Convergence of BCM and Information Security at Direct Energy

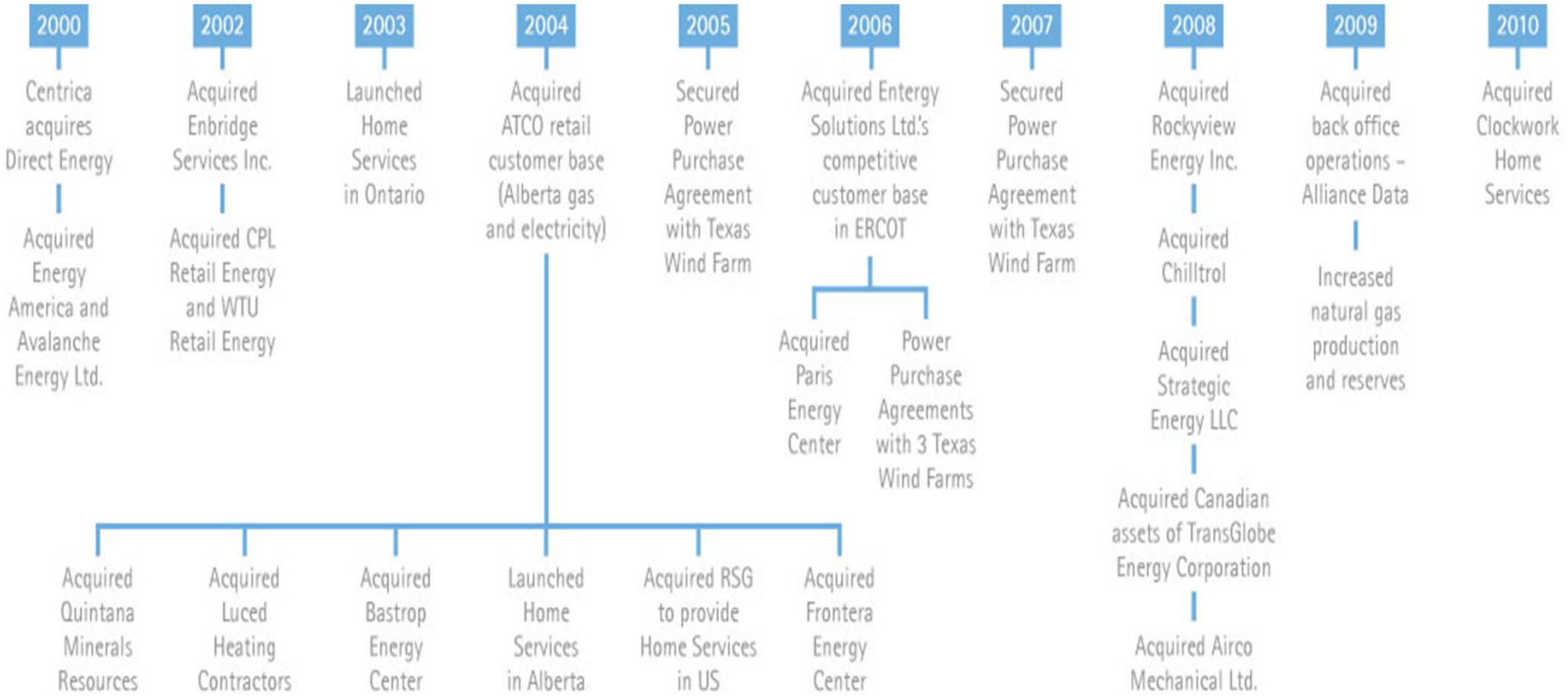
Karen Kemp
Direct Energy

Session ID: GRC-403
Session Classification: Advanced

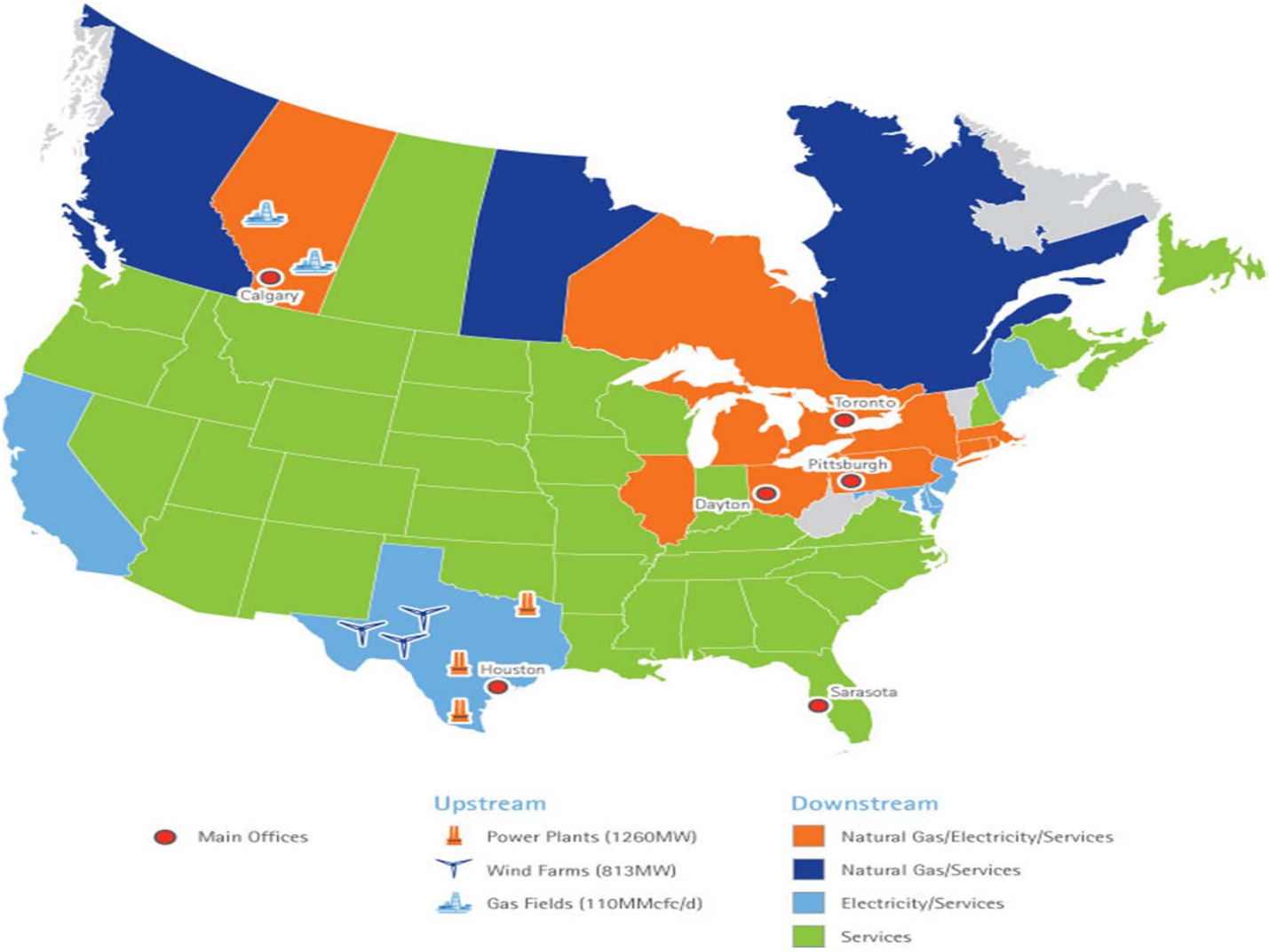
About Direct Energy

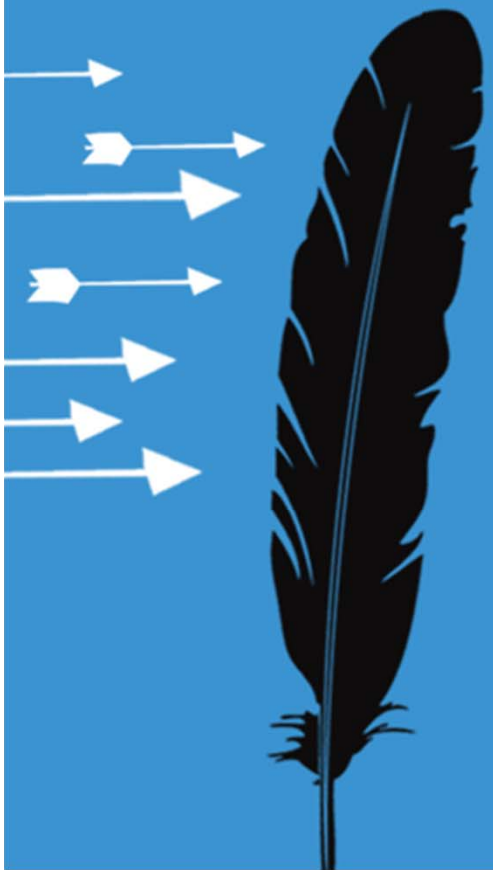
- Direct Energy was acquired by Centrica Plc in 2000
- In ten years Direct Energy has grown into a large multinational organization
  - over 6 million customer relationships
  - more than 70 facilities across North America
  - over 6000 employees
- Winner of the 2008 Disaster Recovery Institute Canada (DRIC) Award of Excellence in 2008 for large organizations in Business Continuity Management

