# Project Controls Expo
## 09/10 Nov London 2011

Enterprise Risk Management (ERM).

# Speaker Profile

- Michael Higgins, born in 1979, 1 wife to be, 4 children, 1 dog and a people carrier.
- BAE Systems 1996 – 2004
- BMT Sigma 2004 – 2007
- Thales 2007 – 2009
- Eurocopter 2009 – 2011
- Xacom Ltd 2011 – not too sure yet

# Introduction

- What is ERM?
- NAO – Good Practice Report
- What does ERM look like?
- Implementing ERM
  - Organisation
  - Process
  - Toolset

# What is ERM?

- Enterprise risk management (ERM) in business includes the methods and processes used by organisations to managed risks and seize opportunities related to the achievement of their objectives.

- ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal control, Sarbanes-Oxley Act and strategic planning.

Source: http://en.wikipedia.org/wiki/Enterprise_risk_management

# NAO Managing Risks Good Practice Report

- NAO published a report regarding Risk Management in government in June 2011, it focused on six principles:
  - Principle 1 – An engaged board focuses the business on managing the things that matter
  - Principle 2 – The response to risk is most proportionate when the tolerance of risk is clearly defined and articulated
  - Principle 3 – Risk Management is most effective when ownership of and accountability for risk is clear
  - Principle 4 – Effective decision-making is underpinned by good quality information
  - Principle 5 – Decision making is informed by a considered and rigorous evaluation and costing of risk
  - Principle 6 – Future outcomes are improved by implementing lessons learnt

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# Findings from the report

- **Principle 1 – An engaged board focuses the business on managing the things that matter**
  - **Leadership and ownership of risk management is inconsistent**
  - **Discussions do not always focus on those significant issues that could pose the biggest risk**
  - **There is more for boards to do to visibly communicate their commitment to and understanding of risk management, build a climate of trust and embed risk management in their organisations.**

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# Findings from the report

- **Principle 2 – The response to risk is most proportionate when the tolerance of risk is clearly defined and articulated**
  - **Risk tolerance is too difficult to define due to the size and diversity of an organisations operations**
  -

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# Findings from the report

- **Principle 3 – Risk Management is most effective when ownership of and accountability for risk is clear**
  - **Lack of clarity over ownership of, and accountability for risks**
  - **Lack of risk escalation processes**

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# Findings from the report

- **Principle 4 – Effective decision-making is underpinned by good quality information**
  - **Risk information reported to the board is not fully integrated with performance and financial information**
  - **Discussions are focused on the content of the Risk register rather than the actions required to mitigate the key risks**

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# Findings from the report

- **Principle 5 – Decision making is informed by a considered and rigorous evaluation and costing of risk**
  - **Little costing of risks and mitigations**
  - **Costing of risk is deemed too difficult or not practical given the nature of business operations**

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# Findings from the report

- **Principle 6 – Future outcomes are improved by implementing lessons learnt**
  - **Lessons learnt not used actively as part of a drive towards continuous improvement**
  - **Internal audit functions often repeat findings within their audit reports.**

Source: http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government

# What does ERM look like?

Project Controls EXPO

# Implementing ERM

- Set the Vision for ERM
  - Provide a consistent Risk picture across an organisation, from risk owners to executives
  - Develop risk management practices up to becoming a key driver in decision making
- Set the Objectives for ERM
  - Get the awareness, from operations to XMT, of the risks and opportunities with regards to the business objectives
  - Control and monitor, at each level, risks to take, risks to mitigate or hedge and risks to report or escalate
  - Be compliant with corporate policy and governance

# Organisation

- For ERM to be effective in an organisation it's key to have an organisation that can both support the transition and running of ERM.
  - Top level Executive sponsorship from the CEO
  - Dedicated RMO reporting to the CEO
  - Dedicated ERM leads responsible for Divisions or departments
  - ERM function/sub-function of the PMO
    - Toolset experts
    - Process experts
    - Trainers
  - Risk Managers, owners and wider stakeholders

# Process

- It's essential that policy is set at the highest level in the organisation on flowed down to all stakeholders
- Processes need to be defined and communicated
- Specific toolset processes need to be generated
- Processes should be tailored and adapted for key ERM roles and responsibilities

# Toolset

- Integration of the appropriate software
- Where appropriate a company wide roll out of a fully integrated ERM software package
- Access levels defined and set in line with ERM roles and responsibilities
- Customisation of reporting
- Sandbox area for development and training purposes before production cut-over

# Index


- http://web.nao.org.uk/search/search.aspx?Schema=&terms=managing+risks+in+government
- Cannon, Tom, A Guide to Integrated Risk Management, (London: AIRMIC, 1999)
- Doherty, Neil A., Integrated Risk Management: Techniques and strategies for Managing Corporate Risk, (McGraw Hill, 2000)