




ISO17799 project at

BMO  **Financial Group**

Presentation to ISO 17799 User Group 30 January 2004

Marc Stefaniu, P.Eng., MBA, CISSP
marc.stefaniu@bmo.com

BMO  Financial Group

Contents

- Purpose – share experience
- IS Functions at BMO – Mandate and Organization
- Scope of proposed project - IS Operations
- Benefits
- Project road map
- Gap analysis findings
- Preliminary lessons learned
- Next steps

Technology and Solutions ~ WWREI ~ Information Security 2

Purpose of this Presentation

Share BMO's experience on the road to adopting ISO17799 Standard.



Information Security function at BMO

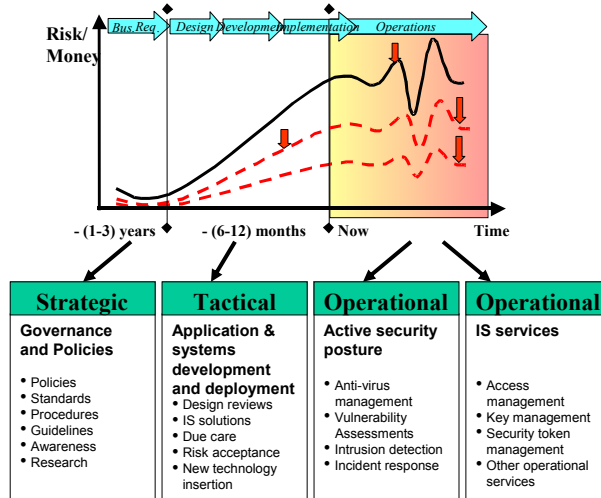
Mandate Lead the Enterprise in understanding and managing the information security risks associated with information technology.

Provide expert direction, planning and consultation on information security best practices and integrated processes, and ongoing active information security leadership and management expertise, to BMO Financial Group

Scope Bank of Montreal
Nesbitt Burns
Harris Bank (Chicago)
Overseas offices

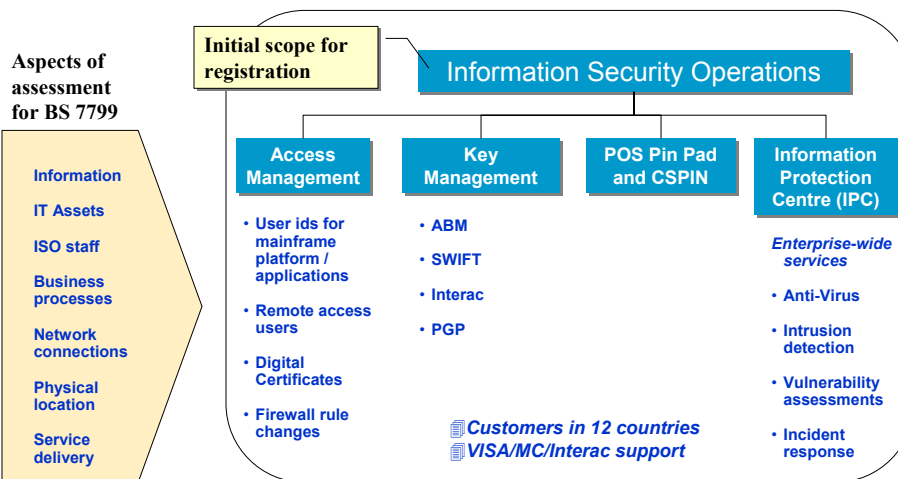
People Five PhDs
One ISMS Lead Auditor on staff
35% of the staff have one or two University degrees
30% of staff have college diplomas
58% of the staff have CISSP, SANS GSEC and other professional certification

Information Security function at BMO



Organization chart is aligned with security service delivery based on this Lifecycle model

