opportunities
- Embedded process
- Effectiveness improved
- Supports performance management



Enterprise Wide Risk & Assurance Management

Process

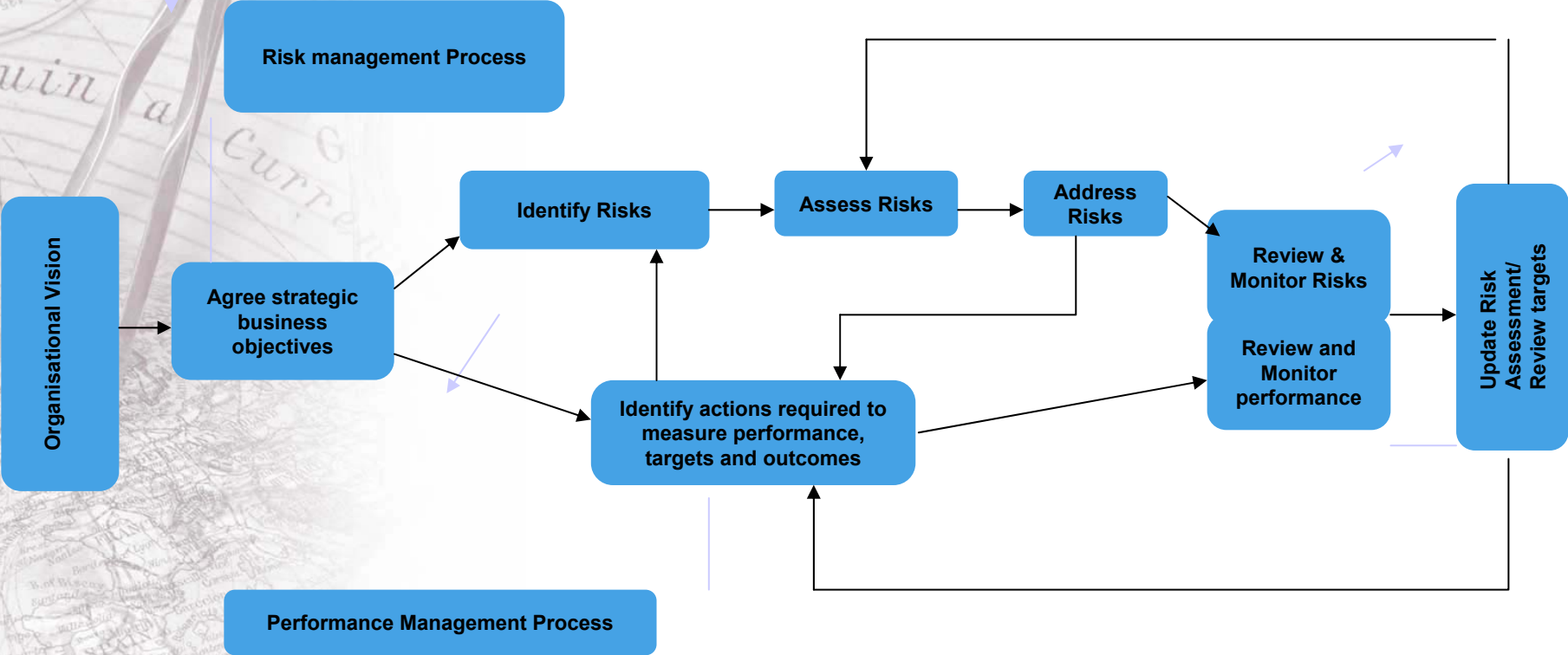
- Objectives & outcomes
- Key performance indicators
- Key business processes
- Threats & opportunities
- Assess likelihood & impact
- Current controls
 - Residual risk
 - Too little?
 - Too much?
- Balance costs of risk & mitigation
- Monitoring & assurance
- Iterative process



