EFFECTIVE RISK MANAGEMENT

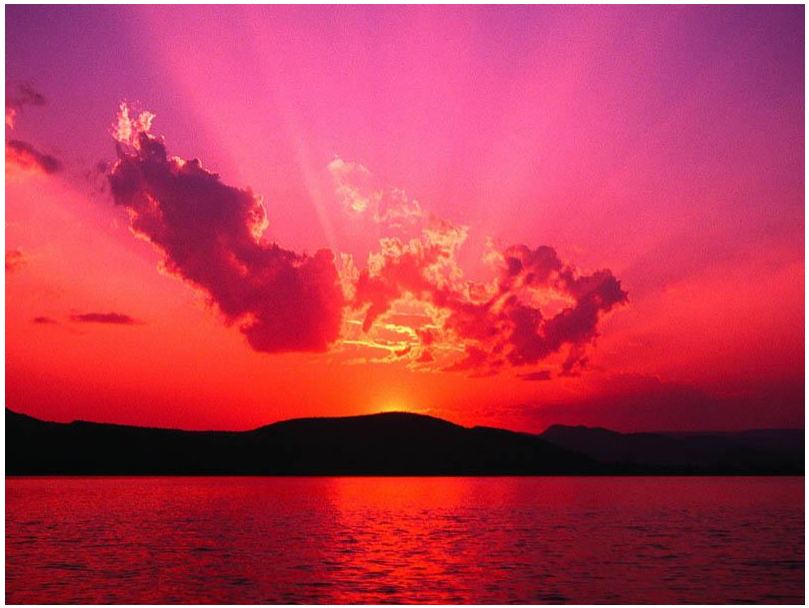
Steve Giles
(MA Oxon. ACA)

Course Objectives

- Awareness of modern risk management tools & techniques
- A better understanding of risk and how to take a risk-based approach
- How to use risk to constrain threats and take advantage of opportunities
- Increased knowledge through shared experiences

Course Timetable

- Introductions
- The nature of risk
- Business risk management framework
- Risk management in action: financial crime
- Effective business risk management
- Summary & conclusions
- Quizzes, exercises & presentations



Risk – Brutal Refresher Course

- Credit risk – subprime (2007)
- Liquidity & counter-party risk – Lehman's (2008)
- Financial crime risk – Madoff (2009)
- Sovereign risk – Eurozone bonds (2010)
- Geo-political risk – Egypt etc. (2011)
- Environmental risk – BP (2010), Fukushima (2011)
- Reputational risk – Barclays, HSBC, Fifa, VW (2012 - 2015)

Risk Awareness Soundings

- What is risk?
- Who has responsibility for managing risk in your firm?
- How is risk measured?
- Are you looking to minimise risk in your organisation?
- What are the two fundamental questions that you need to ask about internal controls?
- What are the essential features of an effective risk management process?
- Why should firms look to manage risk in a systematic way today?

Session 1 – The Nature of Risk

- Definitions, impact & probability, risk appetite
- Business risks in the 21st Century
- Reputation
- Risk management cycle & risk value charts
- Examples of failures to manage risk effectively

Risk Management - What is it?

- **Risk** - uncertainty of outcome
- **Management**:

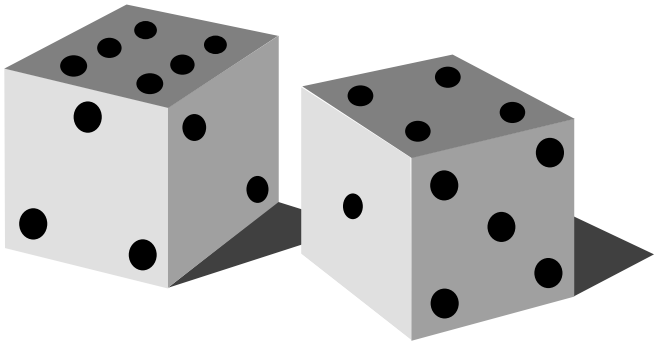
✓ a consistent & systematic process

✓ identify, analyse, evaluate, mitigate, monitor & communicate risk

- **In an uncertain world, two things can happen:**

✓ the chance of loss

✓ BUT also the opportunity for gain



Definitions

- **Risk**

  "The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood."

SO

✓ No business can eliminate all risk, so risk has to be managed effectively. This is best done through a risk-aware culture.

- **Risk Management**

  "A process to identify, assess, manage and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation's objectives."

OR

✓ **"A discipline for managing uncertainty"**

Key Risk Terms

- **Impact & probability – the "measures" of risk:**

✓ impact = severity of the event should it materialise

✓ probability = likelihood of an event materialising during a certain period of time

- **Risk registers (matrices, maps, profiles):**

✓ visual aids showing expected loss frequency and expected severity

✓ highlight control gaps

✓ aim is to ensure risk is acceptable. Risk matrices highlight areas of high residual risk, which must be reduced by extra controls to bring them within the corporate risk appetite

Risk Appetite

- "Are we looking to minimise risk in our business?"
- **Risk appetite is the amount of risk, on a broad level, that an entity is willing to accept in the pursuit of value**
- Use quantitative or qualitative terms (e.g. earnings at risk vs. reputation risk), and consider risk tolerance (range of acceptable variation)
- It is important for boards to agree their appetite and tolerance for individual key risks
- **Examples of key questions:**

✓ what risks will the company not accept? *(e.g. environmental or quality compromises)*

✓ what risks will the company take on new initiatives? *(e.g. new product lines)*

✓ what risks will the company accept for competing objectives? *(e.g. gross profit vs. market share)*

- Modern definition (BIS Corporate Governance Guidelines – July 2015)

✓ **"the aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan"**

21st Century Business Risks

- Reputation
- Conduct
- Third-party
- Health & safety
- Security
- Financial crime
- Human capital
- Ethical
- Financial
- Competition
- Technological
- Environmental
- Legal & regulatory
- Operational
- Cyber
- Others

The Edward Snowden Case

- Worked in IT at the CIA
- Resigned in 2009 – employed by Dell as a contractor at the NSA
- Transferred to Hawaii in 2012 – works at the NSA's regional cryptology centre
- March 2013 takes a new job with Booz Allen Hamilton – systems administrator at the NSA
- May 2013 disappears – re-surfaces in Hong Kong, then in exile in Russia
- Stole thousands of top secret documents from the NSA and made them public via media disclosures
- Method – download onto thumbnail drives
- **Implications:**

✓ Security threats

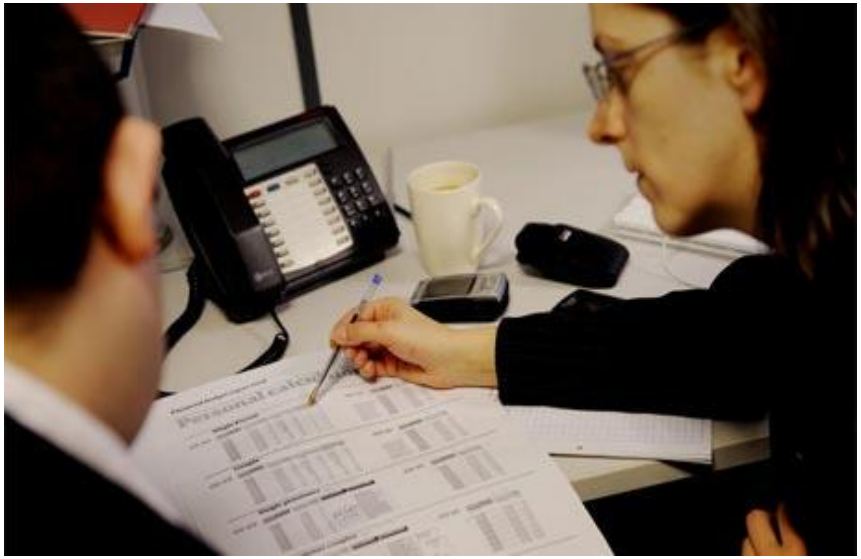
✓ Ethical risks

Aon 2015 Bi-Annual Global Risk Survey

- Damage to reputation (4)
- Economic slowdown (1)
- Regulatory/legislative change (2)
- Increased competition(3)
- Failure to attract/retain top talent (5)
- Failure to innovate and/or meet customer needs (6)
- Business interruption (7)
- Third-party liability
- Cyber-crime
- Property damage

Reputation Risk – Example: Arthur Andersen

- One of the “Big 5” accounting firms
- Became embroiled in the Enron scandal
- Found guilty at first hearing of obstructing a criminal investigation by shredding documents
- Lost its reputation for professionalism & integrity
- Judgment overturned on appeal
- Too late!

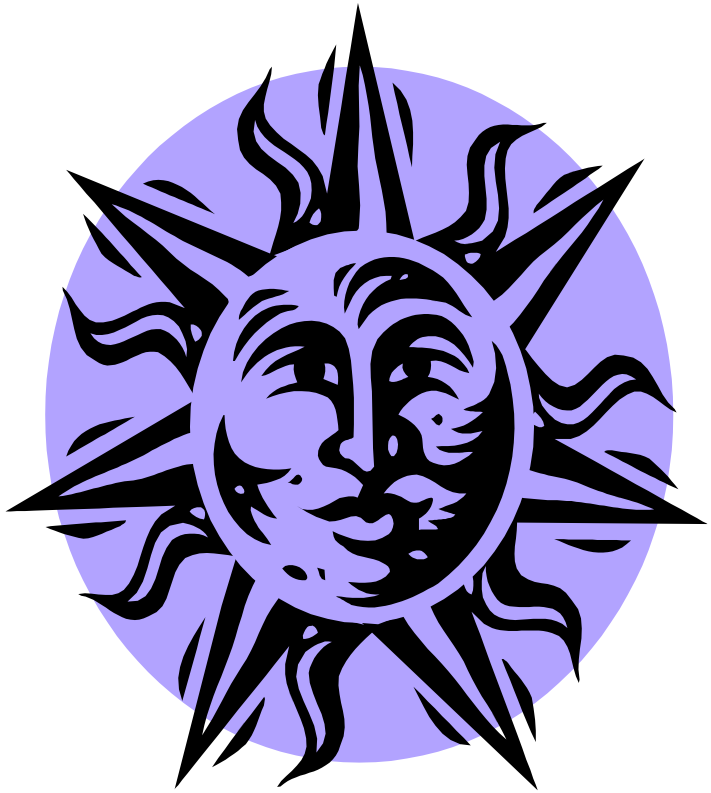


Reputation Risk – Example: BP

- History of safety scandals:
- ✓ Alaskan pipeline
- ✓ Texas City oil refinery
- ✓ Macondo oil well
- "pervasive problem of a complacent industry"
- $40 bn is the estimated cost to BP of the Deepwater Horizon oil spill
- Effect on share price
- Effect on careers

What is Reputation?