A History of Growth



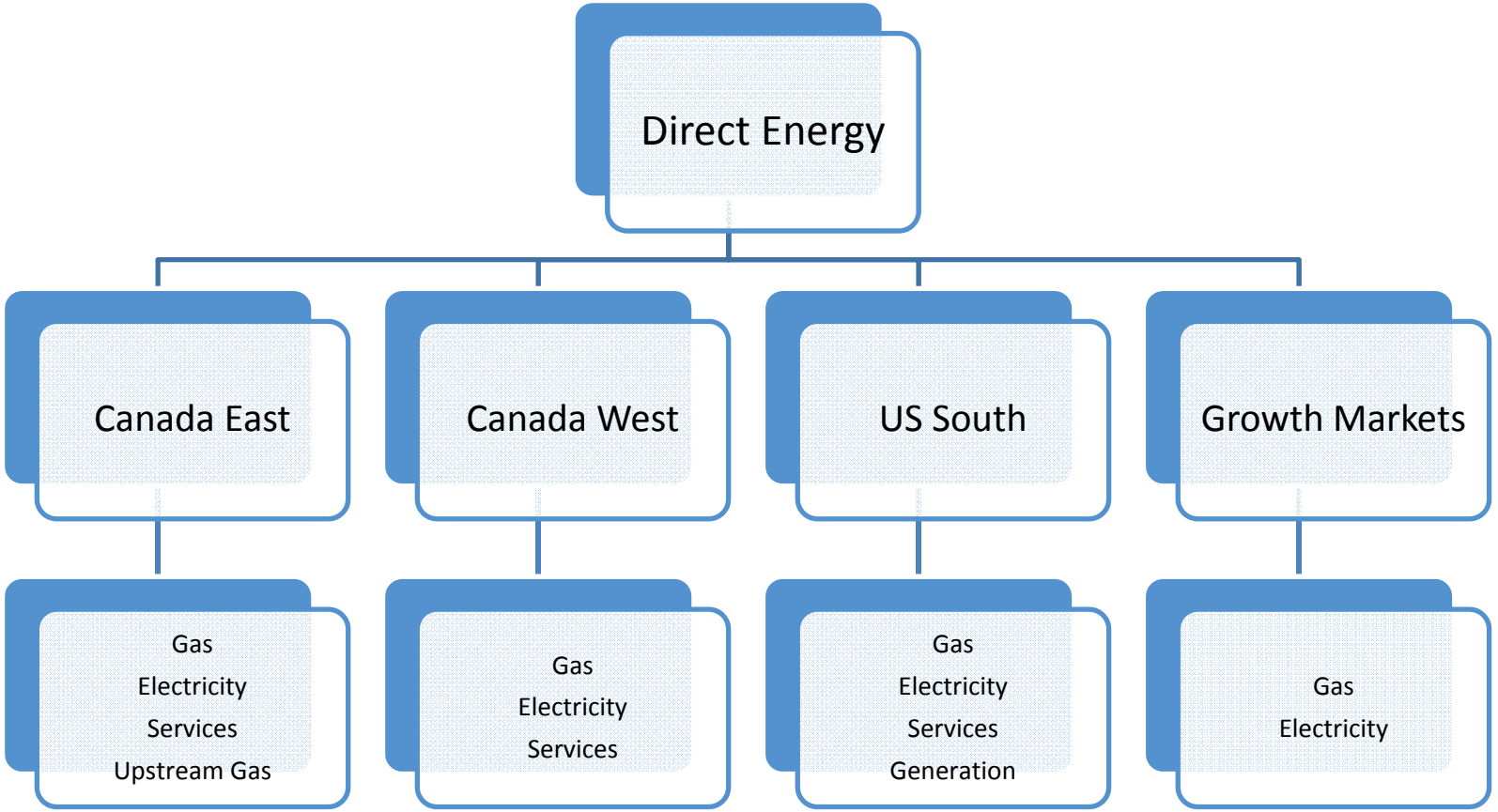
Marketplace



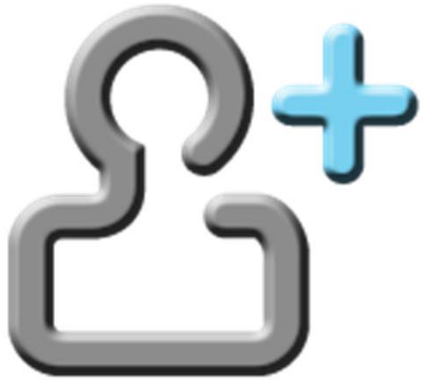


Early Days

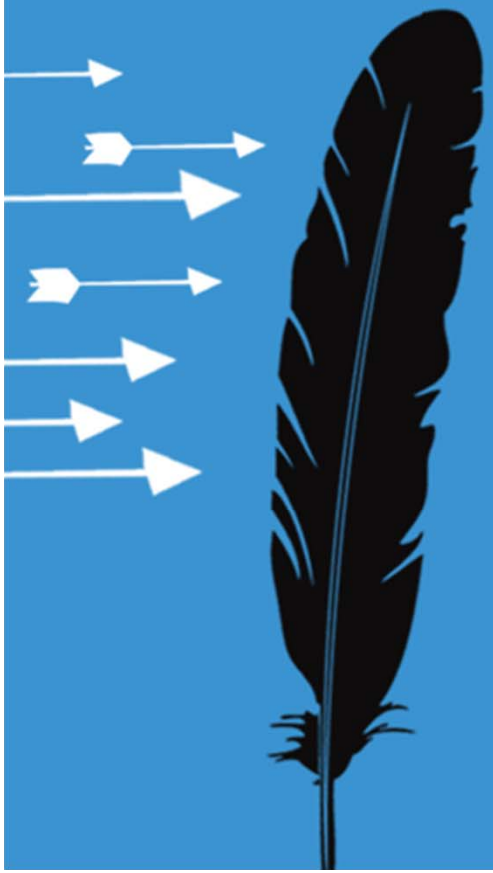
Early Business Model



Lets add BCM!



- 2002 IBM Commissioned to conduct a Business Impact Analysis
- 2003 Permanent BCM position added
- 2003 BCM Policy issued
- Q3 2003 – Q1 2004 Business Impact Analysis activities in earnest across North America
- Mandate to achieve was directly linked to the CEO's performance objectives

