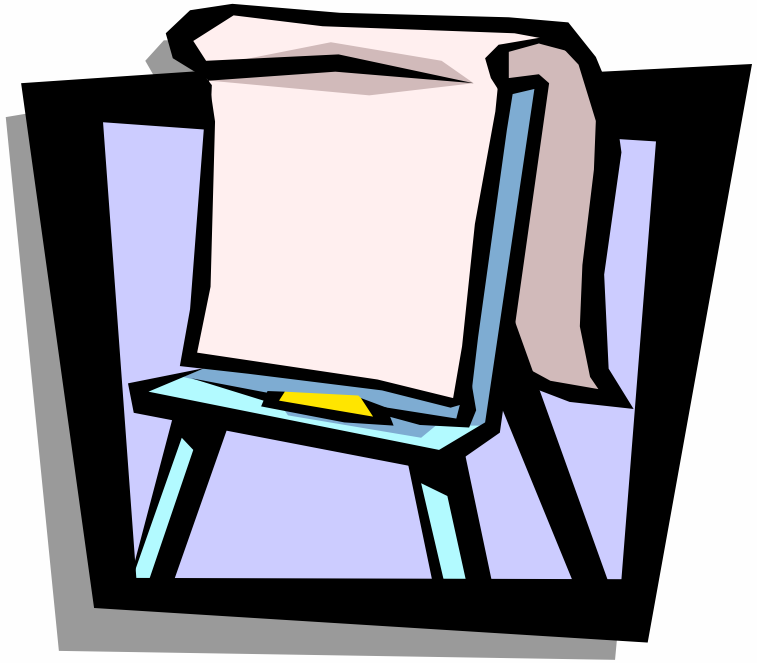
Information Security Governance Using a Risk-based Approach

Eric Holmquist
VP, Director of Operational Risk Management
Advanta Bank Corp.
eholmquist@advanta.com

Agenda

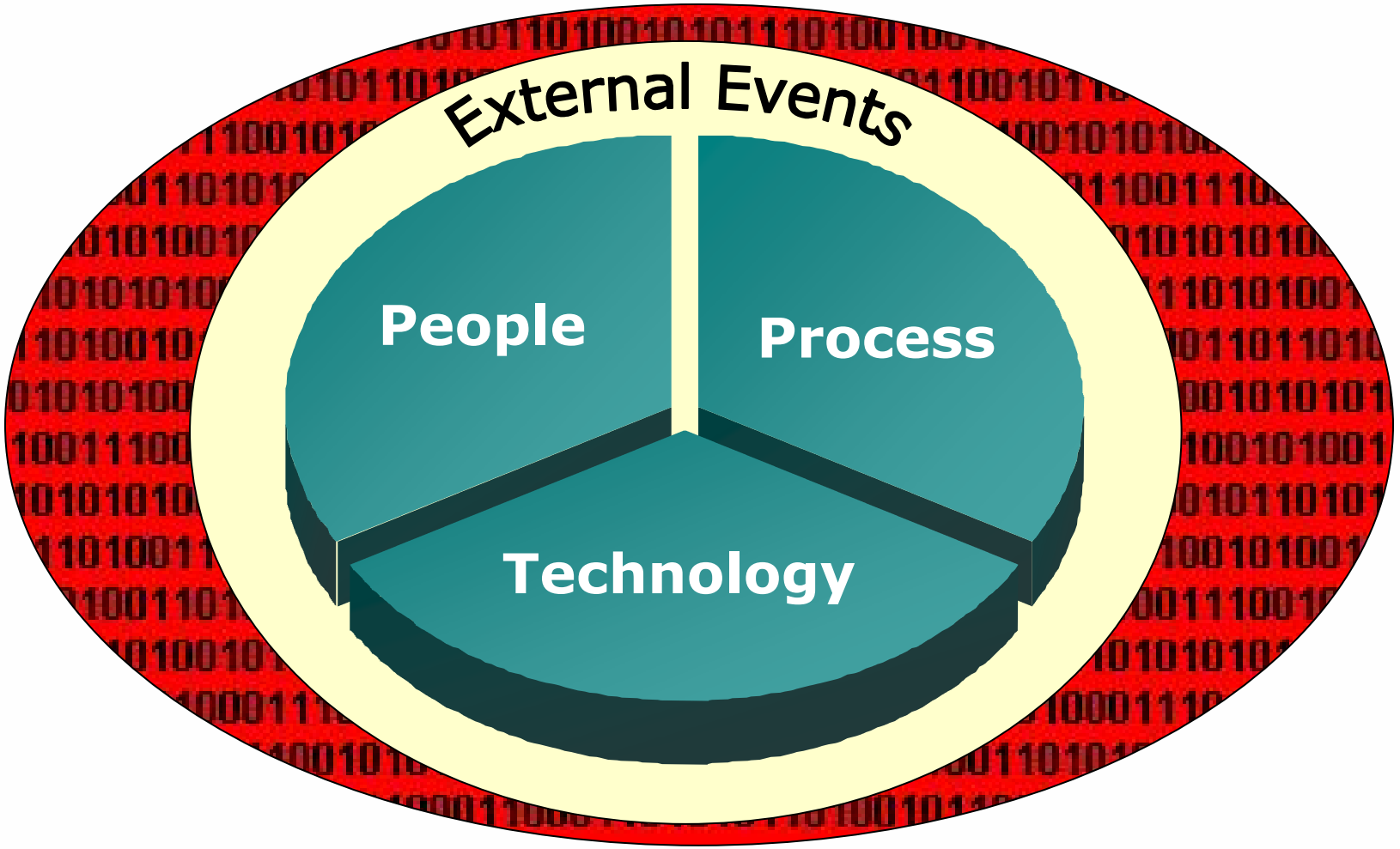
- Risk based approach
- Governance
- Assessing risk
- Other tactical points
- Q&A