- **Four key components:**
- ✓ Leadership (success & innovation)
- ✓ Fairness (giving customer a good deal and treating stakeholders fairly)
- ✓ Corporate responsibility
- ✓ Trust
- **Other factors:**
- ✓ Consistency
- ✓ Brand (meaningful, different, salient)
- ✓ Past record & future promise



Reputation Re-Build – Example: Siemens

- Europe's largest engineering conglomerate
- 2006-08 corruption scandal – widespread bribery of officials to win contracts
- **Root cause** – poor culture and failure of legal and regulatory risk management
- **Consequences include**: $1.6bn fines; ban from procurement lists; share price fell > 50%; directors and managers sacked & prosecuted
- **Trust re-build**:

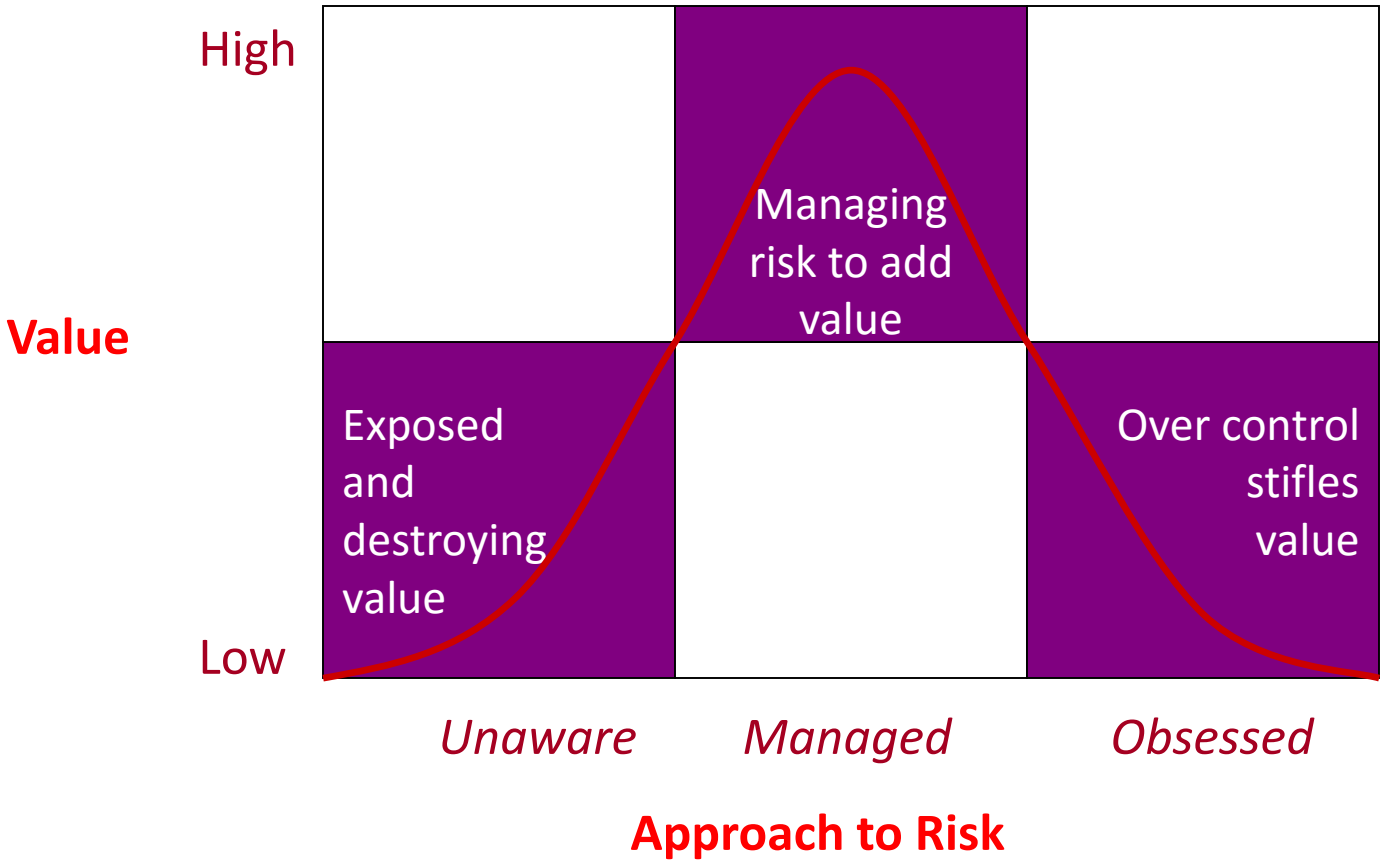
✓ Apologise and commit to full investigation

✓ Change at the top

✓ Compliance greatly enhanced - increase in numbers from 60 to 600 and head given a seat on the management board

✓ Cultural change – e.g. comprehensive training programme and compliance now an integral part of incentive pay system for managers

Managing Risk to Add Value



5-Stage Risk Management Cycle

- **Stage 1 - Set the strategy & assign responsibilities**

✓ Governance dimension

- **Stage 2 - Identify risks**

✓ Workshops and/or horizon scanning

- **Stage 3 - Prioritise risks**

✓ Risk scoring methodology

- **Stage 4 - Assess control effectiveness**

✓ Beware of simplistic and over-optimistic assessments

- **Stage 5 - Monitor & measure improvements**

✓ A continuous process

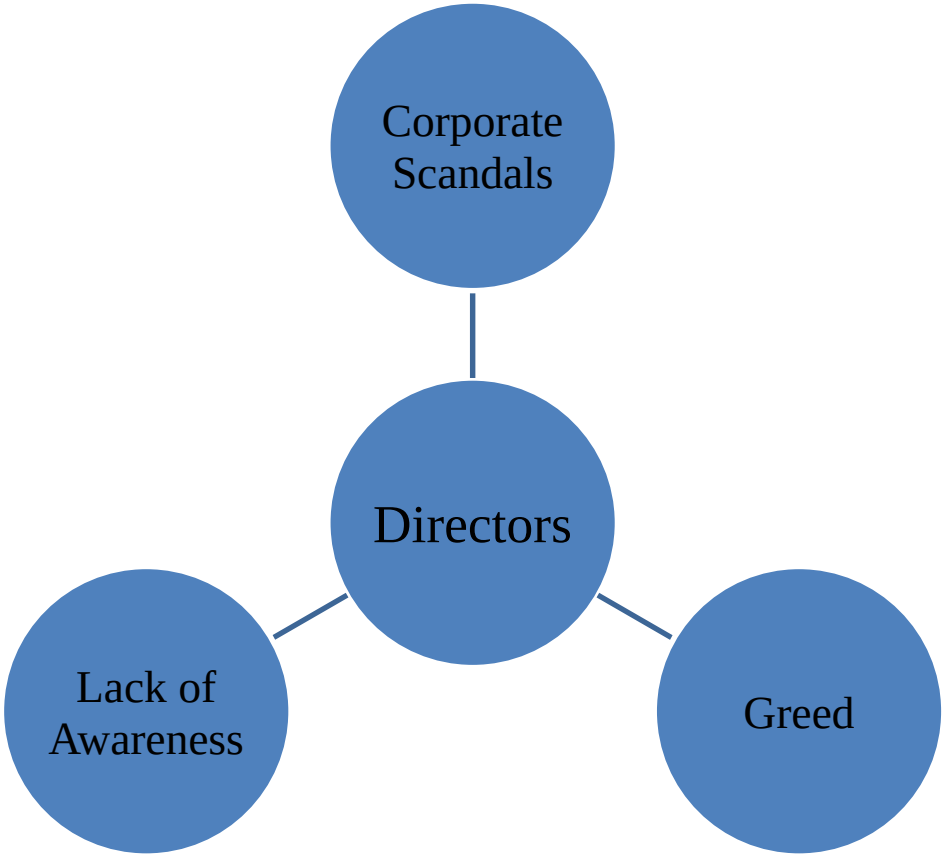
Business Risk Management Framework

- Scandals and crisis – examples of failures of risk management
- Risk and internal controls theory
- Modern risk management models
- The key risk management tools
- Group Case Study

Examples of Scandals and Failures 2012-2015

- Barclays
- Olympus
- RBS
- HSBC
- Standard Chartered
- G4S
- JP Morgan
- News Corporation
- Coutts
- Galleon/McKinsey
- GlaxoSmithKline
- UBS
- BBC
- Findus
- Target
- Serco
- Vatican Bank
- NHS – Mid-Staffs
- Liberty Reserve
- National Security Agency
- Co-op Group
- FIFA
- BNP Paribas
- Bank of America
- Petrobras
- Tesco
- Thomas Cook
- Tom Hayes
- VW

Failure & Scandal Overview



Modern Risk Management Models

- Turnbull & SOX
- COSO, Basel Capital Accords
- Three Lines of Defence
- But the key area is operational risk. All models are vulnerable to technological failure and human factors:

✓ glitches and back office shortfalls

✓ human error; poor judgement; unexpected events; “gaming” the system; negligence and complacency

Turnbull Framework – Four Stages

- **Identify & assess risks**

✓ completeness, likelihood, impact, timeframe

- **Design controls**

✓ prevention/detection, cost perspective, objectives

- **Test controls**

✓ are the controls operating efficiently and effectively?

