



**Alberta Health  
Services**  
Capital Health

# **Privacy and Security Assessments**

Prairie Health Privacy Day  
Winnipeg, Manitoba

October 22, 2008



# Assessments At Capital Health

## What we have done

- Where we were
- Where we are
- Where we are going
  - Four strategies for improving your assessments

## Lessons Learned



# Where We Were

# Where We Were

## Past Assessments

- Alberta Health and Wellness
  - Security grants to implement ISO 17799
  - Gave us something to start assessing ourselves against
  - Told us we needed to think about oversight and governance and have a framework (ISO 17799)
- Internal Audit
  - Following standard audit methodologies including CoBIT and ITGC
  - Reinforced message that oversight and governance are critical

# Where We Were

## Past Assessments

- Contracted Resources
  - Independent view and methodology
  - Only as focused as we told them to be
- External Involuntary Participation
  - Smile for the cameras!



## Where We Are

### Many Assessments, Many Recommendations

- AHW Security Grants
    - + Internal Audit
    - + Contracted Resources
- = 115 recommendations to implement (Fall 2007)



# Issues



## Issues With Past Process

- Strong Internal Audit = Aggressive Audit Plan
  - Scenario: Year 1, do Audit 1
  - Year 2, do Audit 2, PLUS do follow-ups on Audit 1
  - Year 3, do Audit 3, PLUS do follow-ups on Audit 2 and 1
- Since the plan was aggressive, we did not have enough time to finish implementing controls before we had to start the process again



## Issues With Past Process

- No coordination with our audits
  - Internal Audit and Auditor General
    - Both want to review ITGC, EUC, Access Admin, etc.
    - Caused us to get cited for the same thing by multiple groups
- Scope was too big to contain
  - Broad assessments are good in Year 1
  - After that, focus on specific areas



## Issues With Past Process

- Reactive, Reactive, Reactive!
  - React to the government
  - React to Internal Audit and Auditor General
  - React to our own contractors
  - React to external parties we cannot control
- Nothing wrong with these groups ... but we were never in control



# Strategies

## Where We Are Going

### Strategy #1 – Love The One You’re With

- Get in bed with your auditors
- Have open, regular, meaningful communications
- Bring them on your side
  - Engage them
  - Ask for their opinion
- Appoint a single liaison to build the relationship and to isolate IS/IT/IM as much as possible



## Where We Are Going

### **Strategy #2 – Get Regular Checkups But Always Self Examine**

- Self assessments are critical
  - But back them up with regular external reviews
- Share your audit results with your auditors
  - Get them to help with recommendations
  - If you are self-assessing, convince the auditors to not audit that area
- Remember to focus



## Where We Are Going

### Strategy #3 – Don't Avoid Your Boogeyman

- Assess the areas that keep you up at night
- Be very focused
  - Data Loss, Wireless, Removable Media
- Focusing on one area will allow you to develop detailed recommendations and action plans
- Detailed audits on one area will help prove / dispel myths and could reduce anecdotal horror stories
- The sooner you get started, the farther ahead you will be on your auditors – Proactive, Proactive, Proactive!

## Where We Are Going

### Strategy #4 – Pick Your Poison(s)

- Frameworks are great, so why only pick one?
- CoBIT – business governance and how to run an IT shop
  - Auditors love CoBIT and understand it (or at least say they do)
  - Use CoBIT to talk to your auditors in their language
- ITIL – IT operations governance
  - Helps to get IS/IT thinking in terms of rigor, process, etc.
- ISO 17799 – Security best practices



# Lessons Learned



# Lessons Learned

## You Need Multiple Tools

- One size does not fit all for assessments
- Have different Threat and Risk Assessments for
  - Internal projects
  - Externally facing projects
  - Vendor and third-party access
  - “Trusted” partners

## Lessons Learned

### You Will ALWAYS Find Something

- Critical to get senior management to realize this!
- The point of an assessment is (should be) to find areas and fix them
  - Not to be a witch hunt or to pick on one group
- However!
  - Fail an assessment once, that's okay
  - Fail the same assessment twice, that's not okay