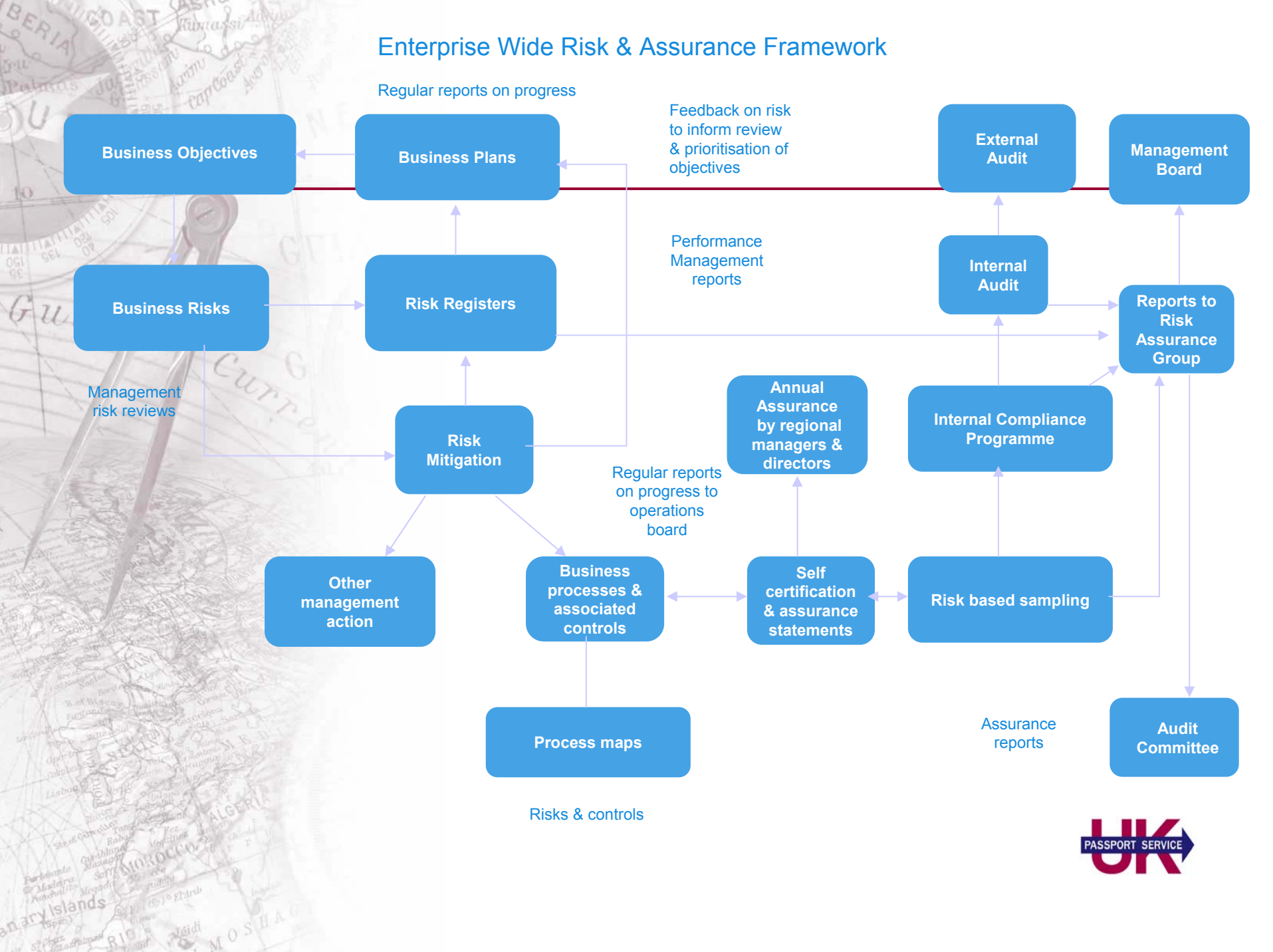
Performance Management

- Business Plans
- Objectives
- Activities
- Processes
- Dependencies
- Key Performance Indicators
- Vital Signs
- Business reports

Performance Management



Enterprise Wide Risk & Assurance Framework





Risk impacts

- Operational disruption
- Missed productivity and other targets
- Quality standards not achieved
- Timescales
- Costs (increased &/or unbudgeted)
- Missed objectives
- Resource pressures
- Fraud prevention/detection
- Change programme



Cost of risk

- Lost production
- Additional staff
- Inefficiencies
- Fraud levels
- Compensation payments
- Rework
- Reputation
- Multiply by likelihood
- Exceeds mitigation cost?