- **Governance dimension**

✓ Assess principal risks

✓ Report on effectiveness of risk management and internal control systems

UK Code of Corporate Governance – C.2 Risk Management and Internal Control

- **Main Principle**

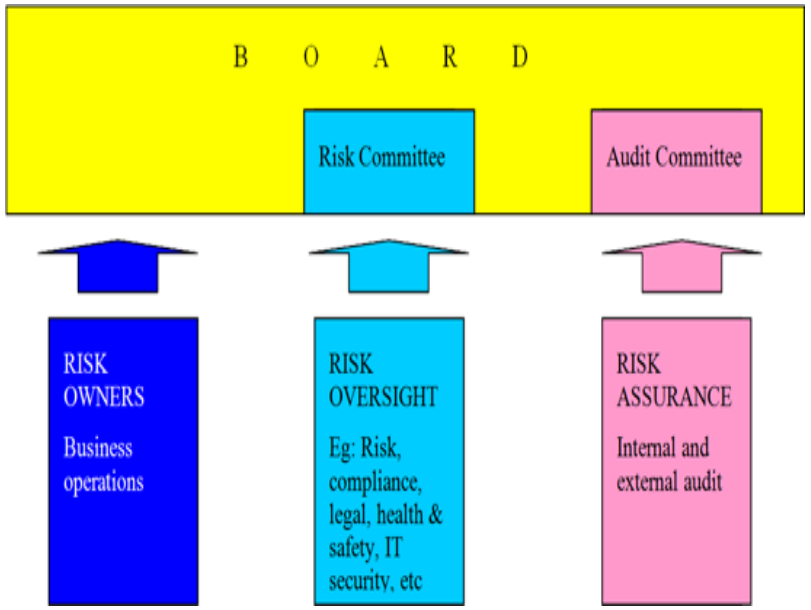
✓ "The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems."

- **Code Provision**

✓ "The board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems and should report to shareholders that they have done so. The review should cover all material controls including financial, operational and compliance controls."

Three Lines of Defence Model

- **First line of defence** – business line management
- **Second line of defence** – the risk management function
- **Third line of defence** – an independent review & challenge



Basel Accords - Key Aspects

- Capital adequacy standard for financial institutions
- Aim: promote the safety & soundness of the banking system
- Emphasises the importance of improved RM throughout
- Requires a loss database & a conceptually sound RM system
- Designed to boost investor confidence
- Reforms following the banking crisis
- Towards Basel 3

Basel II & Operational Risk

- A “new” risk category for banks
- Definition:

  “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”
- Operational risk is an independent risk category that must be backed by regulatory capital
- The management of operational risk involves the identification, assessment, monitoring and control and/or mitigation of risk
- **Components of operational risk:**

✓ Internal fraud

✓ External fraud

✓ Employment practices & workplace safety

✓ Clients, products and business practices

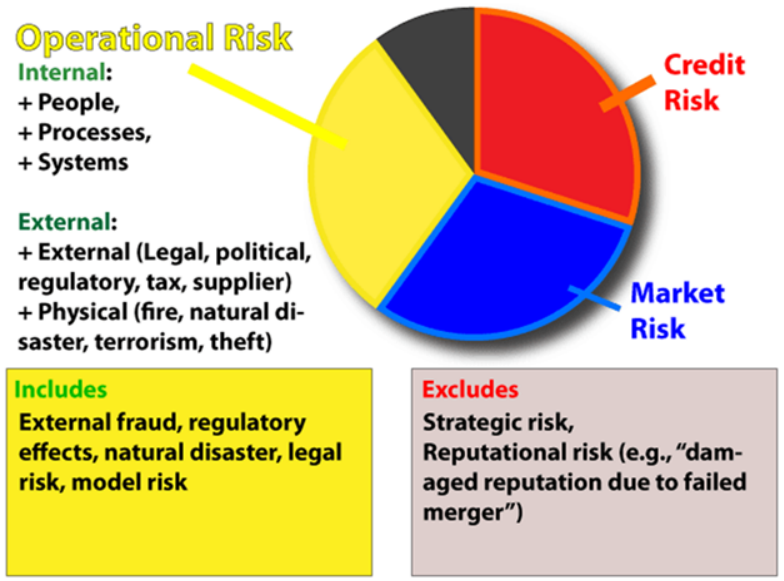
✓ Damage to physical assets

✓ Business disruption & systems failure

✓ Execution, delivery & process management

Basel Committee on Banking Supervision

- Sound Practices for the Management & Supervision of Operational Risk (June 2011)
- An update on 2003 paper
- Based on 11 principles covering:
  - Governance
  - Risk management environment
  - Monitoring & reporting
  - Control & mitigation
  - Business resiliency/continuity
  - Role of disclosure
- Principles are relevant to all banks



COSO – The “Enterprise-Wide” Approach

- A holistic approach – avoids “silo risk management”
- A documented process (e.g. system of risk registers)
- Focus on:

✓ incident reporting

✓ detecting warning signs

✓ contingency planning & risk mitigation

- Danger of complacency

The COSO Models

- The Committee of Sponsoring Organisations of the Treadway Commission (“COSO”)
- 1992 - developed an integrated framework for internal controls (updated in 2013)
- 2004 – developed the integrated Enterprise Risk Management (“ERM”) framework

Key Points of the COSO Model

- **Definition:**

✓ *"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

- **Underlying principles:**

✓ Every entity, whether for-profit or not, exists to realize value for its stakeholders

✓ Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day

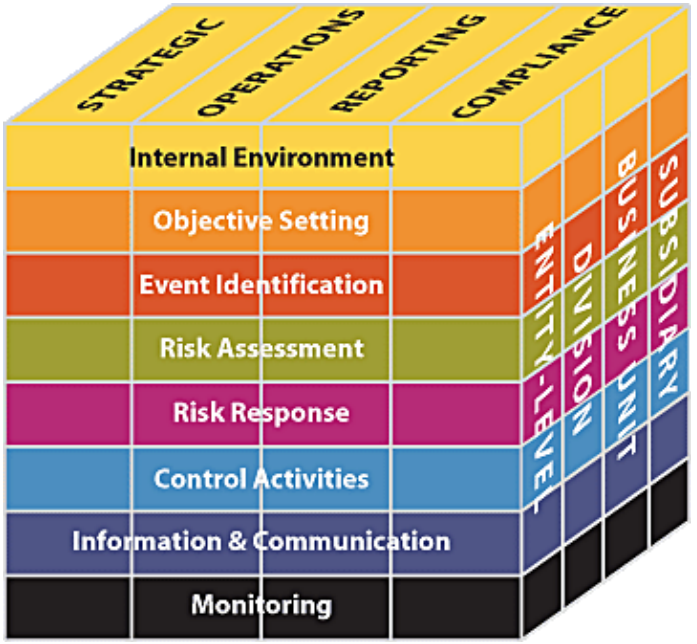
- **ERM supports value creation by enabling management to:**

✓ Deal effectively with potential future events that create uncertainty

✓ Respond in a manner that reduces the likelihood of downside outcomes and increases the upside

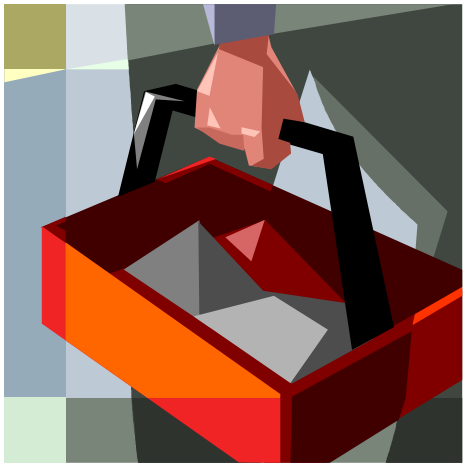
The ERM Framework

The eight components of the framework are inter-related…..



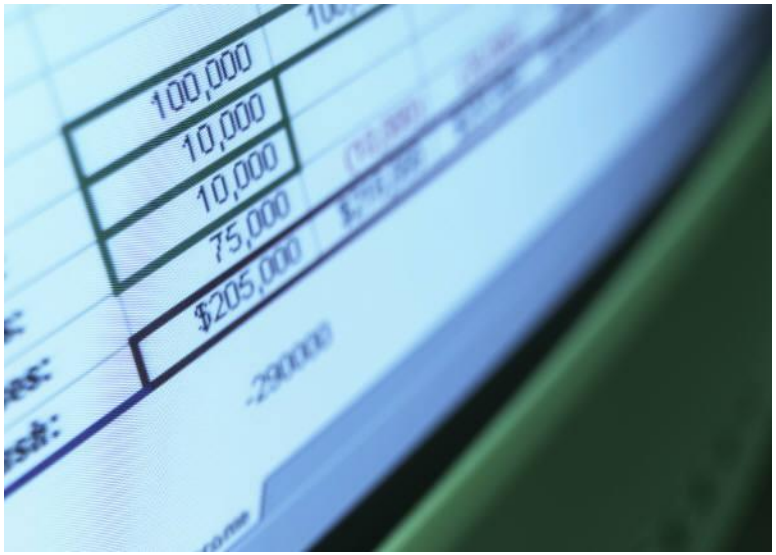
Risk Management Toolkit

- Qualitative
  - risk registers
  - key risk drivers
- Quantitative
  - loss event database
  - key risk indicators

