The Institute of Internal Auditors
Ottawa Chapter
Lunch and Learn
November 20, 2013

The Threat and Risk Assessment (TRA)

John F. Clayton
Senior Security Analyst
Risk Management Consulting
Bell Canada
The Threat Risk Assessment (TRA)

- Audit Context
- Audits and Security
- The TRA Process
- The TRA as Audit Evidence
- Assessing the TRA
- References and Training
- Final Questions
3.1 Internal auditing in the Government of Canada is a professional, independent and objective appraisal function that uses a disciplined, evidence-based approach to assess and improve the effectiveness of risk management, control and governance processes.

Source: Policy on Internal Audit
Audits and Security

- Management Accountability Framework
  - Area of Management 8: Management of Security
  - Area of Management 9: Integrated Risk Management
- Policy on Government Security
  - 3.1 Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence.
- Program and Service Delivery
Audits and Security

Employees + Tangible assets → Deliver Services

Affect

Intangible assets
Employee perceptions
Client expectations

Source: HTRAM, Annex B, section 2.6
The TRA Process

- Preparation
  - TRA Work Plan
- Asset Identification and Valuation
  - Statement of Sensitivity
- Threat Assessment
- Risk Assessment
  - Vulnerability Assessment
  - Calculation of Residual Risk
- Recommendations
The TRA Process

\[ R = f (A_{\text{Val}}, T, V) \]
The TRA as Audit Evidence

• Vulnerability Assessment Measures Safeguard Effectiveness
• May Provide an Objective Appraisal of Risk Management, Control and Governance Processes

• Indicators of Inadequate Control and Governance
  • No TRA (Unless Standards Are Applied)
  • TRA Outdated
  • Incomplete TRA
  • TRA Recommendations Ignored
Assessing the TRA

- Methodology
- References
- Interviews
- All Assets Identified
- All Threats Addressed
- All (Relevant) Controls Assessed
  - ITSG-33
  - Physical Security Standard
- All Values Explained
References and Training

• Policy on Government Security (PGS)

• TRA-1 – Harmonized TRA Methodology

• ITSG-33 – IT Security Risk Management: A Life Cycle Approach

• Operational Security Standard on Physical Security
References and Training

- Communications Security Establishment Canada (CSEC)
  103 - Harmonized Threat and Risk Assessment (HTRA)

- Canada School of Public Service (CSPS)
  Harmonized Threat and Risk Assessment (HTRA) (A341)