PERKINS & CO

Let's get there

Privacy Risk Assessments

Michael Hulet

Principal

November 8, 2012

Agenda

Privacy Review

- Definition
- Trends

Privacy Program Considerations

Privacy Risk Assessment

- Risk Assessment Tools
  - Generally Accepted Privacy Principles
  - AICPA Privacy Tools
  - Privacy Maturity Model
- Other Resources

Privacy Review

What is Privacy?

No Single Definition...

“the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.”

What is Privacy?

Examples of Customer Data:

- Email addresses
- Customer name
- Social Security Number
- Address
- Telephone number
- Drivers license number
- Credit card number
- Credit data
- Bank account number

What is Privacy?

Examples of Employee Data:

- Ethnic & Gender Info
- Physical Address
- Social Security Number
- Salary & Position
- Health Information
- Phone Numbers
- Name
- Date of birth
- Retirement & Other financial data (e.g. bank account numbers for employee direct deposit)

Privacy Trends

Regulators more proactive & aggressive → Shift from consumer responsibility to organizational accountability

Increasing collection & Use of information—More than consumers know → Customers more willing to provide personal information, expecting that corporations will be accountable for its safekeeping

Sharing data with third parties is increasing → Services can be outsourced but accountability cannot

@PerkinsCo

Regulatory Trends

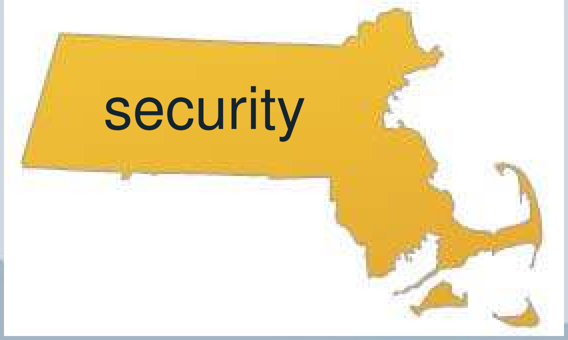
Regulatory Landscape

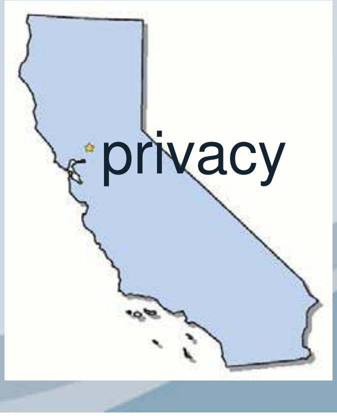
Since 1998, over 200 laws in over 150 countries

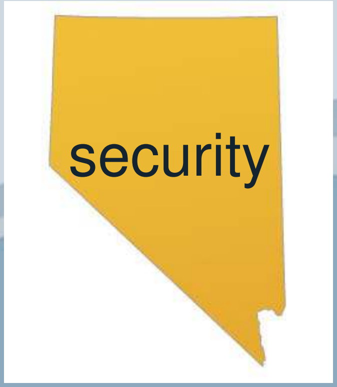
Since Jan 1, 2003, over 75 new privacy laws in the U.S.

46 State Breach Notification Laws, plus U.S. territories

Three leading states:







@PerkinsCo

Regulatory Trends

Federal enforcements are on the rise:

- FTC: Stop Unfair and Deceptive Practices
- HHS-OCR: Audit Review of Technical, Physical, and Administrative Safeguards
- FCC: Telephone Consumers Protection Act (TCPA)
- CFPB: Dodd-Frank Act § 1033
- SEC: Guidance - Cybersecurity Risks and Cyber Incidents

Technology Trends

Technology leads to changes in security

- Cloud technologies
- Mobile technology
- Social networking
- Online behavioral advertising
- Privacy by design

Privacy Program Considerations

Privacy Program Considerations

Challenges to Privacy Program Success

- An ineffective governance structure
- Lack of a strong culture and attitude at all levels
- Lack of resources committed to building and sustaining a privacy program
- Lack of a single global framework to address all rules and requirements
- Incomplete or partially completed Data Inventory

10 Keys to a Successful Program

- Effective governance structure
- Strong culture and attitude at all levels
- **Effective risk assessment process**
- Complete, dynamic, current lifecycle data inventory that includes third parties
- **Controls aligned with a selected framework**
- Effective training and awareness program
- Effective team that ensures compliance with laws and regulations

@PerkinsCo

10 Keys to a Successful Program

- **An effective auditing and monitoring function**
- Current, communicated and followed policies and procedures
- Effective, documented and tested incident response plan

Designing, implementing, maintaining and monitoring a solid privacy and information security program requires effective support, resources, skills, time and discipline