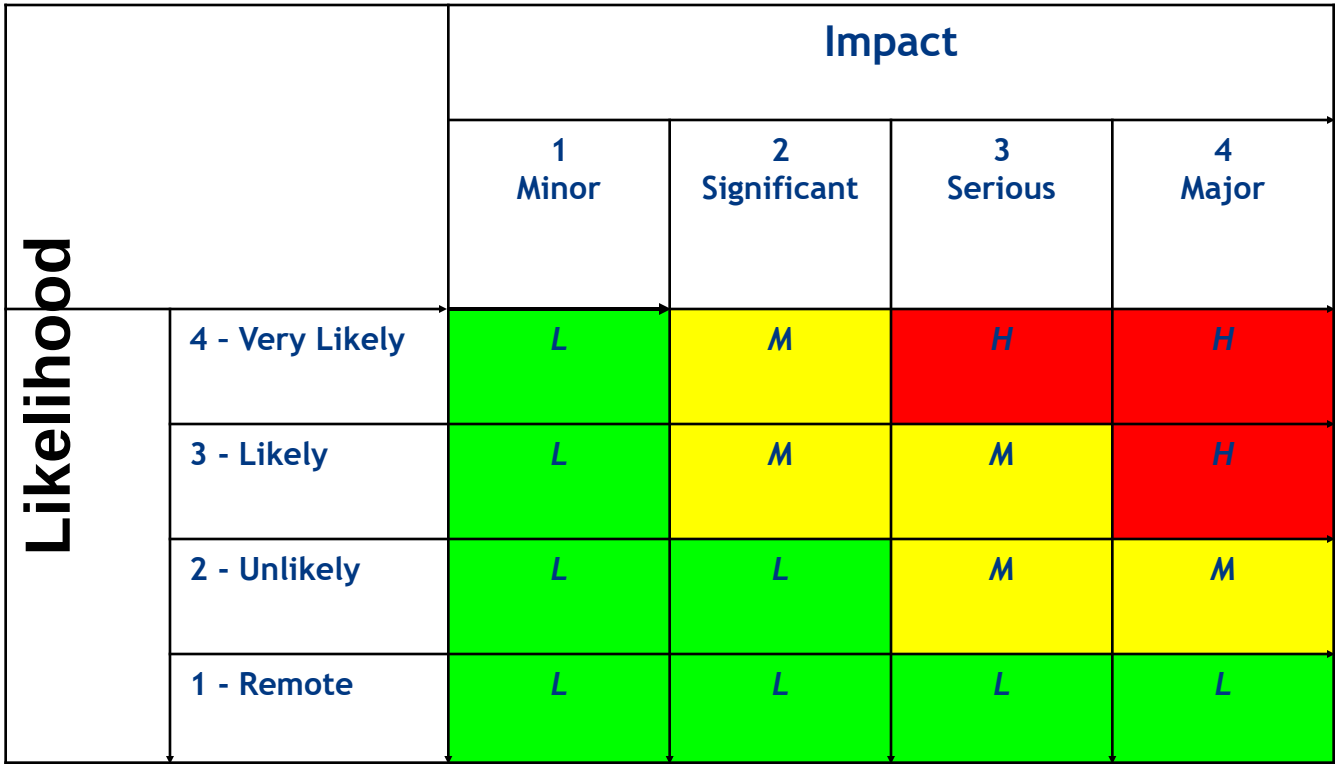


Practical Management - The Risk Register

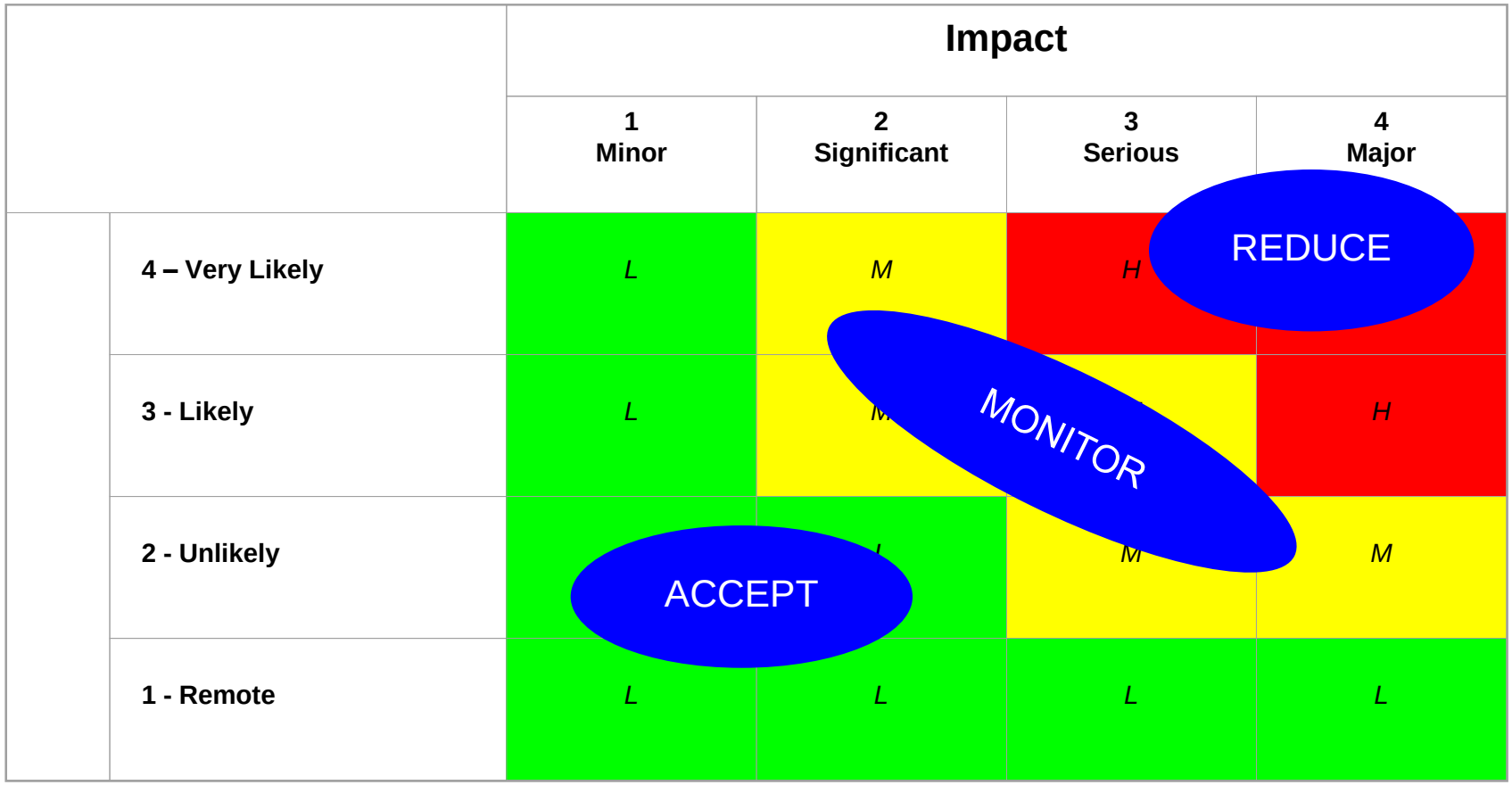
- The key risk management tool
- Based around impact & probability measures
- Top down and bottom up approach
- Combines risk assessment & risk mitigation measures
- Spreadsheet, often with “traffic light” features
- Responsibility, action plans & timescales for improvements
- Regularly reviewed & updated



Risk Assessment



Acting on the Risk Profile



Key Points on the Risk Register

- Purpose is to highlight control gaps
- Aim is to manage risk within the risk appetite
- No blame attached to “red”
- Needs conscientious review, action plans and escalation process
- Provides evidence of discharge of responsibilities - risk assessment should be “periodic, informed and documented”

Key Risk Drivers

- Measures that drive the inherent risk profile
- Examples:
  - state of the economy
  - transaction volumes
  - staff levels
  - level of change
  - product maturity
  - customer satisfaction
- Are forward looking & predictive of future issues

Loss Event Database

- Need to build up history of empirical data
- Comprehensive
- Capture all loss events and quantify them
- Use the past as a predictor of the future
- Supplement with external information on high impact/low probability events

Key Risk Indicators

- A broad category of measures used to monitor control environment
- Examples:
  - overtime/error ratios
  - systems reliability
  - complaints levels
  - temp. or agency staff/permanent staff ratios
  - adverse comments on social media
- Need escalation criteria and risk awareness embedded in culture

Focus Session: Internal Controls

- “A strong system of internal control is essential to effective enterprise risk management” (COSO)
- Reasons for internal control
- Types of internal control

Controls Concept

- Control divides into:
  - external (governance-type)
  - internal
- Management is primarily responsible for internal control
- Two-tier test for the adequacy of internal controls:
  - are they fit for purpose, are they designed adequately; and
  - are they working in accordance with the design?

Purpose of Controls

- Internal controls set up by management to:

