

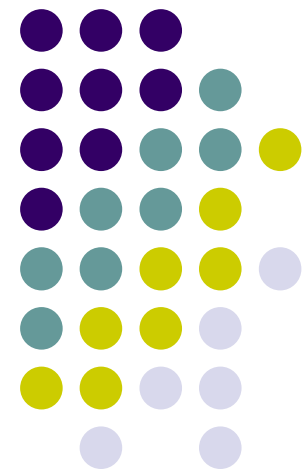
# Best Practices From Banking/Finance

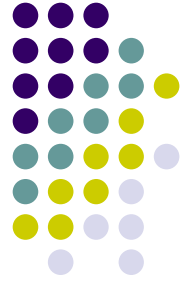
---

**CPO Roundtable**

**Johnna Koso  
Director, Privacy Office  
BMO Financial Group**

**March 7, 2007**





# Presentation Overview

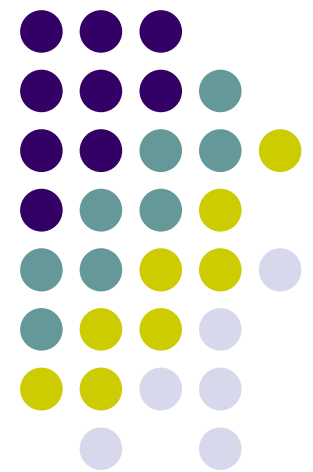
Financial institutions (FIs) have great expectations placed on them from both customers and regulators, and with good reason. It could be argued that FIs deal with some of the most sensitive information about an individual or business that can be had. With that in mind, this presentation will focus on practical matters the Privacy Team at BMO and our colleagues at other FIs have worked through and the top issues privacy professionals face today.

Topics for discussion will be based on experiences with:

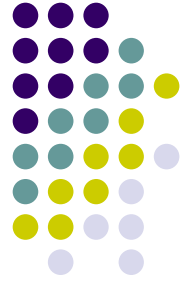
- Developing a privacy program in a multi-national corporation that has to deal with a variety of regulations, a myriad of businesses and a company that's expanding
- Managing diverse issues and complaints
- Monitoring of issues and the resolution of those issues
- Watching what happens to others, not only other Financial Institutions, but companies in other industries and in other jurisdictions

# Setting the Stage

---



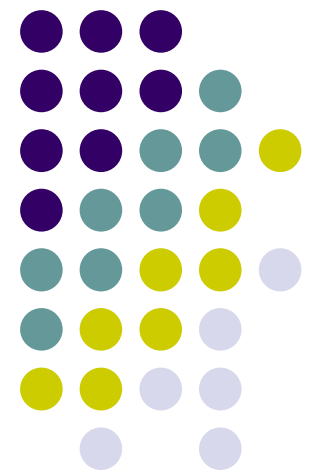
# Business Realities Shape Our Approach to Privacy



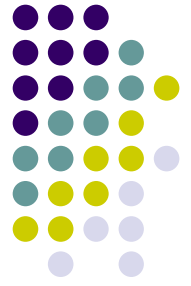
- Built on a foundation of trust
- Customers have high expectations
- Highly regulated
- Anytime, anywhere transactions
- Highly sensitive information in large quantities
- Directly impacted by losses from financial fraud and identity theft

# Challenges and Solutions

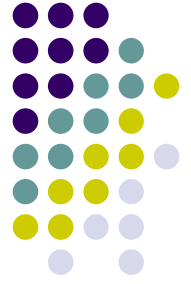
---



# Challenges We've Faced in Developing Privacy Programs



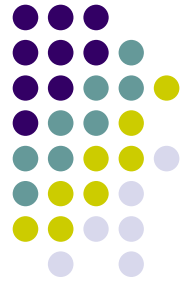
- Management and Employee Engagement
- Complex, changing, multi-national organizations
- Changing regulatory requirements and risks
- Identifying and managing complex issues
- Training and awareness



# Best Practices

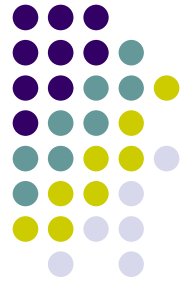
- Organizational acceptance
- Governance approach
- Strong security programs
- Training and Awareness
- Monitoring
- Processes for managing complex issues
- Working with and learning from others

# Organizational Acceptance – Obtain Board and Executive Management Commitment



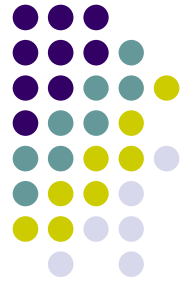
- Acknowledgement of importance
- Chief Privacy Officer with accountability to the Board
- Dedicated resources
- Continued engagement

# Organizational Acceptance – Work with Internal Networks/Partners



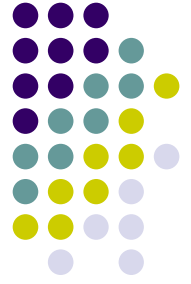
- Don't try to do it on your own
- Partner with corporate areas
- Privacy representatives in business areas
- Regular communication