Where do we start?

Information security must be approached as a business issue not a technology issue. Once we agree on this then we can consider using risk management practices.

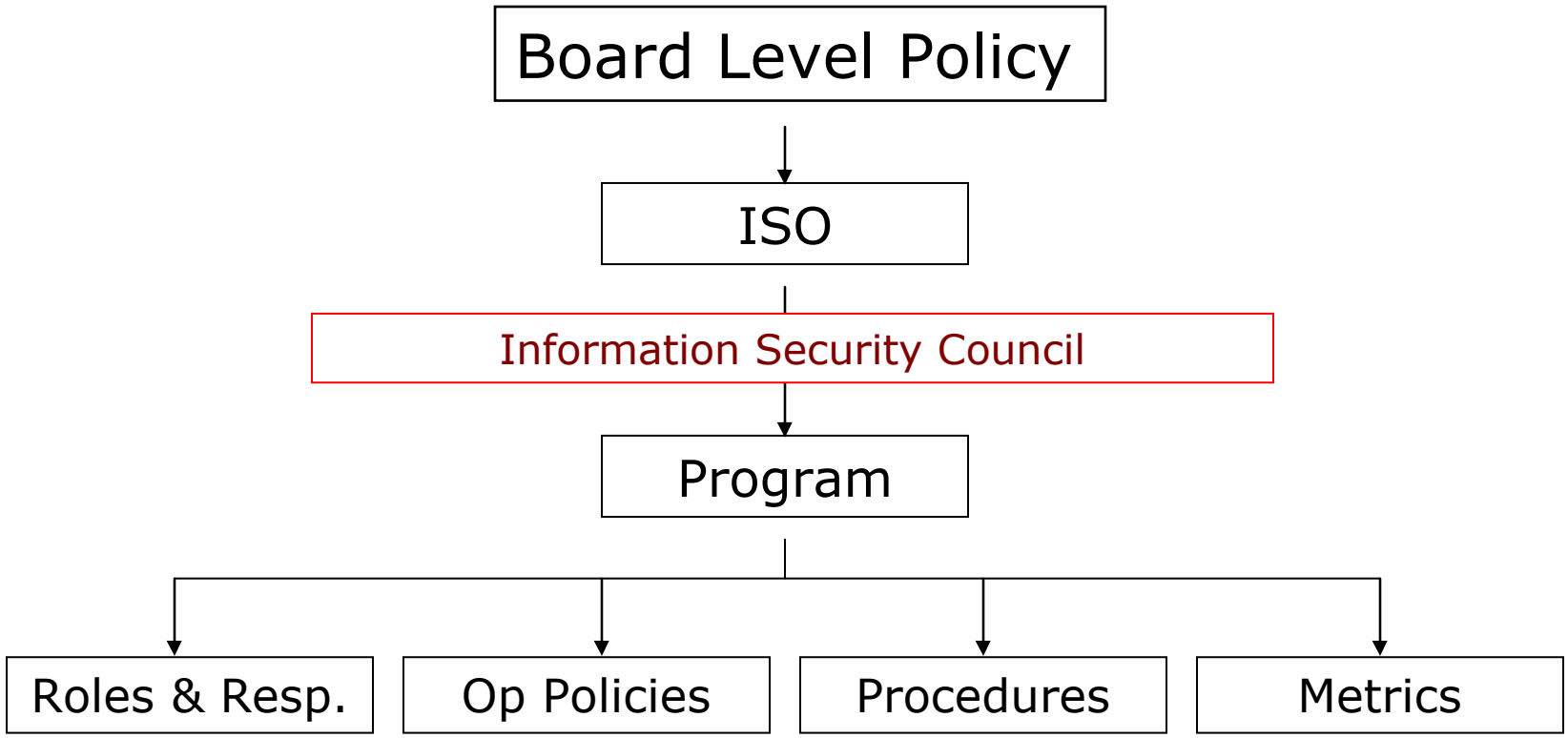
Information Security



Taking a risk based approach means:

- Cross functional governance
- Comprehensive risk assessment methods
- Dynamic risk measurement methods
- Ownership and accountability
- Effective communication
- Ensuring ability to quickly respond
- Meaningful reporting mechanisms
- Face it, historical loss data is worthless

Governance Structure



Information Security Policy

- Board level policy
- Establishes issue as business risk
- Defines the role of the CISO
- Sets mandate for program
- Establishes program expectations
- Not detailed on program specifics

Information Security Program

- Regulatory requirement
- Supports issue as business risk
- Documents major components
- Eliminates unspoken assumptions
- Sets clear responsibilities
- Defines risk-based approach
- Establishes training curriculum
- Supported with operating policies

Engaging senior management

- Starts with education and awareness
- Once educated, solicit active input
- Language is the key!!!!

Information Security Council

- Give it authority to set policy
- Get senior participation
- Make it cross-disciplinary
- Make it visible
- Make it safe

Build a big army

- Create a culture of cooperation
- Build social intolerance to data exposure
- Make disclosure safe
- Don’t underestimate people’s “gut”
- Make it everyone’s responsibility