✓ help manage risks

✓ assurance re compliance with applicable laws & regulations

✓ bring order & efficiency

✓ ensure policies are followed

✓ safeguard assets

✓ ensure completeness & accuracy of records

Control Characteristics

Preventative

stop an event or risk occurring

Detective

Indicate when an event or risk has occurred

Manual

somebody has to actually do something

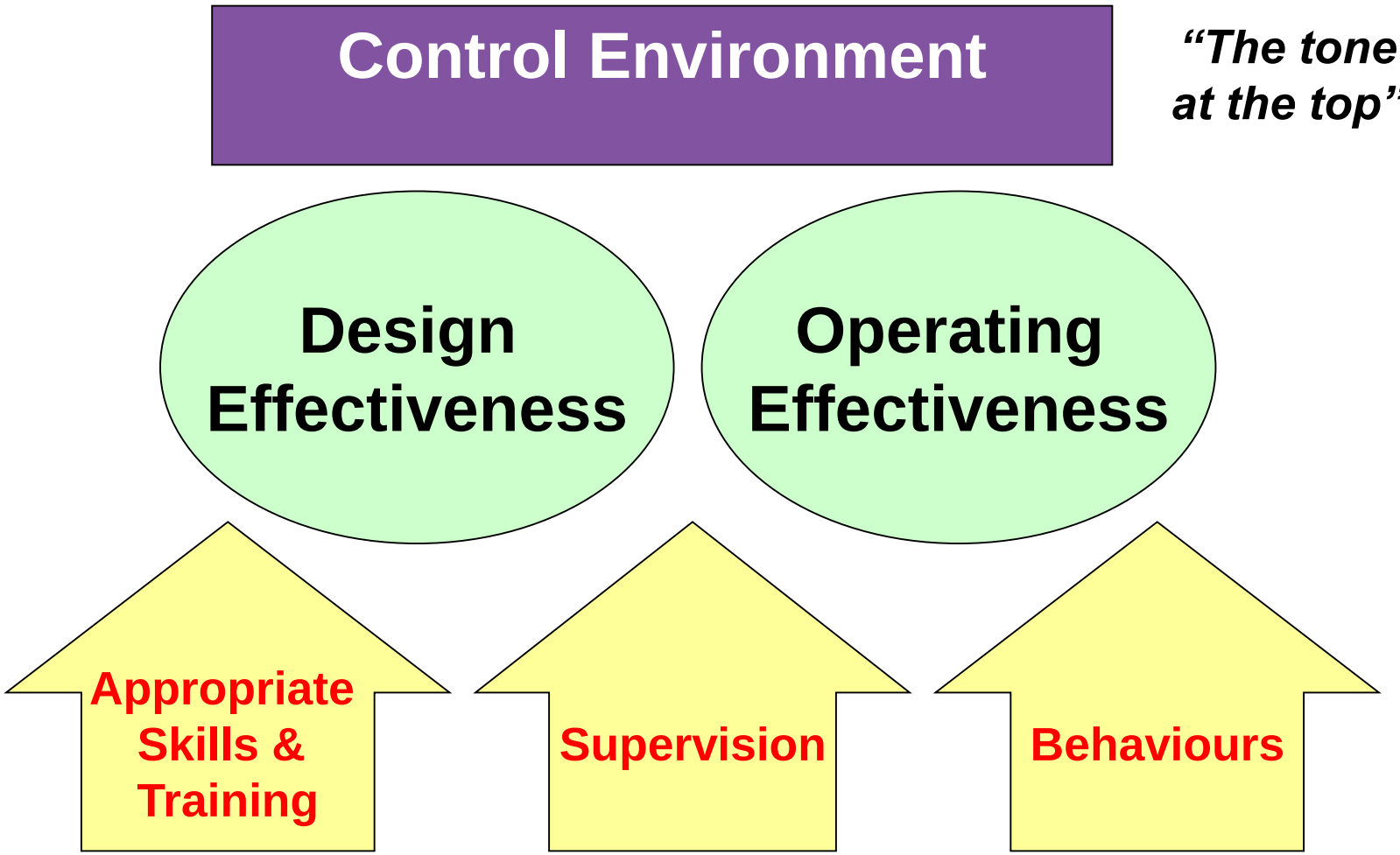
Automated

programmed / inherent in the system being used

Control Types

Policies & Procedures	**Reconciliation**
Authorisation Controls	**Segregation of Duties**
Key Performance Indicators	**Physical Security & System Access**
Recruitment & Exit	**HR Practices**
Training & Development	**Internal Audit**
Management Review	**Automated Exception Report**

Effective Controls



The “4 Ts” Approach to Risk Management

- Every risk exposure can be managed by utilising one of four “Ts” as follows:

✓ Tolerate - accept the risk;

✓ Transfer - let someone else take part of the risk;

✓ Terminate - eliminate the risk; or

✓ Treat - take cost-effective in-house actions to reduce the risks

Key Points on the “4Ts”Approach

- Shows the range of techniques available to manage risk
- Traditional controls reduce probability risk
- Use other methods (insurance, contingency plans etc.) to reduce impact risk
- Highlights the importance of insurance
- Understand where the “red lines” are in your business
- Don’t waste time and effort in areas of low risk

Risk Management in Action – Financial Crime

- Financial crime compliance and risk management framework
- Overview of anti-money laundering , fraud and bribery and corruption threats
- The AML risk-based approach
- Adequate procedures and the Bribery Act 2010
- The “Top 10” anti-fraud controls
- The role of auditors in the prevention & detection of fraud
- Financial Crime Quiz

Global Financial Crisis 2008

- **Central issue** – impact of poor credit decisions on bank capital and liquidity
- **Regulators' response**

✓ greatly increase capital and liquidity requirements - Basel III

✓ tighten regulations around financial crime – greater need for due diligence

- **Financial Crime Compliance** is a significant challenge for firms today

Financial Crime Compliance

- **Six categories:** money laundering; bribery & corruption; terrorist financing; sanctions evasion; tax evasion; fraud
- **The new attitude of the authorities**:

✓ Enormous fines (BNP Paribas - $9bn)

✓ Criminal convictions – personal and corporate (Tom Hayes – 14 years for manipulating Libor)

✓ Deferred Prosecution Agreements

✓ Extra-territorial impact (FCPA, Bribery Act, FATCA)

✓ Reputational damage

International Response

- **Worldwide action against corrupt business practices:**

✓ money laundering & terrorist financing; proliferation financing
✓ bribery & corruption; fraud; tax evasion; collusion & cartels; insider dealing

- **Examples of action taken and developing legislation:**

✓ Formation of the Financial Action Task Force 1989 (international AML standards developed)
✓ US Foreign Corrupt Practices Act 1977
✓ US PATRIOT Act 2001
✓ EU Anti-Money Laundering Directives
✓ Terrorism Act 2000
✓ Proceeds of Crime Act 2002
✓ Fraud Act 2006
✓ Anti-Money Laundering Regulations 2007
✓ Bribery Act 2010

- **Development of minimum standards:**

✓ Due diligence; suspicion reporting; risk-based approach; record-keeping; training; audit; senior management accountability and individual responsibility

National Strategic Assessment (NCA 2014)

- Presents a single, comprehensive picture of serious and organised crime affecting the UK– not just a threat, a reality. Costs £24bn pa
- 36,600 organised criminals in 5,300 groups
- **5 cross-cutting issues** – key vulnerabilities that criminals exploit:

✓ **Cyber** -growth in scale & speed of internet communication technologies

✓ **Corruption** – undermines trust, impact is disproportionate to frequency. A means of managing risk for the criminals

✓ **Money laundering** – scale is a threat to UK's economy and reputation

✓ **Borders** – importance of transnational crime

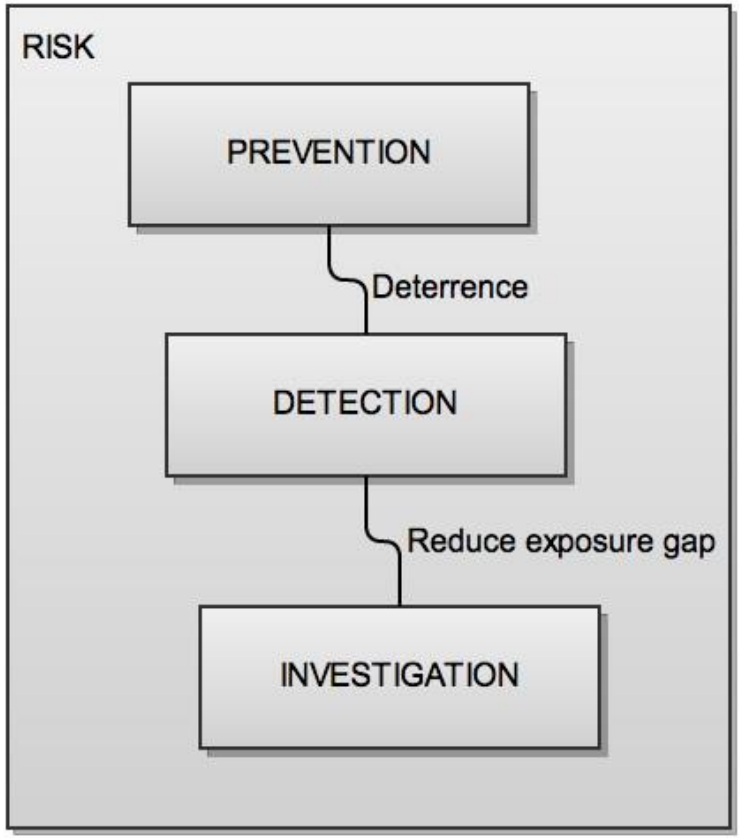
✓ **Identity** – both a commodity to be traded and needed to disguise true identity

- Key threats:

✓ Child sexual exploitation & abuse; criminal use of firearms; cyber crime; drugs; economic crime; organised acquisitive crime; organised immigration crime & human trafficking; serious and organised criminals in prison and under lifetime management

Framework for Managing Financial Crime Risk

- Risk-based approach
- Strong preventative approach
- Deterrence measures and awareness of the “perception of detection” factor
- Detective controls that reduce the exposure gap
- Access to investigative expertise
- The governance dimension – senior management responsibility and reporting lines



Money Laundering Framework

Crime	Cash	Scale of Operations	Severity of harm	Most affected population
Drug dealing	Exclusively	Very large	Severe	Urban minority groups
Terrorism	Mix	Small	Most Severe	Broad
White collar	Mix	Mix	Medium	Broad
Bribery and corruption	Sometimes	Large	Severe	Developing countries

Fourth Money Laundering Directive – Five Key Changes

- **Risk-based approach**. Increased emphasis on and broader application of the RBA: to apply at national level, to supervisors and to FIs and DNFBPs:

✓ appropriate to the size and nature of the entity

✓ "have to be documented, updated and available"

- **Politically Exposed Persons (PEPs).** Enhanced due diligence measures will always be appropriate for PEPs. Definition widened to include domestic individuals occupying prominent public positions
- **Increased scope**. Lowering the threshold for one-off transactions in cash requiring CDD from Euro15k to Euro7,500 (high value dealers)
- **Beneficial ownership.** 25% control threshold remains but transparency is increased by requiring companies (and trusts) to hold information on beneficial ownership and make it available (public registers)
- **Tax crimes.** Inclusion of tax crimes as predicate offences for the first time in the EU

The Risk-Based Approach

- The adoption of a risk management process for dealing with financial crime
- Key change – move from “tick-box” regime to one based on judgement
- Allows for a more efficient use of resources
- Each firm is unique, so need to design a risk profile appropriate for one’s own firm
- For individual business relationships, risk assessment is no longer customer-centric

AML – A Practical Approach

- **Aim** = to assess the most cost effective & proportionate way to manage & mitigate the risks faced
- **5-Step approach**:

✓ identify the money laundering & terrorist financing risks that are relevant to the firm

✓ assess and document the risks according to various factors (e.g. clients, products, delivery channels & geographical areas of operation)