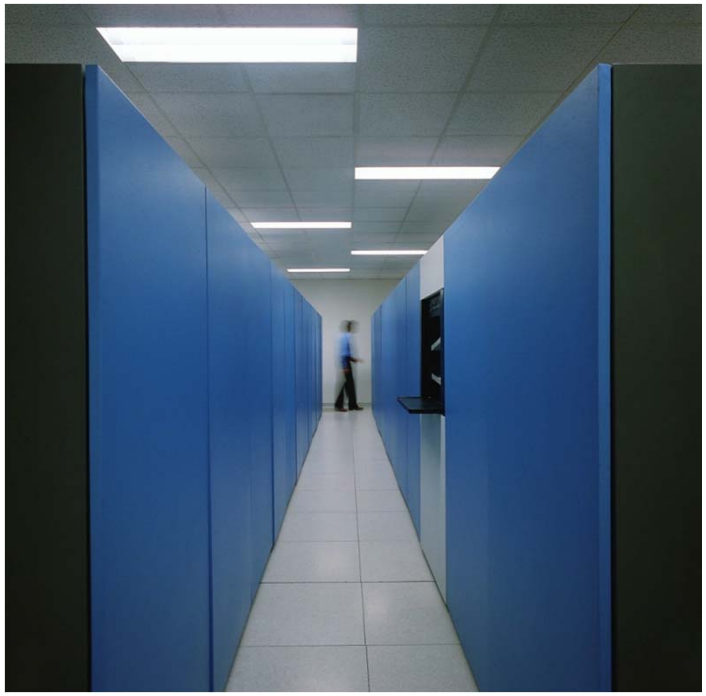


Implementation of BCM

BCM Matures in DE..

- Cultural Integration was critical to BCM Success
- The execution of the Business Continuity Program supports DE's brand promise to be a resilient and responsible service provider
- The program was well started and achieving success as evident in the 2005 Platinum Award for the execution of plans during Hurricane Rita in Texas

Data Centre Recovery



- Risk = Single Data Centre
- Risk factors: Atria III
  - Located along two of the busiest highways in Canada
  - Located on the glide path of Pearson and Buttonville Airports
  - Close proximity to major rail lines
- Largest single risk to the company

Recovery Data Centre Design

- Dual data centre design
- Split processing to minimize impact of any potential event
- Loss limited due to distributed nature of applications and hardware
- Resilience in power sources (two separate grids)
- Fit for purpose site ‘building in a building’ design

Networking Resilience

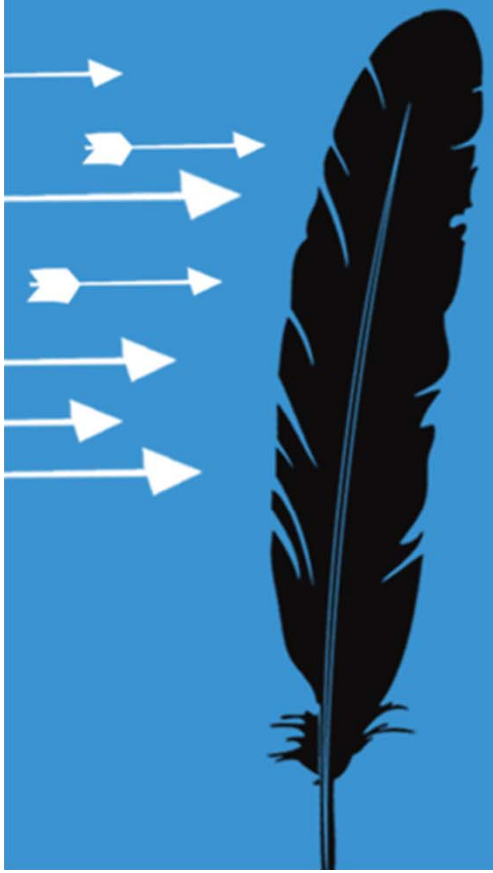
- The team implemented an advanced high capacity, self healing communications network connecting our data centers and key business locations.
- This ring network significantly increased network redundancy

Fibre Ring Approach

- Removed single points of failure throughout the GTA, and provide enhanced redundancy for many others:
  - 7 critical buildings throughout the GTA
  - 1x wireless network (circa 2005)
  - MPLS connections to Stamford, Houston and Calgary
- The network was implemented at less than the cost of a traditional point-to-point network and can carry 100 times the capacity.

Data Centre Recovery
Completed December '05

- The project took over two years to complete
- The BCM team maintained close contact with all lines of business, third parties and the internal IT team
- Another outstanding achievement of this program is the cost of operation. This innovative and robust solution was designed so well that additional IS staffing levels are not required
- Mitigation of value at risk is never easily stated but conservative estimates place risk avoidance values in multimillion dollar range



Things Change

2005 Re-organization

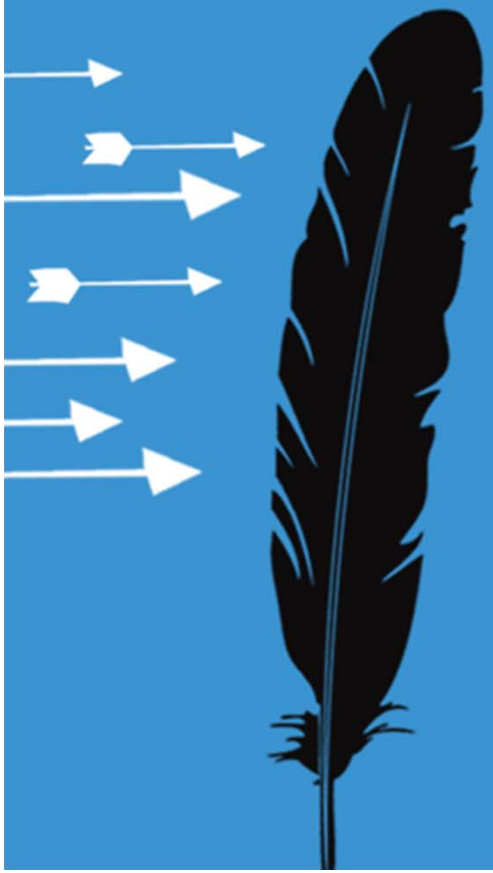
- Central Operations is outsourced
- BCM function moved to IS
- New CIO hired in March 2005
- New CIO reports to the CEO and is a member of the top team
- Promoted to IS Leadership
- Functional addition:
  - IS Audit Liaison, Controls and Compliance

