Festival Hydro INC.

OEB Framework Planning

Background

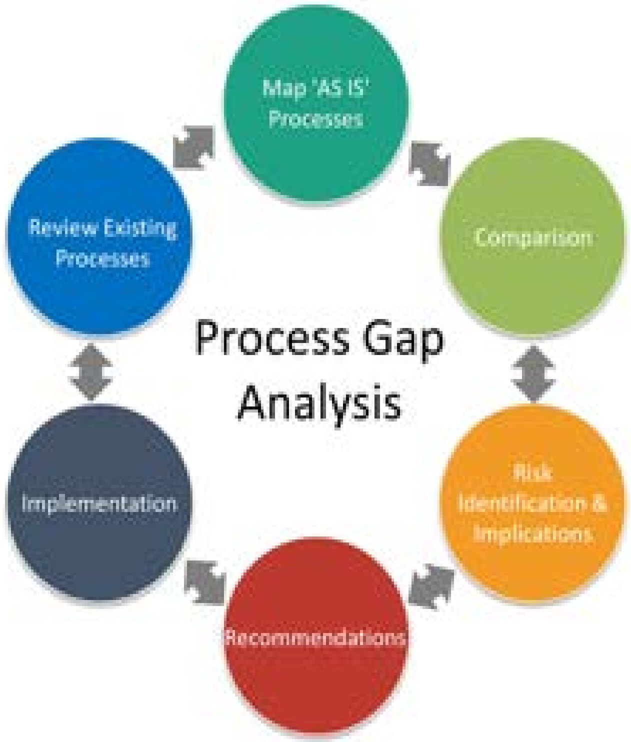
15+ Years in IT

- Service Delivery Manager - Libraries NI
  - OGG in terms of Risk, ITIL, Program and Project Management – wrapped in corporate Governance
- CIO for HP School Board
  - Digital Student Security and Privacy with Canadian regulations – MFIPPA and PIPEDA
  - Best practice related to IT Security (OGC)
- Festival Hydro
  - Moved to LDC 12 months ago and commenced working with OEB Framework

Approach

Gap Analysis

- Baselining current operational service
- Identification of services, products, assets and key vendors supporting service
- Identify gaps in service operation against standards in OEB Framework
- Plan to address the gaps
- Assess progress



Policies and Standards

Development of Policy controls

- Governance of IT operations

Creation of Standard Operating Procedures for IT

- Asset Management, Change Management, Configuration Management, Risk Management
- Deliverables include: Asset Management Program, Risk Management Program, Incident response Plans

Asset Management

Do we have any valid licences?

- The Asset Challenge:

Are we vulnerable to the latest threat?

How do you mange what you don’t know you have?

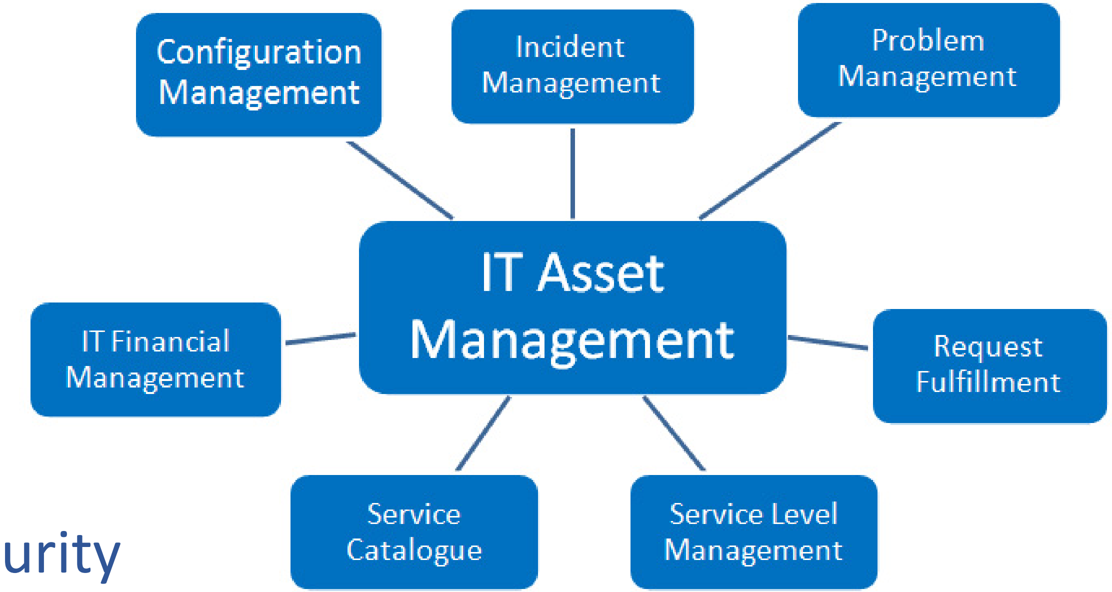
Does every device have the most up to date patch installed?

How many devices do we need to replace next year?

Do we know who’s laptop accessed the VPN last?