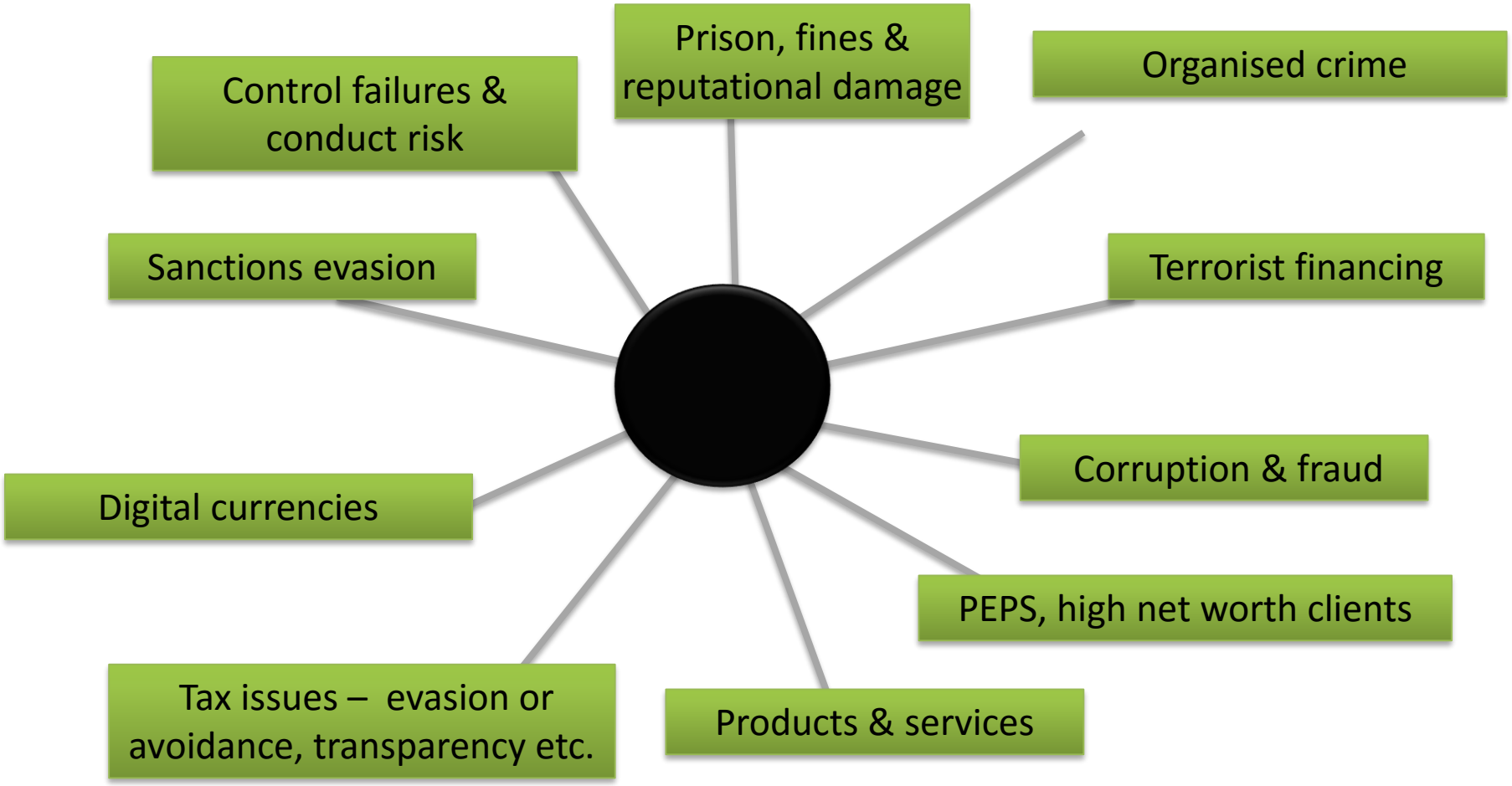
✓ design & implement controls to manage & mitigate the assessed risks (based on official guidance e.g. JMLSG or CCAB Guidance)

✓ monitor & improve the operation of controls

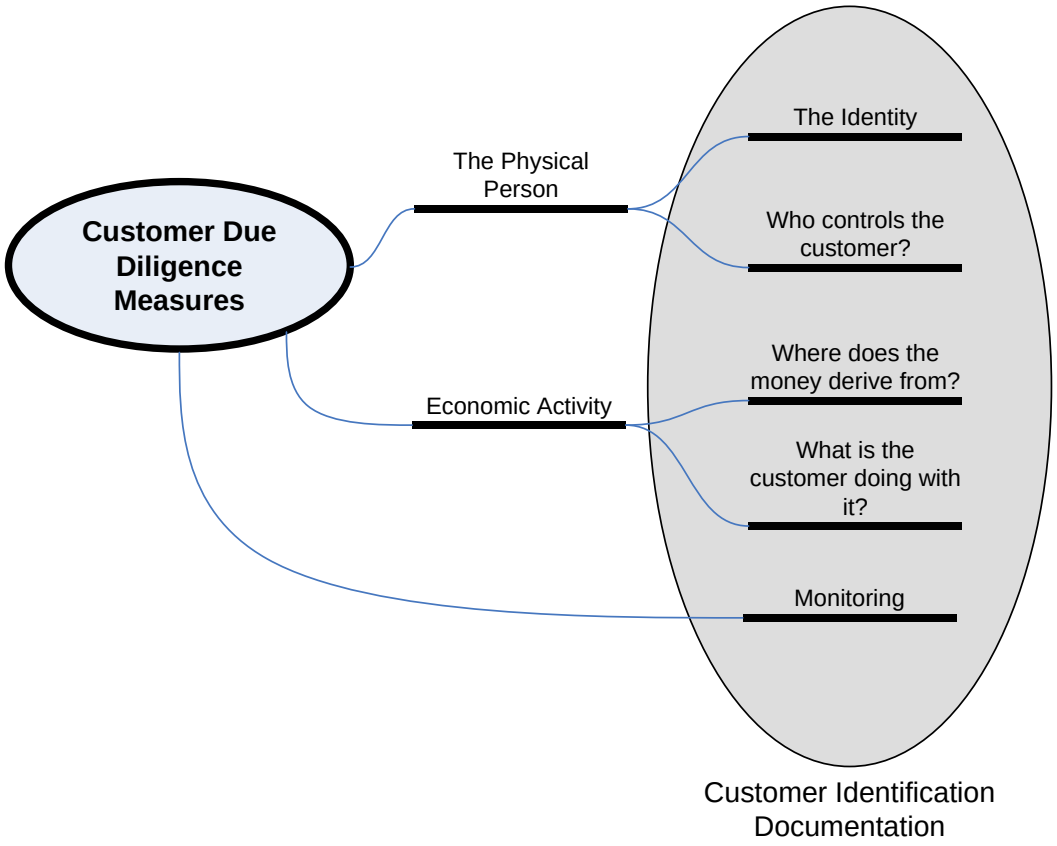
✓ record appropriately what has been done and why

- The system used should be appropriate to the firm's circumstances
- No system will detect and prevent all money laundering or terrorist financing

Money Laundering Threat Landscape



Customer Due Diligence Framework



AML Summary - Key Controls Include:

- Senior management involvement
- Compliance culture
- AML & CFT policies
- Risk assessment
- Customer due diligence processes
- Checks to proscribed lists
- Comprehensive training
- Transaction monitoring process
- Reporting suspicious transactions
- Individual accountability

“Necessary and Sufficient”

- **Necessary – the systems and controls that must be in place:**

✓ systems & training to prevent money laundering

✓ customer identification and due diligence procedures

✓ record keeping procedures

✓ reporting procedures (including the identification of a Nominated Officer, normally the MLRO) both internal and external

- **What is sufficient? Indicators of sufficiency include:**

✓ number of SARs filed

✓ number of potential clients the firm has turned down

✓ ongoing commitment of resources (especially regular training)

✓ the position held by the MLRO (any premium paid?)

✓ risk assessment that is evidenced, informed and updated

External Fraud

- Affects all of us
- A particular problem in financial services, including threats from organised crime
- Cybercrime and threats to data security
- Specific fraud trends (e.g. mortgage fraud and investment fraud)
- People risk:
  - placement of criminal associates in banks
  - staff targeted by criminal gangs and threatened
  - bribery of cleaners, call centre-staff and others

ACFE Fraud Tree: Unique Factors

DESCRIPTORS	FRAUDULENT FINANCIAL STATEMENTS	ASSET MISAPPROPRIATION	CORRUPTION
Fraudster	Executive management	Employees	2 parties
Size of fraud	$1m - $258m	$93,000	$250,000
Frequency of fraud	6%	71%	23%
Motivation	Egocentric (stock prices, bonuses)	Pressure, dissatisfaction	Economic (business drivers)
Benefactors	Company & fraudster	Fraudster (over company)	Fraudster
Size of victim company	Large	Small	Depends
Materiality	Likely	Unlikely	Depends

Fraudulent Financial Statements

- Governance dimension - fraudulent financial statements erode investor confidence
- Aspects of accounts manipulation:

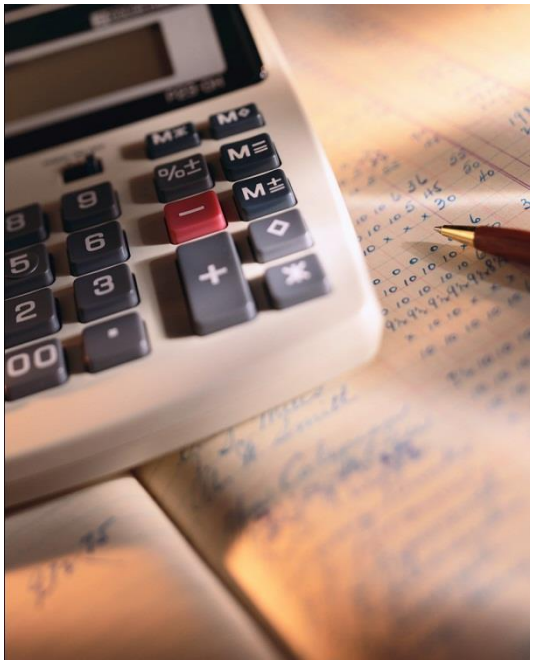
  - timing differences (improper treatment of sales)

  - fictitious revenues

  - concealed liabilities (improper recording of liabilities)

  - information omitted

  - improper asset valuation



Financial Statement Fraud – Example: The Satyam Case

- Fourth largest computer outsourcing company in India and listed on the Bombay, New York and Amsterdam exchanges
- 2009 letter from the Chairman, Mr Raju, confessing involvement in a massive and long running accounting fraud
- $1bn cash black hole
- Creation of 6,000 forged invoices
- Creation of 13,000 “ghost” employees
- Criminal charges against Mr Raju, six former executives, the ex-head of internal audit and the former external auditors
- Implications for Indian corporate governance