The beginning of convergence…

- The addition of the Information Security governance role prompted shift in thinking within the team
- What is our current level of security?
- An additional FTE was required

Complex Operating Landscape

- Multiple regulators
- Multiple legal jurisdictions
- Multiple market operators
- Multiple states and privacy/records regulations
- Multiple industry regulations (i.e. PCI)



Adding Controls

Integrated Control Framework

- Revision and reissue of the Information Security Policy from 124 pages down to 33 (2006)
- The framework is the glue that connects the team

Foundation for the Framework

- COBIT was selected as the blueprint or the Information Technology General Controls (ITGC) and the connection to the COSO financial framework

- ISO 27001 (formerly 17799) was selected to cover technical and application controls

- Once the base was established other regulations and/or standards such as PCI, NERC Cyber Infrastructure Protection Standards were mapped to the framework

Send in the consultants!

- An independent review of the control framework was commissioned
- A CobiT assessment and documentation project was executed by PWC

ICF Project Execution

- The project consisted of the following activities:
  - Selection of key IT processes and control objectives.
  - A high level understanding of the control activities with process owners.
  - An overall maturity assessment for each IT process based on the control objectives selected.
  - Identification of gaps that require remediation.
  - Review and agree assessment results

ICF Project Scope

- The CobiT framework identifies 34 processes and 318 control objectives for measuring the effectiveness of IT management
- 23 of 34 processes were selected as applicable and high priority
- The directors and staff from Infrastructure Services, Operation Services, Corporate Systems, Operations Risk and Business Management were interviewed to evaluate the design effectiveness of the IT processes and key control activities

ICF Objectives

Plan and Organize

Define a Strategic Plan
Define the IT Processes, Organization and Relationships
Manage the IT Investment
Communicate Management Aims and Direction
Assess and Manage IT Risks

Acquire and Implement

Acquire and Maintain Application Software
Acquire and Maintain Technology Infrastructure
Manage Change
Install and Accredit Solutions and Changes

Cobit Control

Deliver and Support

Define and Manage Service Levels
Manage Third-Party Service

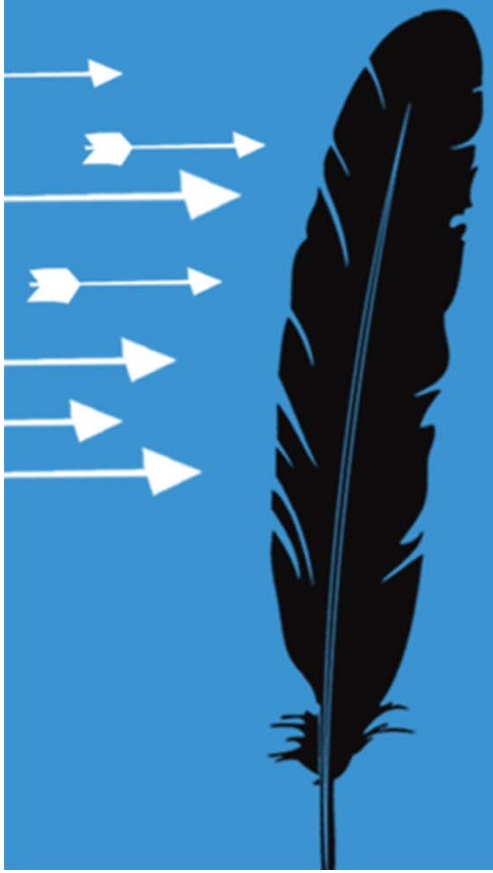
Ensure Continuous Service
Ensure Systems Security
Educate and Train Users
Manage Service Desk and Incidents
Manage the Configuration
Manage Problems
Manage Data (Back and Recovery)
Manage the Physical Environment
Manage Operations

Monitor and Evaluate

Monitor and Evaluate IT Performance
Monitor and Evaluate Internal Control
Provide IT Governance