Risk Assessment - Severity

- Red (High) severity risk. There is significant concern about carrying this risk. It has the potential for a severe, if not a disastrous impact on business activities and/or reputation. Immediate action is required.
- Amber (Medium) severity risk. There is unease about carrying this risk, but the consequences are not severe and can be managed by timely actions. Action plans require development and the risk should be kept under continuous review. Risks with a Severe Impact score, but overall Medium Severity rating, should be considered for more immediate attention – in effect treated as High Severity.
- Green (Low) severity risk. UKPS is content to carry this risk or feels that it is under effective control. The risk status requires periodic review.



Risk Tolerance & Appetite

What is an acceptable risk?

- One that is effectively mitigated by an internal control – even if a high risk
- One that cannot be mitigated cost effectively
- Within agreed thresholds

What is an unacceptable risk?

- Impact on ability to meet business objectives
- Causes failure to achieve Key Performance Indicators
- Exposes UKPS to risks of fraud
- High risk with ineffective &/or incomplete control
- Threatens UKPS reputation
- Outside agreed thresholds



Key Risk Indicators

Risk triggers, for use at a corporate and local level:

- Linked to Key Performance Indicators and associated management information reports
- Providing early warning signs of likely risks
- Related to requirements for effective business processes and controls
- The absence of effective and/or complete controls which would increase the probability/impact of a business process risk

The background of the slide features a faded, historical-style map of the Mediterranean region, including parts of North Africa (Morocco, Algeria) and the Iberian Peninsula. A large, semi-transparent compass rose is visible in the upper left corner, and a pair of metal dividers is positioned over the map, pointing towards the bottom left. The title 'Mitigation Strategies' is prominently displayed in a bold, dark red font at the top center.

Mitigation Strategies

- Treat
- Transfer
- Tolerate



Risk Mitigation/Control

- Cease activity
- Alternative solution/method of delivery
- Transfer risk
- Take risk back
- Reduce likelihood &/or impact
- Accept & retain
- Take advantage of risk
- Contingency – if outside of control

A background image featuring a map of the Mediterranean region, including parts of North Africa (Morocco, Algeria) and the Iberian Peninsula (Spain, Portugal). A compass rose is visible in the upper left, and a pair of dividers is positioned over the map. The text 'UPPER GUIN' is partially visible on the map.

Risk Control Assessment

- Current control
- Residual risk
- Additional controls needed
- Escalate risk to achieve control needed?



Risk Responsibilities

Risk ownership

- Part of management responsibilities
- Aligns with objectives & outcomes
- Person best placed to achieve effective overall management of risk
- Assess risk & mitigation options
- Monitor mitigation owners actions
- Regular progress reports