Asset Management Program

- Asset Governance
    - Inventory
    - Ownership (responsibility)
    - Software & licence compliance
    - Secure Disposal



- Asset Categorization
    - Visibility of assets needing enhanced security

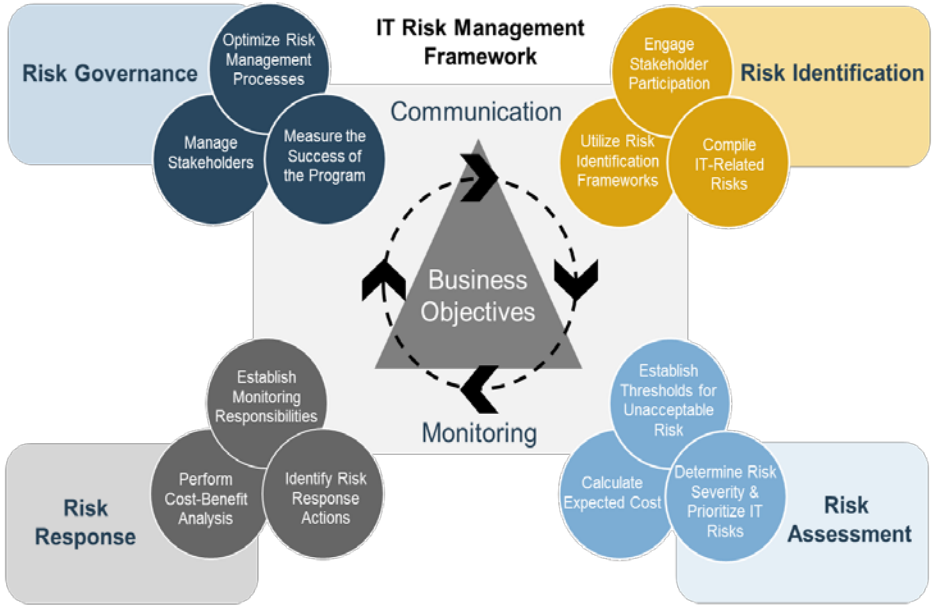
- Consistent approach to IT and OT assets

Festival Hydro INC.

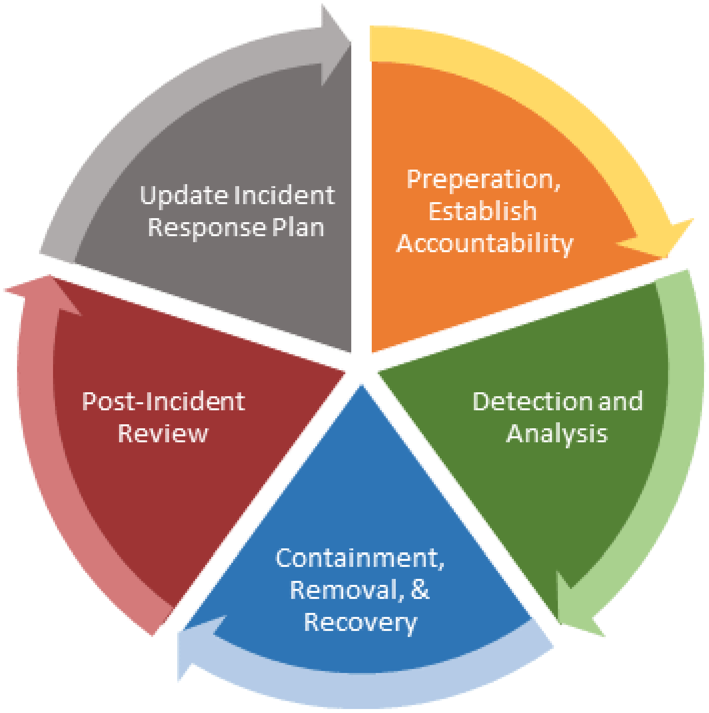
Risk Management Program

- Standardize risk management processes
  - Describe activities which are necessary to maintain risk governance, Identify & assess risk and determine appropriate response
  - Working group with USF to create a standard approach to RM for utilities
  - Encompass both IT & OT operational risk
  - Provide mechanism for feeding to ERM

- IT Risk thresholds defined by the standards in OEB Framework
  - Risk responses defined and incorporated within Incident response plan


IT Risk Management Framework
Risk Governance
Optimize Risk Management Processes
Manage Stakeholders
Measure the Success of the Program
Risk Identification
Engage Stakeholder Participation
Utilize Risk Identification Frameworks
Compile IT-Related Risks
Communication
Business Objectives
Monitoring
Establish Monitoring Responsibilities
Perform Cost-Benefit Analysis
Identify Risk Response Actions
Risk Response
Establish Thresholds for Unacceptable Risk
Calculate Expected Cost
Determine Risk Severity & Prioritize IT Risks
Risk Assessment

Incident Response Planning


Update Incident Response Plan
Preperation, Establish Accountability
Detection and Analysis
Containment, Removal, & Recovery
Post-Incident Review

- Classification of Incident types
  - Incident scope with appropriate response
- Roles & Responsibilities
  - Must be clearly understood by team
- Response plans
  - Plans must be in place for each incident type – can be as simple as a workflow with links to checklists & documentation
- Testing and review of plans annually

Vulnerability Management

- Threat Intelligence and awareness
  - Subscription to US-Cert.Gov for alerts related to vulnerabilities
  - Plans for remedial action
  - Internal staff communication
  - Communication to Board members
- Staff Training and communication
  - Phishing software – test campaigns for staff
  - Training repository
  - Inclusion in Vulnerability management plan

Raising Security Awareness

- Education and awareness
  - Senior Management Team
    - Training carried out by AESI
    - Secure practice and awareness championed by SMT
    - Supporting Policies and Procedures governing secure operations
  - Board Awareness Training
    - Conducted by AESI in October 2018
  - Communication to all staff members
    - Awareness of new Policies and Procedures to guide secure operations
    - Education related to individual responsibilities
    - More communication around potential impact of an incident on the organization

Audit & Review

- Audit
  - Audit booked with AESI to review progress to date and feedback on remainder of plan
  - Phase 2 of plan to be refined with feedback from audit and approved for implementation

- Next Steps
  - Assessment of vulnerability management systems
  - Ongoing implementation controls
  - Schedule for employee testing ongoing
  - Schedule for live DR testing