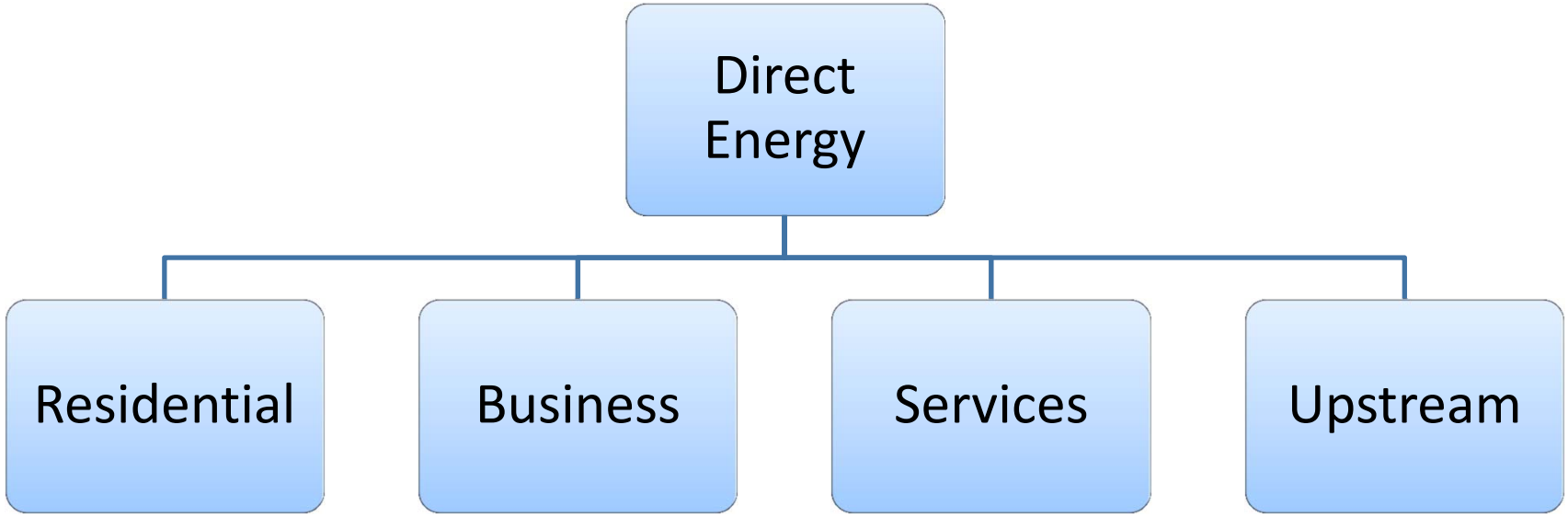
Improved Understanding

- Work on the control framework was underway
  - Processes were documented and recorded with owners in the framework
- Engagement in the change management process (5 methods for 4 LOB and Core IS)
- Change was required to support the re-organization from the Information Security perspective



Things Change Again…

2007 Reorganization



Information Security within IS

- It appears that fragments of the governance and/or assurance for Information Security within projects is placed within the project delivery teams in IS Core

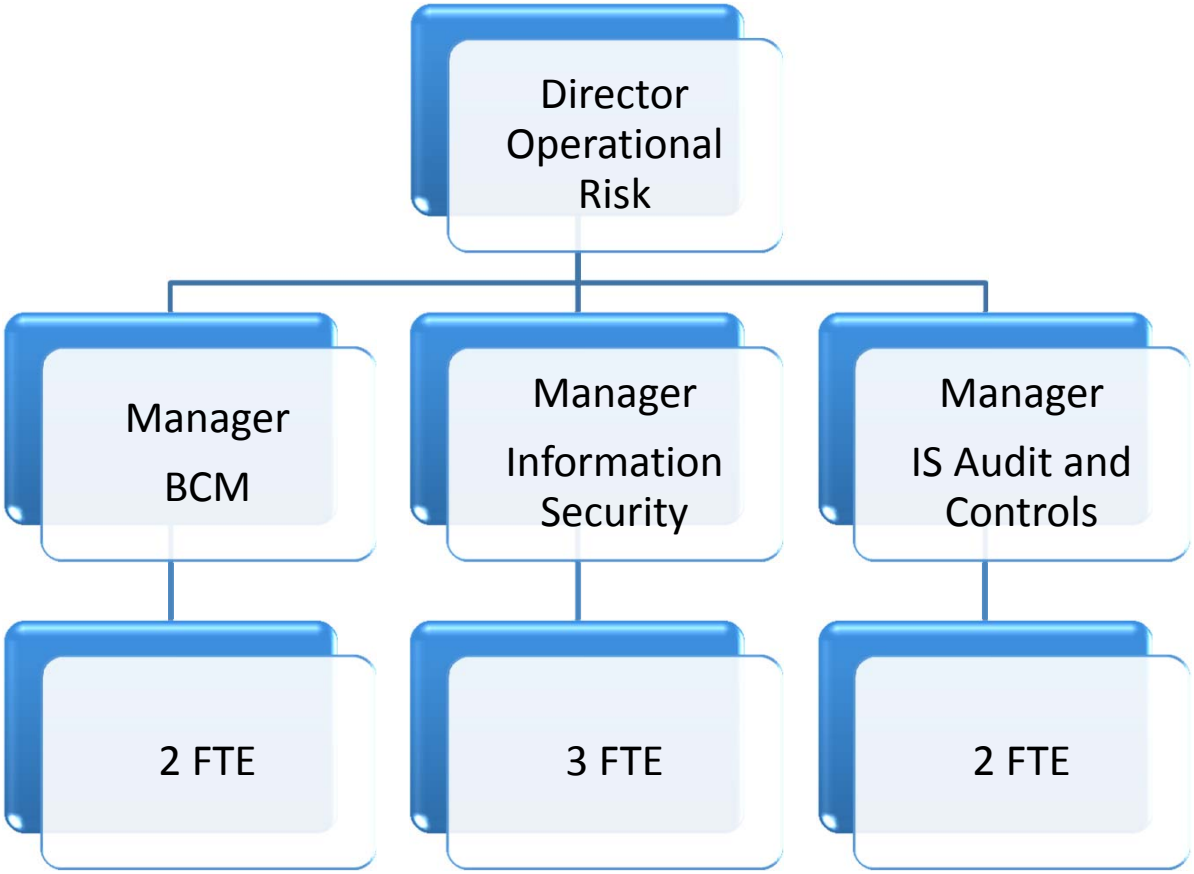
- The enterprise re-organization was the opportunity to make important changes and functional alignments

Areas for Improvement

- Synergies were obvious in the following areas:
  - Placement of the Information Security function
  - Change management process
  - Automation of the integrated controls framework