Action owners

- Responsibility for delivery to timetable & cost
- Regular progress reports

Acceptance of responsibilities

- Performance management processes



Risk Assurance Co-ordinators

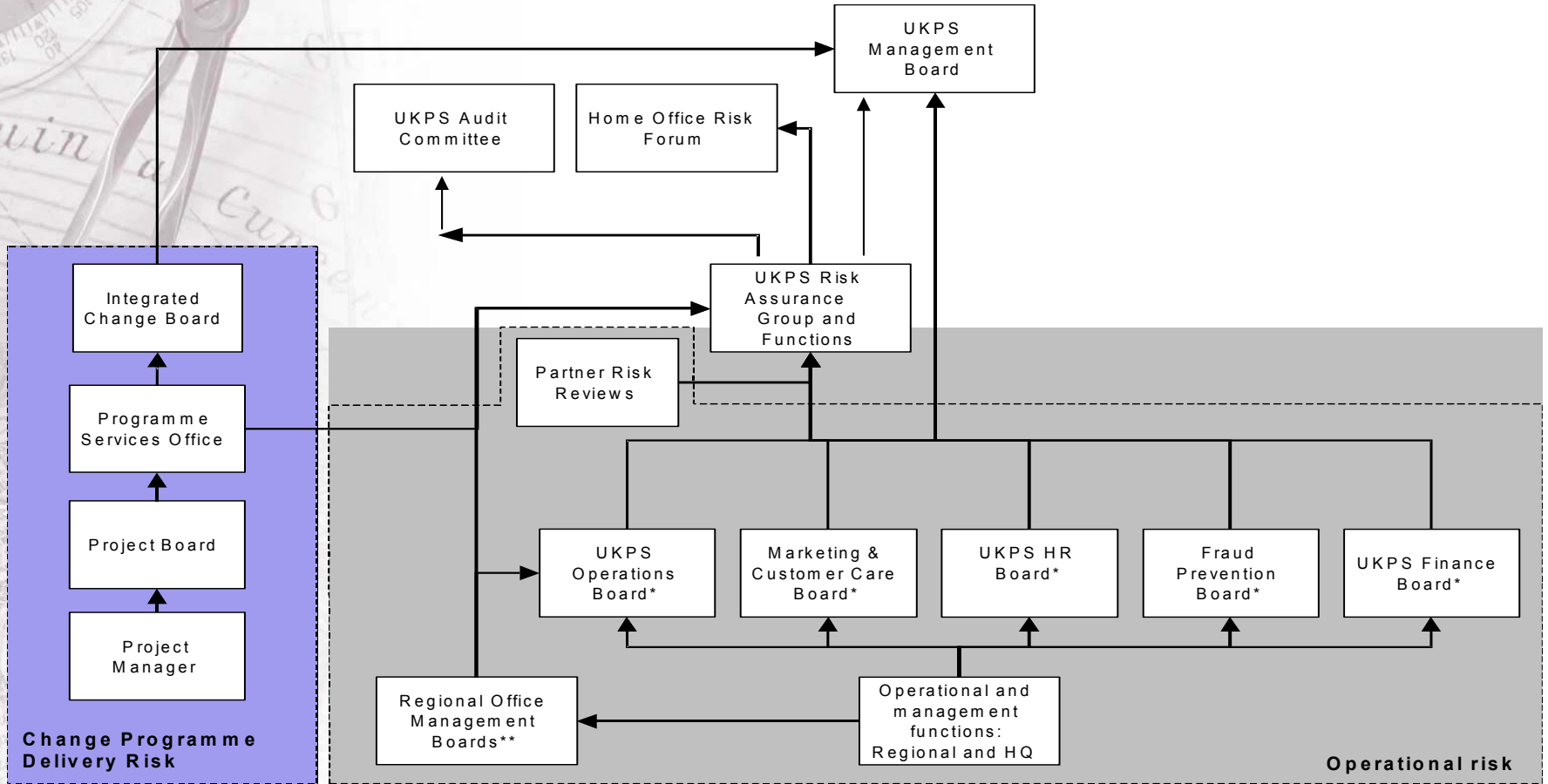
- Directorate/office focus for risk and information management
- Enhance risk awareness within directorate
- Facilitate directorate risk identification and assessment
- Document risks in a directorate Risk Register, in conjunction with risk owners
- Escalate risks to Risk Assurance Group



Risk Escalation

- A corporate objective or KPI is under threat by the risk
- A regional or directorate objective or KPI is under threat by the risk, and local management feel that it is outside of their control
- A major control weakness in a key business process has been identified
- Promotion & relegation!
- Impact on other offices/function/projects
- Cumulative risks