Asset Misappropriation Schemes

- “Misappropriation includes more than theft or embezzlement. It involves the misuse of any company asset for personal gain”.
- The most important component is fraudulent disbursements – schemes where a distribution of funds is made from an account in an apparently normal manner
- Four key groups:
  - billing schemes
  - payroll schemes
  - expense reimbursement schemes
  - cheque tampering schemes

Asset Misappropriation – Example: Jessica Harper

- Former head of online security and fraud at Lloyds Banking Group
- Submitted 93 bogus invoices (2007-2011) to pay herself £2.4m – spent on friends, family and landscaping her garden
- Fraud discovered by internal audit
- Paid £60k p.a.
- Told the police that she saw the opportunity and because she had been working 60 hours a week felt she "probably deserved it"
- Jailed for five years in September 2012

The Bribery Act 2010

- Act came into force 1 July 2011
- **Contains the new corporate offence of failing to prevent bribery**
- Has wide jurisdictional reach, including prosecution of non-UK persons for the corporate offence where they carry on a business (or parts of a business) in the UK
- **Six guiding principles for bribery prevention:**

✓ Proportionate procedures
✓ Top level commitment
✓ Risk assessment
✓ Due diligence
✓ Communication (including training)
✓ Monitoring and review

Adequate Procedures - Summary

- Tone at the top – clear top-level buy-in & responsibility
- An anti-bribery culture
- A statement of zero tolerance towards bribery
- Continuing bribery risk assessments
- On-going training programme
- Whistleblowing (“speak up”) mechanisms

Adequate Procedures - Summary

- Clear policies on bribery, gifts & hospitality, political donations, tendering etc.
- Monitoring & review
- Appropriate due diligence on agents and other third parties
- Anti-bribery clauses in contracts with counterparties
- Individual accountability

Responsibilities of Auditors re Fraud

- General perceptions – the expectation gap
- **External auditors:**

  - audits should be planned & performed to obtain reasonable assurance that financial statements are free from material misstatements
- **Internal auditors:**

  - should have sufficient knowledge to identify indicators of fraud but are not expected to have the expertise of a person whose prime responsibility is preventing & detecting fraud

Limitations of Traditional Audit Approach

- Fraud = motive + opportunity
- Audit focus is on opportunity but ignores motive
- Opportunity is addressed through internal controls but this is of limited value because of:

  - low awareness of fraud risks (often insufficient focus on control design)

  - audit testing of control effectiveness is based on samples (to provide “reasonable assurance”)

  - timing is pre-planned

  - controls can be over-ridden by management & circumvented by collusion

SAS 99 & ISA 240: Fraud in a Financial Statement Audit

- "In planning and performing the audit to reduce audit risk to an acceptably low level, the auditor should consider the risks of material misstatements in the financial statements due to fraud"
- Increased emphasis on fraud risk during the audit but no change in auditor's responsibilities
- **Key ideas:**

  - increased emphasis on professional scepticism
  - brainstorm how fraud could occur
  - discuss fraud risk with management
  - use tailored fraud detection measures where risk is high
  - recognise the risk of management override of controls

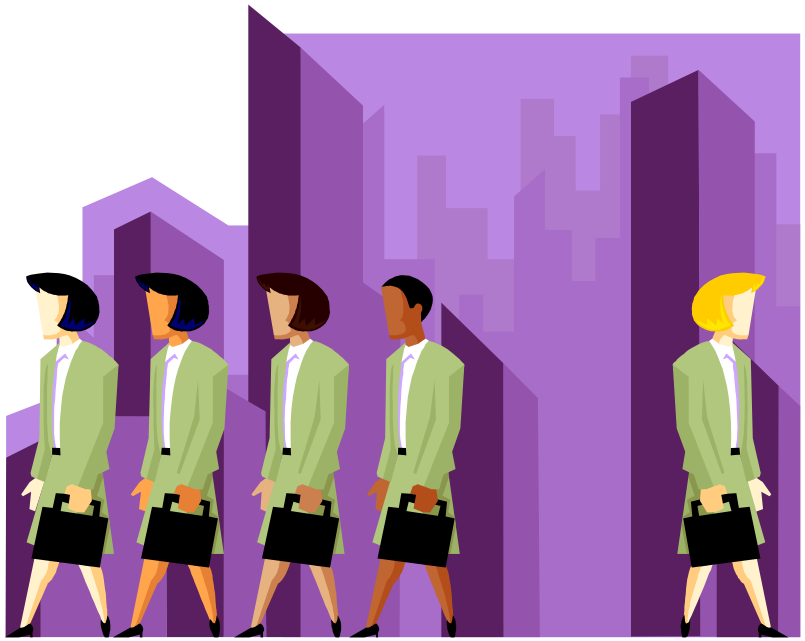
Behavioural Red Flags

- Does employee have:
  - past history of dishonesty?
  - known financial pressures?
  - obvious dissatisfaction?
  - changes in lifestyle or behaviour?
- Living beyond one's means is a key red flag
- Personal control issues:

✓ Antagonism - over-personalises business matters

✓ Unwilling to share duties

✓ Bullying attitude



Control Weaknesses

- In practice, fraud is enabled by key control weaknesses:

  - failure of the two-tier control test (the design not fit for purpose and/or the control not working in accordance with the design)

  - lack of management review

  - management override of existing controls

- Concealment strategies ("control inhibitors")

  - collusion

  - blocking the flow of information

  - processing transactions below the "control radar"

  - false documentation

Summary – Top 10 Anti-Fraud Controls

- **Prevention Controls**

✓ Management review
✓ Staff vetting (especially credit reference checks)
✓ Job rotation & mandatory holidays
✓ Awareness training (for both managers and employees)
✓ Anti-fraud policy

- **Detective Controls**

✓ Whistleblowing hotlines
✓ Surprise audits
✓ Data mining software
✓ Management review
✓ Audit (both external and internal)

Financial Crime Risk – Modern Themes

- Governance – a risk-based approach with senior management accountability
- Controls that are proportionate and appropriate to individual circumstances
- Control essentials:

✓ Policies & documentation

✓ Risk assessment

✓ Due diligence

✓ Training

- Critical dimension of ethics, culture and individual accountability

Effective Business Risk Management

- Modern risk “hot spots”
- Conduct risk and how to manage it
- Tone at the top and components of risk-aware culture
- Reporting and the governance dimension
- Risk Fitness Quiz
- Questions & answers
- Summary & conclusions

Aspects of Modern Risk Assessment (1)

- Risk governance dimension
- Importance of “Black Swan” events
- Focus on high impact events, especially, “hidden or under-estimated” risks. Examples:

✓ Supply chain and outsourcing

✓ Financial crime, especially bribery & corruption

✓ Cyber crime, IT failures

✓ Reputational damage (e.g. social media)

The “Black Swan” Problem

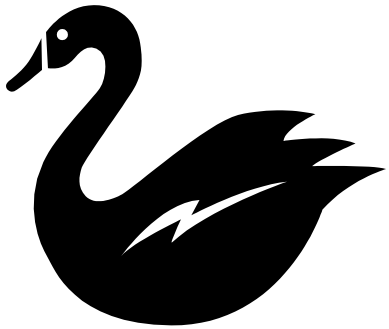
- **Characteristics of a “Black Swan” event:**

✓ Rarity
✓ extreme impact
✓ retrospective predictability

- **In reality, rare events are not as rare as one might think –** our overall understanding of “tail risk” in normal distribution curves is weak

- **Need for:**

✓ Reporting channels (whistle-blowing)
✓ Resiliency (understanding principal risks & contingency planning)
✓ Due diligence (an important part of good governance today)



Risk Hot-Spot: Crisis Management

- Pace and scale of modern media coverage
- Key area of judgement for senior executives
- Have a crisis management plan (responsibilities, scenario analysis, rehearse)
- Focus on communication, including social media
- Make use of PR agencies
- Engage with stakeholders
- Aim is to build assurance of resiliency

Aspects of Modern Risk Assessment (2)

- **Conduct risk** – FCA focus on outcomes and treating customers fairly
- **Four key components**:

✓ Incompetence – address via training

✓ Complacency, lack of engagement and simple negligence

✓ Counter productive workplace behaviours (including fraud and corruption)

✓ "Custom and practice" – behaviours, "perks" etc. all without reference in policies and procedures

Key Points on Conduct Risk

- Human factors (e.g. negligence or malign intent) are higher risk than process failures
- **Need a compliance framework**:
- ✓ **Oversight**
- ✓ **Internal controls and behaviour management** (codes, training, incentives, hotlines, discipline)
- ✓ **Risk and reporting** (including audit & accounting)
- ✓ **Managing third parties** (due diligence, M&A work)
- Need management oversight in SMEs

Risk Hot-Spot: Integrity Due Diligence

- Objective is to establish trust between counterparties (not only for AML purposes)
- Purpose is two-fold:
  - supplement legal & financial due diligence
  - provide an informed understanding of the human risk of entering into a new association
- Asks “difficult” questions:
  - has disclosure been complete & honest?
  - does the company behave in an ethical manner?
  - is the reputation of the company healthy?
  - are the individuals competent, honest & respected?
- Use external company

Risk Hot-Spot: Risk-Aware Culture

- **Culture** is defined as:

✓ the combined set of individual & corporate values, attitudes, competencies & behaviour that determine a company's commitment & style

✓ Tone set from the top is crucial - aim is to create a positive culture where behaviour is openly assessed, challenged, developed & rewarded

- **Risk culture** - the tone setting and ethical environment in place at all levels

✓ "So today we are moving back to the future in a sense – with the regulatory system placing far more emphasis on good judgement and less on narrow compliance with a set of rules. Hopefully to a culture where the 'ethic of care' – doing what is right takes precedence over the 'ethic of obedience' – doing what is allowed". (Martin Wheatley FCA October 2013)

Risk-Aware Culture: Bi-Polar Review

- Proactive
- Accountable
- Informed judgement
- Sceptical
- Transparency
- Add value
- Optimise
- Enabler
- Bottom-up
- Balanced, well thought out risk taking