- These areas required the participation of each team in order to ensure that we had the proper alignment across all functions

Operational Risk 2007/08

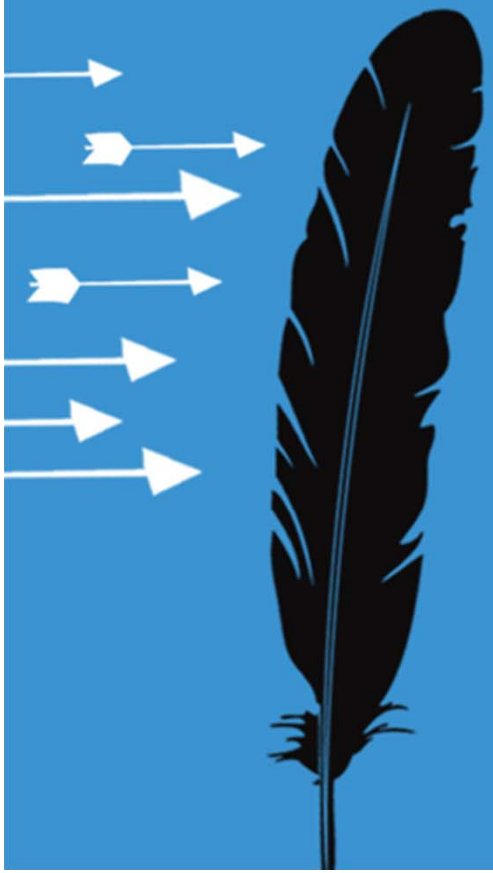


Change… so many projects, so few resources

- Given the size of the team it was not possible to gain full engagement in the change process
- What was needed was a tool to prioritize the work using a risk based approach
- The team began work on the ORD Engagement model

Team Requirements

- BCM ensures updated BIAs, strategies and finally plans accommodate ongoing change
- Information Security ensures that the security levels for the project are consistent with our policies and other obligations (up front)
- In some, but not all, cases the Audit and Controls group would be required to conduct audits for project assurance



How to automate?

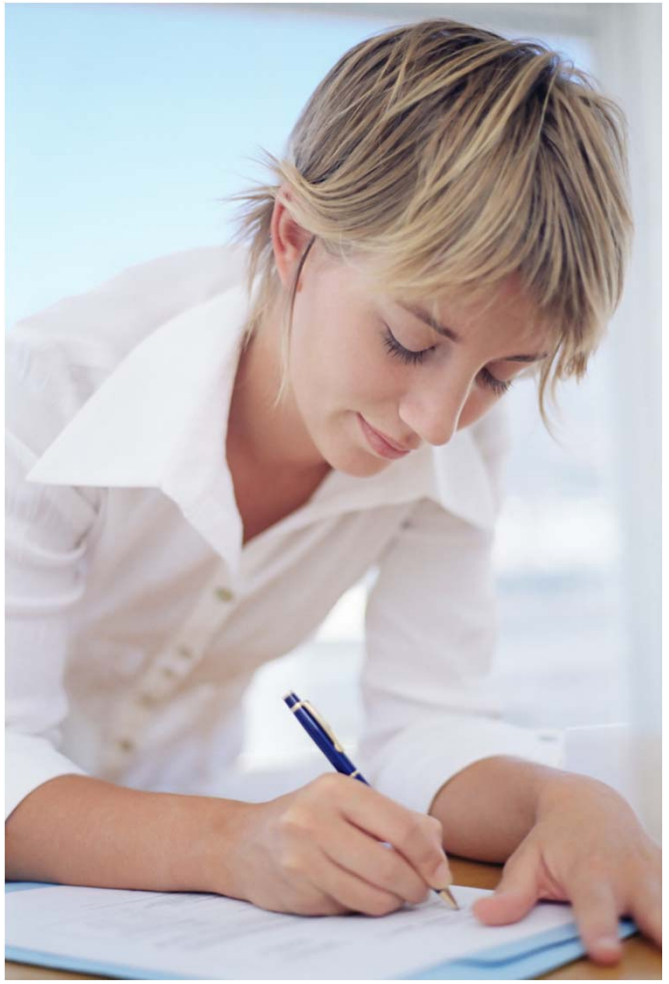
Tool requirements

- The involvement of all players within Direct Energy
- Defined a framework and process whereby Operational Risk Department can engage with Business Units, Core IS
- The ability to facilitate the implementation and monitoring of information risk processes