# Organizational Acceptance – Imbed Privacy in Practices



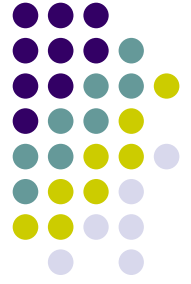
- Build privacy requirements into business processes
- Participate in projects, supplier reviews, due diligence
- Every employee plays a role

# Governance – Complex Organizations Need Formality



- Enterprise-wide approach
- Multiple, competing and changing regulatory requirements
- Geographically dispersed
- Cross-border considerations
- Multiple lines of business

# Governance – Programs Must be Adaptable to Changes



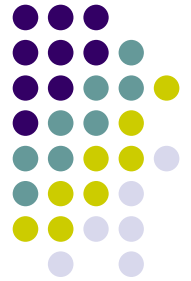
- Changing business strategies
- Changing technology
- New products/services
- Outsourcing
- Acquisitions/Divestitures

# Security Programs – Protect What’s in the “Vault”



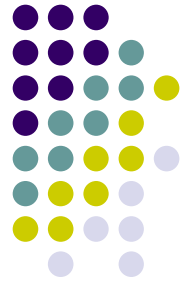
- It’s not just about the money
- Don’t forget about physical security
- Keep it simple – demystify information security

# Security Programs – Make them Adaptable



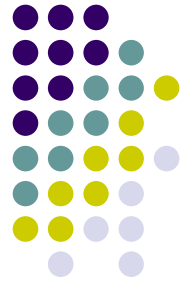
- Information classification
- Business requirements
- Regulatory requirements
- Changing technology
- Changing risks

# Training and Awareness – Cover the Head Office to the Front Line



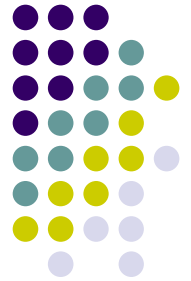
- Make it relevant
- Sometimes you have to repeat yourself
- Address systemic issues
- Be creative!

# Training and Awareness – Consider Customers in Your Plans



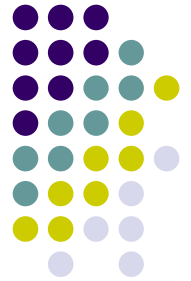
- Customer advocacy
- Address current fraud techniques
- Don't assume someone else will tell them

# Monitoring – Identify Issues Before There is a Problem



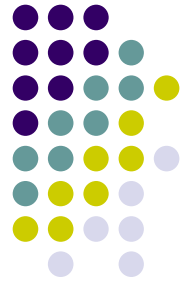
- Leverage other corporate functions
- Learn from complaints and breaches
- Ensure employees know how to reach you

# Monitoring – Be Aware of Your Surroundings



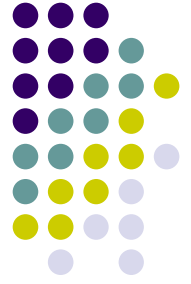
- Pending legislation
- Regulatory guidance
- Learn from the issues of others

# Complex Issues – Be Prepared for Anything



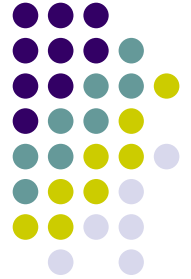
- From isolated to the “big one”
- Variety of sources
- Well intentioned (and not so well intentioned) employees
- Domestic disputes
- Regulatory investigations
- Third party breaches

# Complex Issues – Develop Processes



- Take it seriously
- Utilize dispute resolution processes
- Communicate the process
- Report on issues
- Learn

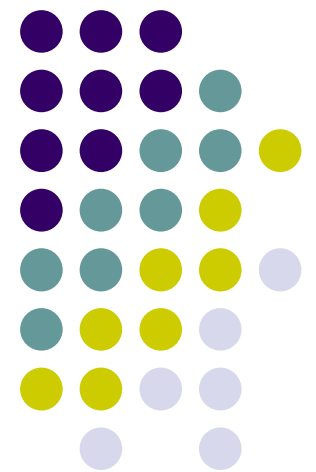
# Working Together

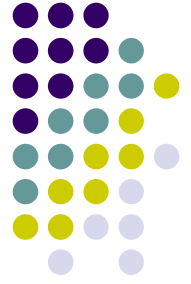


- Participate in industry working groups
- Establish good relationships with regulators

# Looking Ahead

---

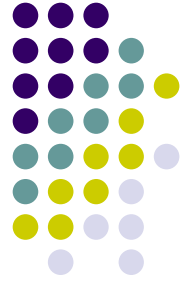




## Current Challenges

- Staying ahead of the fraudsters
- Balancing convenience with control
- Adherence to established processes
- Self-sufficient business units
- New and changing regulatory requirements

# What's Next for Privacy



- Privacy will continue to be a top of mind issue regardless of industry
- Programs will continue to evolve
- More and more information will be collected and aggregated
- New and changing regulatory requirements
- Threats will change

# Questions / Discussion

---