Risk Reporting & Escalation





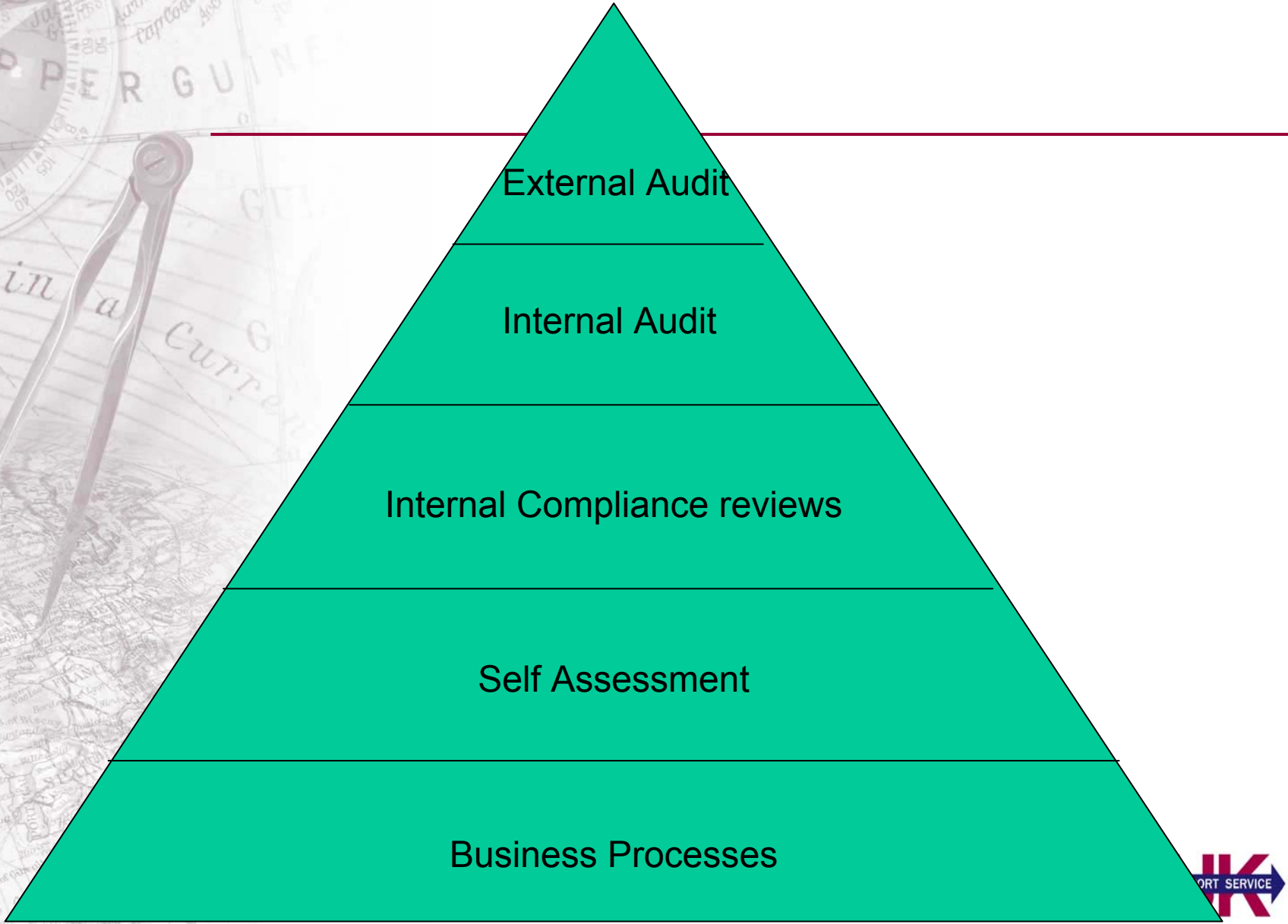
Corporate Governance

- Structure for
 - Strategic planning
 - Management
 - Operations
 - Change
 - Business control
- Accounting Officer
- Statement on Internal Control
- Audit Committee
- Management Board
- Sub Boards/Directorates
- Regional Office Management
- Integrated Change Programme



Assurance processes

- Risk registers
- Self assessment
 - Risk based
 - Evidential support
 - Exception reports
 - Management sampling
- Internal compliance reviews
 - Risk based
- Internal audit
- External audit