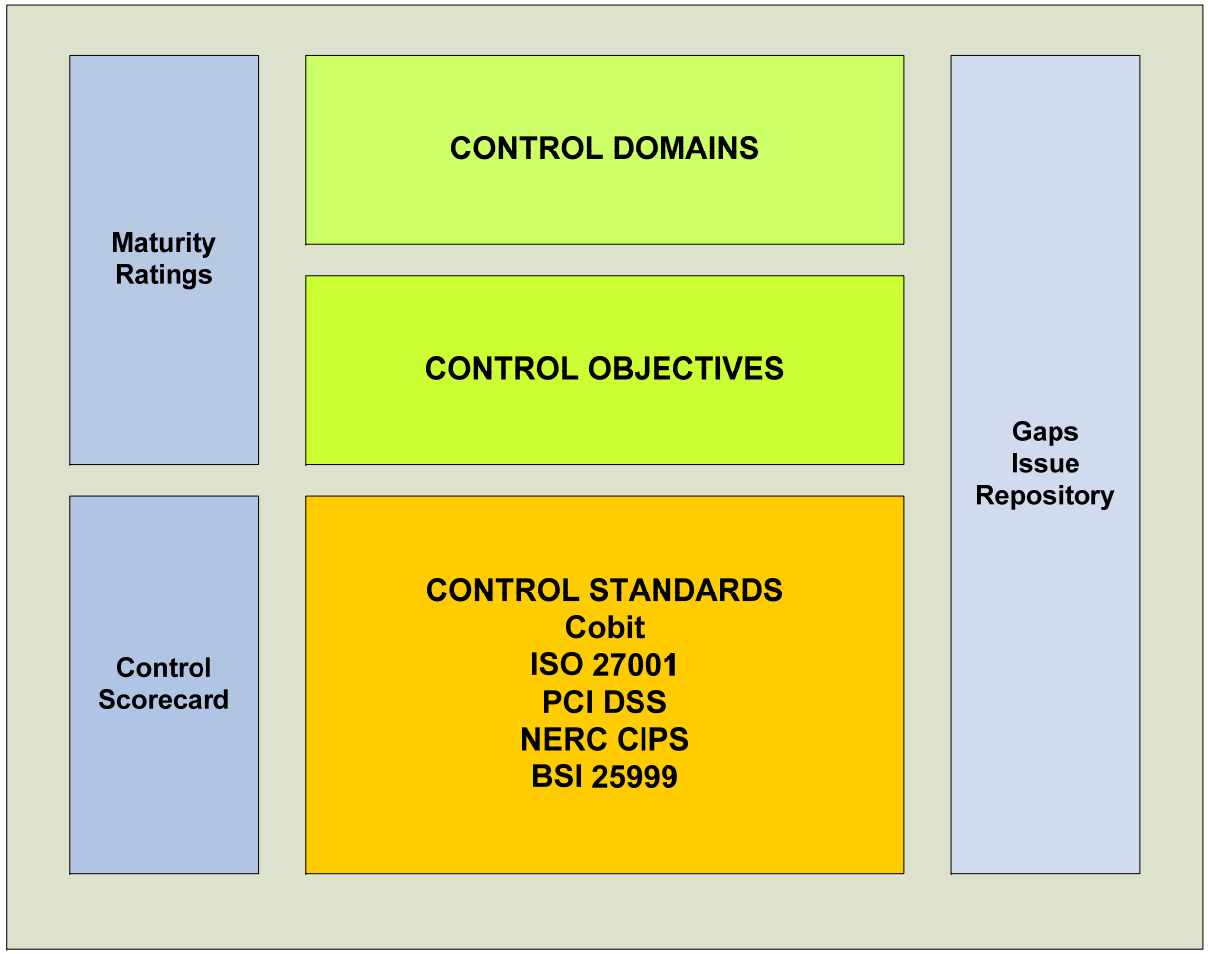
ICF Automation

- The control framework is built in Sharepoint largely by Operational Risk staff

- Small investments for internal development have enabled the team to extend and leverage the ICF across IS and enterprise to support and enable the financial RICF program

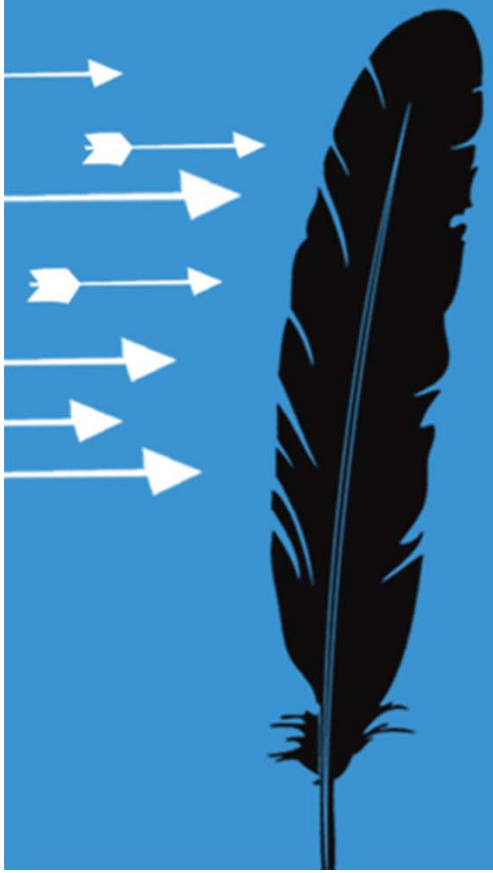


ICF Structure



Cost savings…

- The team is able to leverage the ICF for:
  - Automation of administrative functions such as email reminders for outstanding gaps
  - Single repository for the IS control environment information including:
    - Process details
    - Design details
    - Testing details



Conclusion

Staff Synergies

- Mergers and acquisition work can encompass both disciplines
- Third party audits can encompass both disciplines
- Change management oversight and insights shared amongst the teams
- Incident management teams can have cross trained members and leaders

The experiment continues..

- Active career management with formal cross training requirements
- We have added a controls speciality to our team which will add BCM to a traditionally Information Security function
- More interaction with other risk disciplines (i.e. Internal Audit, RICF)
- Development of Enterprise Risk Management Capabilities

What can you do?

- Investigate the use of internal applications to support development of control frameworks rather than niche tools
- Stop talking about differences and try to seek synergies to provide more value to the business
- Actively manage risk/security/bcm staff. This creates more opportunities and cross functional employees to increase the resilience of your limited resources