Scope of proposed ISO17799 project

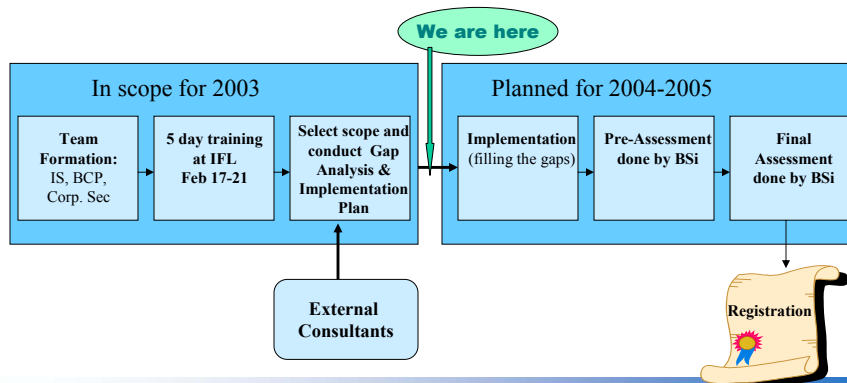


Benefits

- ☐ Provides confidence to trading partners, stakeholders, and customers.
- ☐ Certification demonstrates 'due diligence' by T&S and LOB leaders for risk management.
- ☐ Demonstrates compliance and/or directional alignment with mandates and laws (e.g., HIPAA, Gramm-Leach-Bliley Act of 1999, Privacy Act of 1974, Computer Security Act of 1987, Government Information Security Reform Act of 2001, Basel Accord, OECD principles, ISO9001, etc.)
- ☐ Alignment of language and objectives among departments that handle security functions
- ☐ Sets standard of excellence in dealing with third party connections, IT service providers, or future M&A activities.
- ☐ Provides independent review by third party of BMO's Information Security Management System.
- ☐ Reduces liability risk due to un-implemented or not-enforced policies and procedures related to security.
- ☐ Offers opportunity for staff development and focused staff responsibilities.

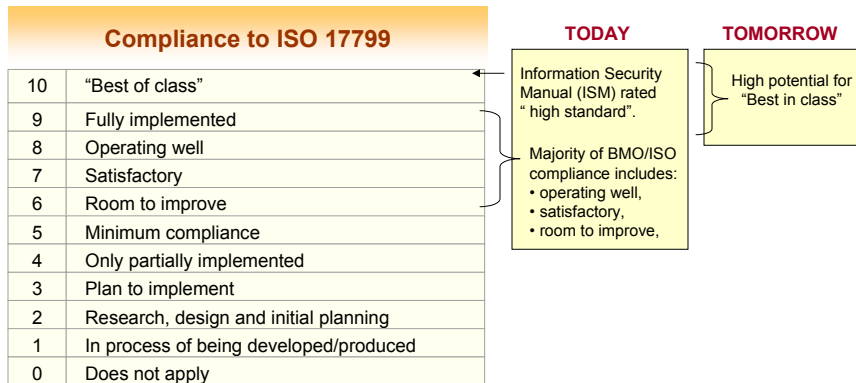
Project road map

- Feb 2003 → Set up core team with focus on obtaining registration for all Information Security department and Operational Risk group
- Mar 2003 → Training on ISO 17799. 16 participants. Session leader: Chris Ferrant - lead auditor for British Standard Institute (BSi).
- May 2003 → Gap Analysis with focus on IS Operations.



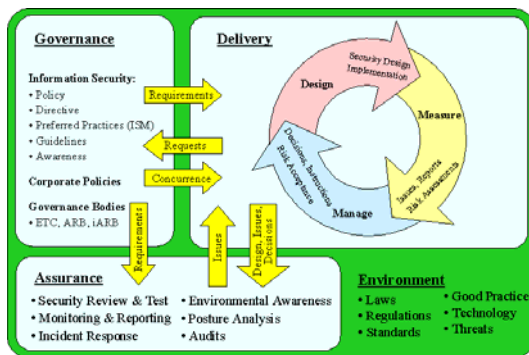
Gap Analysis Findings

- Motivated, competent and responsive team.
- Comprehensive suite of documents
- Strong synergy with 17799 Standard
- Wide range of security controls.
- A sense of information security mindfulness prevails
-But there is room for improvement