External Audit

Internal Audit

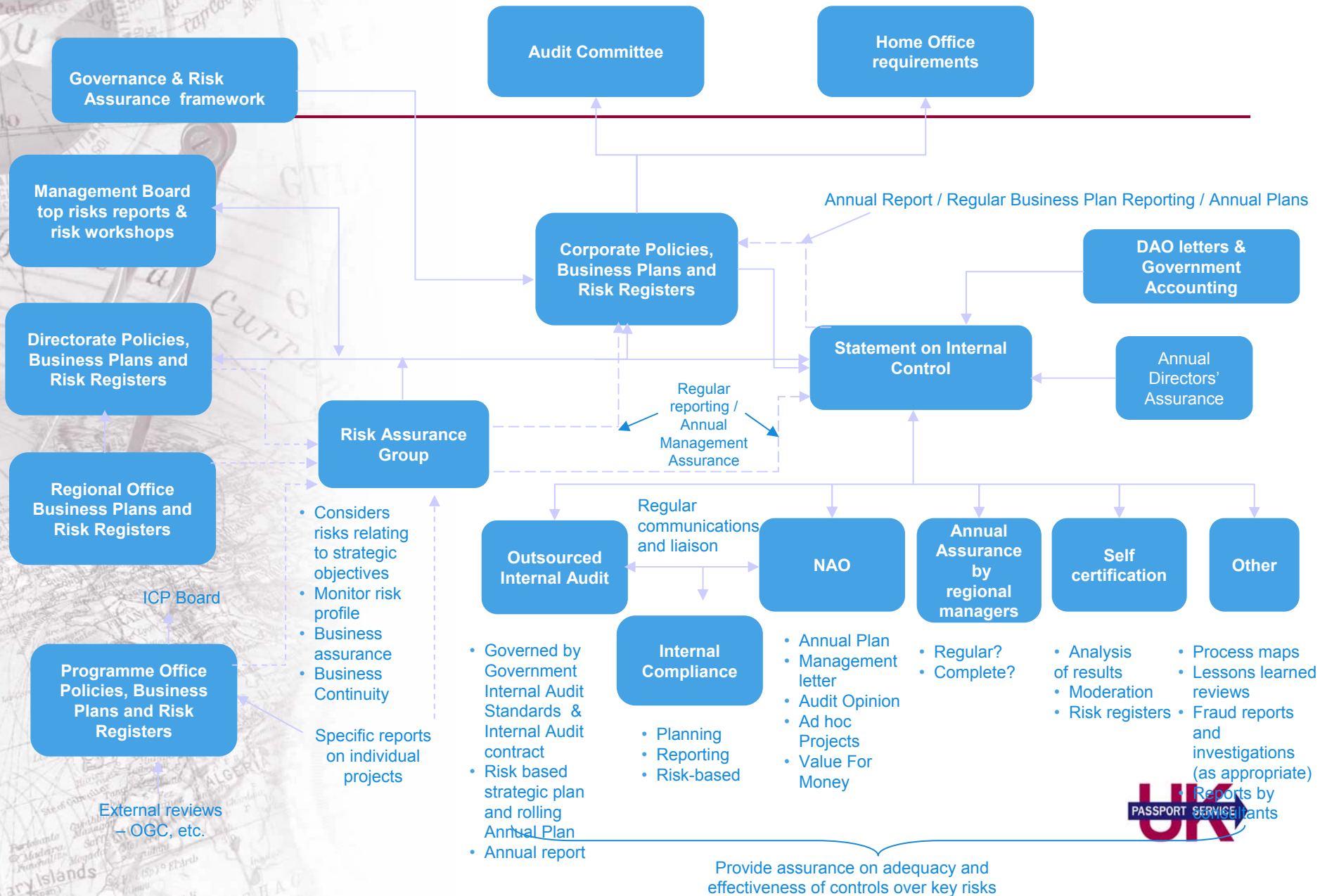
Internal Compliance reviews

Self Assessment

Business Processes



UKPS Risk Assurance Map



Questions?