- Reward creativity

Using a risk based approach

- Everything starts with the risk assessment
- Manage to assessed risk, not perceived risk
- Have to understand inherent vs. residual risk
- Insiders are exponentially more of a threat than outsiders
- Managing a control is not managing a risk
- Ability to respond quickly and effectively is critical

Assessing risk

- **Approach 4 ways**
  - Information systems
  - Electronic data
  - Physical files
  - Third parties
- **Focus on accountability**
- **Some overlap, but each has distinct owners**
- **Use self-assessments vs loss date or scenarios**

Risk quantification

- **Risk is quantified in four broad categories**
  - What's at risk?
    - Customer, corporate, operational, prospect, third-party
  - What would be the impact?
    - Financial, operational, regulatory & reputation
  - What could be the source?
    - Internal, external & natural disaster
  - What can we mitigate?
    - Prevention, monitoring & recovery

Monitoring and Reporting

- **Information security by nature defies M&R**
- **There is a limited amount we can monitor**
  - However, data trends can be meaningful
- **Tie into KRI program – what can we track?**
- **The real value may be in the visibility**
- **Reporting must be timely, clear, root-cause focused and actionable**

And finally…

- Starts with strategy
- Training is absolutely critical
- You're not focused enough on internal risk
- You need more discussion about residual risk
- The worst possible answer to assessing information security risk is…

Questions / Discussion