- Reactive
- “Blame”
- Checklist mentality
- Naive
- Silos
- Bureaucratic process
- Minimise
- Roadblock
- Top down
- “CYA”

Integrity and Trust

- **Integrity – it matters!**

✓ Character & principles, especially respect for the law & honesty

✓ Consistent, fair and dependable, not deceptive

✓ Take responsibility for actions

✓ Integrity makes a leader believable and worthy of our trust

- **Trust – the business x-factor**

✓ Definition: "a judgment of confident reliance in either a person or an organisation" (Institute of Business Ethics)

✓ Trust model – we judge the other party's trustworthiness along three dimensions:

❑ Their ability (technical competence);

❑ Their benevolence (motives and interests); and

❑ Their integrity (honesty and fair treatment)

Ethical Leadership – Three Components

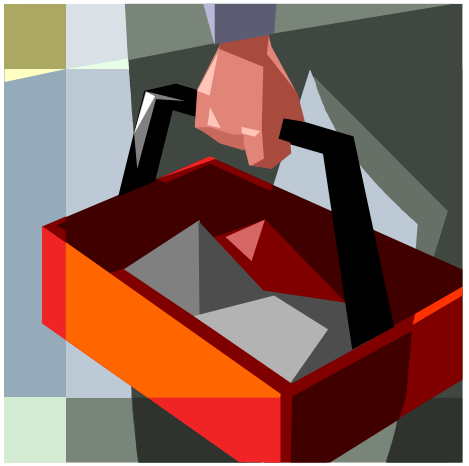
- The ethical person – live with integrity, lead by example
- The ethical manager – making ethical judgements consistently, in good times and bad
- The ethical toolbox – the policies, controls and awareness to give assurance of good business ethics in your business

The Ethical Manager - Tone at the Top

- Honesty can best be reinforced when a proper example is set
- Treat everyone equally
- Don’t set unachievable goals
- Communicate a zero tolerance of unethical behaviour
- Be consistent in judgements and decisions

Corporate Responsibility: The 21st Century "Ethical Toolbox"

- Ethics codes & charters
- Policies, procedures & internal controls
- Whistle-blowing hotlines
- Training & development programmes in business ethics
- Monitoring process



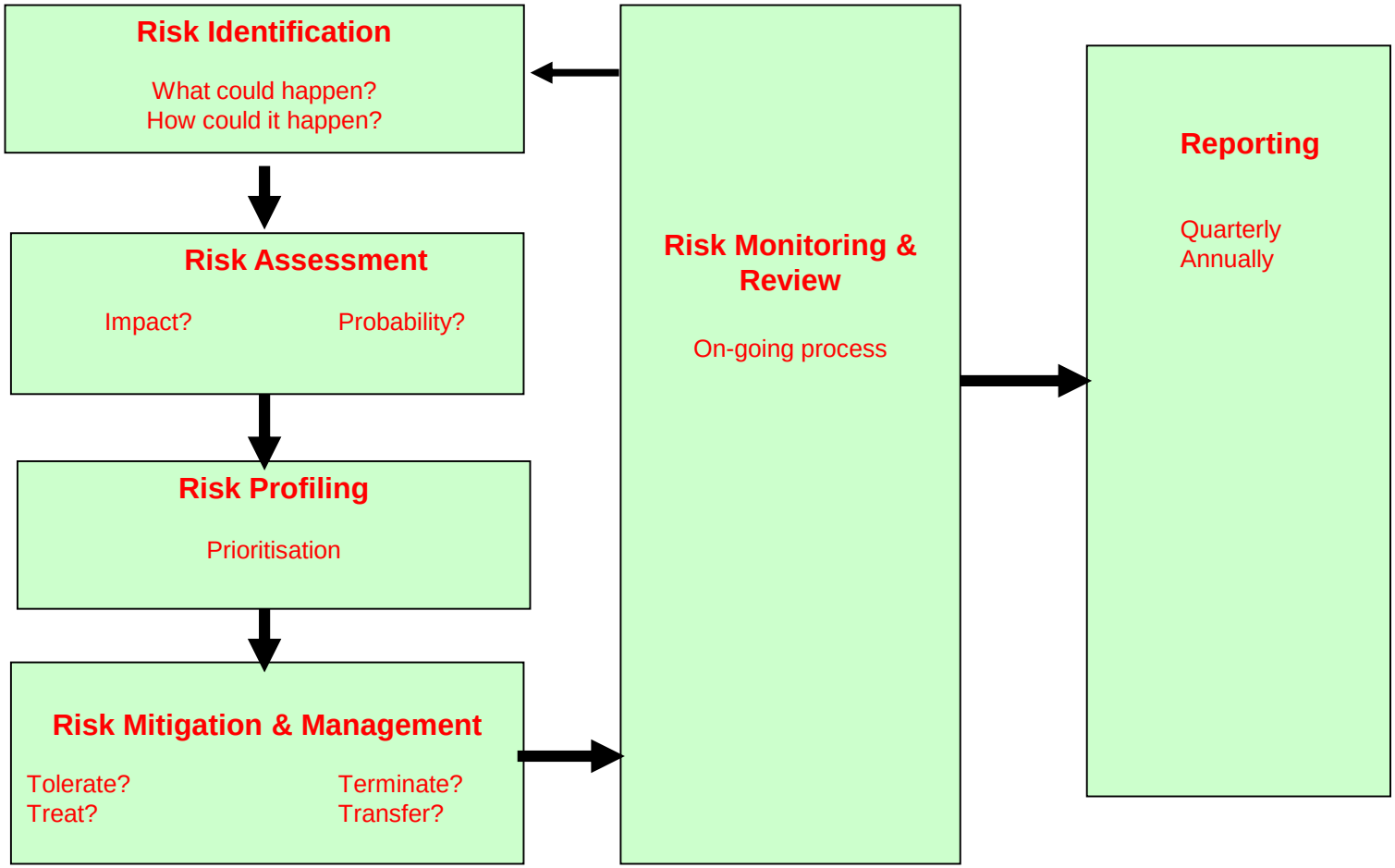
The Governance Dimension & Reporting

- Senior management oversight of the risk process is crucial
- Periodically, obtain direct input from all of the top team on strategic risks
- Define and communicate risk appetite
- Allocate sufficient agenda time for risk
- The importance of risk reporting

Key Points on Governance & Reporting

- Getting the right level of involvement at the top is crucial – discussion, challenge, training
- “If you never disagree you are irrelevant”
- Know where the red lines are
- Strategy and risk go hand in hand
- Do not allow risk reporting to become “routine and by rote”
- Beware of information asymmetry on risk matters

The Modern Risk Management Process



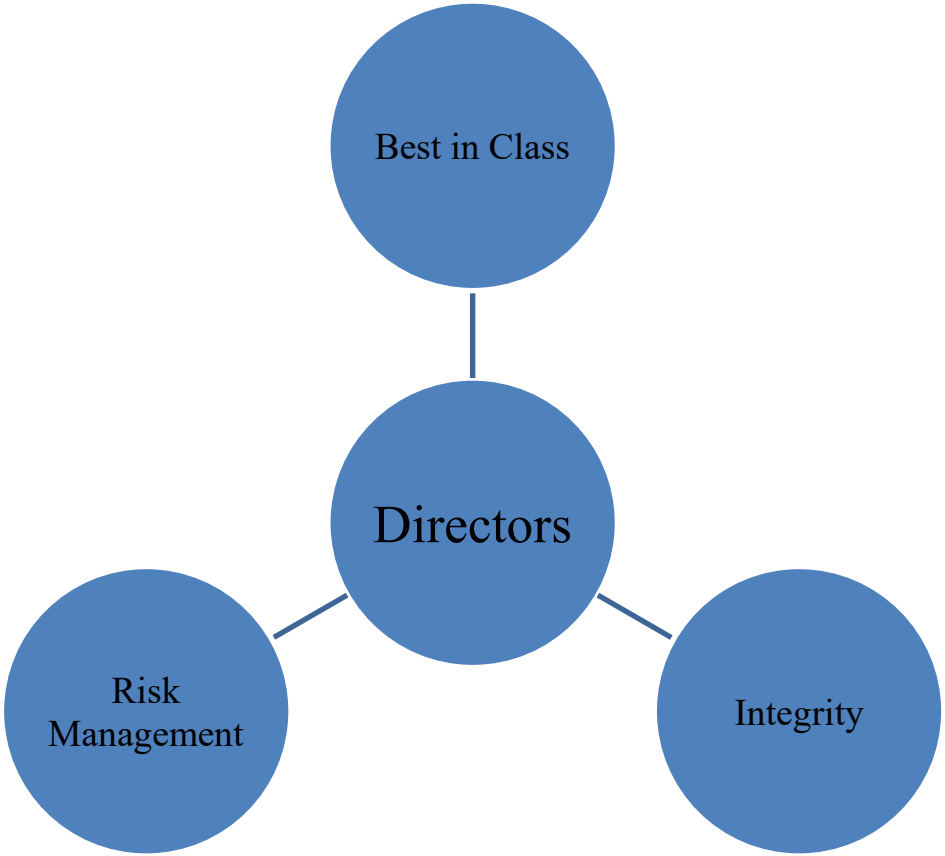
Benefits of an Effective Risk Management Process

- Improved decision making increases chances of achieving objectives, so adding value
- Constrain threats to acceptable levels
- Take informed decisions about exploiting opportunities
- Increased understanding and ownership of risk
- Fewer surprises – issues highlighted quicker
- Provides consistency, visibility & evidence of decisions taken
- Increased confidence for stakeholders in the organisation's corporate governance & ability to deliver

Summary – Risk Management Essentials

- Board involvement & oversight
- Tools – risk registers are used by many organisations today
- Awareness training programme – essential for a risk-aware culture
- Include risk management as part of managers' objectives and in the reward system
- Effective controls & risk mitigation, especially insurance strategy
- Independent monitoring and review
- Effective communication and reporting

Best in Class Overview



Final Thoughts on Risk Management

- Is proactive not reactive
- The objective is not to minimise risk but to optimise it
- Involves probabilities not certainties
- Requires the use of judgement to operate effectively
- Each firm is unique so will have a unique risk profile

Thank You!

- It has been a pleasure meeting you
- Thank you for your attention & participation
- Good luck in the future