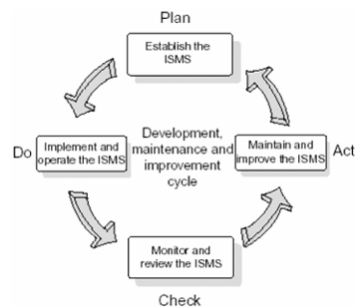


Gap Analysis Findings: *Strong Synergy with BMO's Master Security Process*

BMO Information Security Master Process

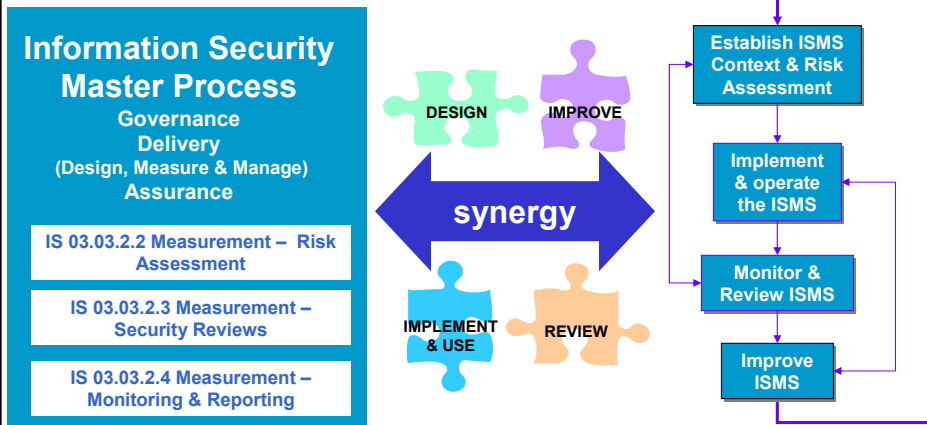


BS 7799 - PDCA Model applied to ISMS processes



Gap Analysis Findings: *Strong Synergy with BMO's IS Manual*

BS 7799 Part 2 ISMS processes



Gap Analysis Findings

Control Compliance

Alignment (I.e. mapping and re-wording) needed between BMO Policies, Procedures, Standards, Guidelines and Controls and ISO 17799 10 control sections, 36 control objectives, and 127 detailed, local controls

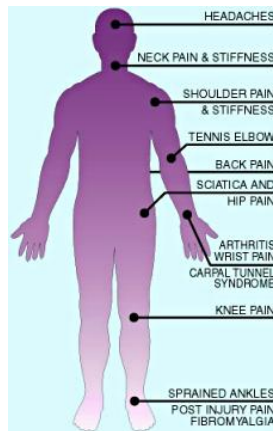
Rating summary: 6 - Hi / Med-Hi, 3 - Med, 1 - Low

Process Compliance

Improvements are needed in BMO processes that demonstrate ongoing compliance with the requirements of the standard, and BMO's own policies and procedures

Rating summary: 2 - Hi / Med-Hi, 2 - Med, 3 - Low

Preliminary lessons learned



Preliminary lessons learned

- Executive support and available budget are key success factors.
- Training is an eye opener. Highly recommended.
- Scope is hard to define. Clear boundaries needed.
- Departmental structure may not align well with the standard's controls.
- Enterprise-wide implementation is costly. Be sure about your benefits.

Next Steps

- Develop detailed plan to close the gaps identified by consultants
- Prioritize tasks based on confidence level
- Acquire resources (software, man-hours, etc)
- Develop all of the key BS7799 documents (e.g. Statement of Applicability)
- Implement ISMS
- Collect data for audit trail
- Obtain certification of ISMS

Questions??