@PerkinsCo

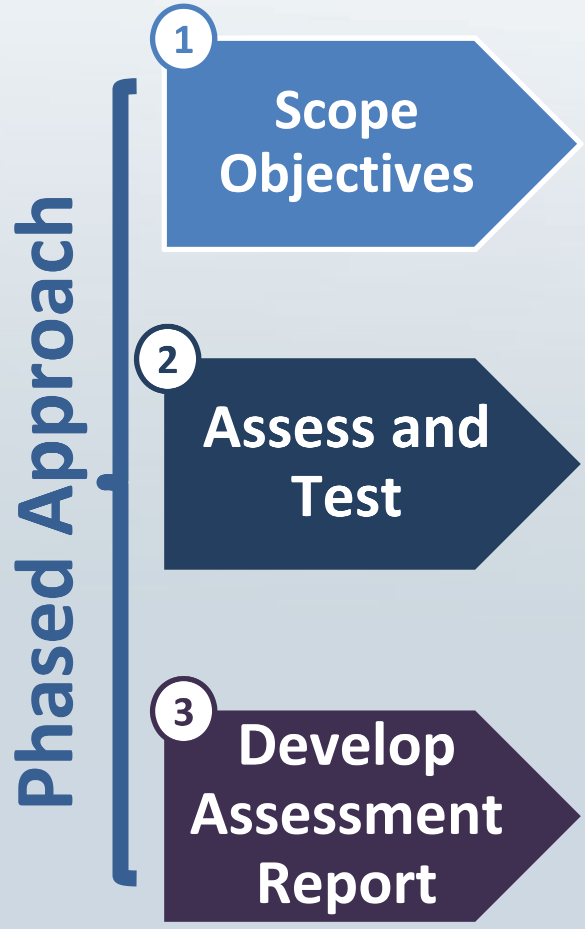
Role for Internal Audit Function

Ongoing independent monitoring of a company’s privacy program could include:

- Completing a privacy and security gap assessment
- Evaluating the company’s periodic privacy risk assessment process
- Evaluating compliance with established privacy policies and procedures
- Evaluating data protection and privacy training and awareness programs
- Ensuring data protection and privacy-related remediation is in place
- Reviewing third party/vendor privacy practices

Privacy Risk Assessment

Privacy Risk Assessment Approach



Phased Approach

1 Scope Objectives

Identify key data privacy objectives (principles and criteria) and define the scope

2 Assess and Test

Assess and/or test the people, process and technology against the defined business objectives. Identify areas of improvement.

3 Develop Assessment Report

Document results of the assessment and testing to be used to support company’s privacy policies.

@PerkinsCo

GAPP Framework

Generally Accepted Privacy Principles (GAPP)

- Developed from a business perspective
- Referenced significant privacy regulations
- Created single privacy objective
  - Supported by 10 privacy principles
  - Created objective, measurable criteria for each principle

GAPP Framework

Overall Privacy Objective

Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA.

GAPP Framework

Privacy Principles

- Management
- Notice
- Choice and consent
- Collection
- Use, retention, and disposal

GAPP Framework

Privacy Principles (continued)

- Access
- Disclosure to third parties
- Security for privacy
- Quality
- Monitoring and enforcement

GAPP Alignment with Regulations

How does GAPP map to US regulations?

Generally Accepted Privacy Principles	U.S. FTC	U.S. Safe Harbor	U.S. HIPAA	U.S. GLBA
Management			Administrative requirements	
Notice	Notice	Notice	Notice	Privacy and Opt Out Notices, Exceptions
Choice and Consent	Choice	Choice	Consent, Uses and Disclosures	Privacy and Opt Out Notices
Collection		Data Integrity		
Use, Retention, and Disposal		(Implied but not specified in the principles)	Uses and Disclosures	Limits on Disclosures
Access		Access	Access	
Disclosure to Third Parties		Onward Transfer	Uses and Disclosures, Accounting of Disclosures	Limits on Disclosures
Security for Privacy	Security	Security	Security Rule	Security Guidelines mandated by section 501(b) of GLBA
Quality	Integrity	Data Integrity	Amendment	
Monitoring and Enforcement	Enforcement	Enforcement	Compliance and Enforcement by the Department of Health and Human Services	Enforcement by financial services industry regulators, the FTC, and SEC

@PerkinsCo

GAPP Alignment with Regulations

How does GAPP map to international regulations?

Generally Accepted Privacy Principles	Australia Privacy Act	Canada PIPEDA	E.U. Directive	OECD Guidelines
Management		Accountability	Notification	Accountability
Notice	Openness	Identifying Purposes, Openness	Information to Be Given to the Data Subject	Purpose Specification, Openness
Choice and Consent	Use and Disclosure	Consent	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation
Collection	Collection, Sensitive Information, Anonymity	Limiting Collection	Principles Relating to Data Quality, Exemptions and Restrictions	Collection (including consent) Limitation
Use, Retention, and Disposal	Identifiers, Use and Disclosure	Limiting Use, Disclosure, and Retention	Making Data Processing Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	Use Limitation (including disclosure limitation)
Access	Access and Correction	Individual Access	The Data Subject's Right of Access to Data	Individual Participation
Disclosure to Third Parties	Use and Disclosure, Transborder Data Flows	Limiting Use, Disclosure, and Retention	Transfer of Personal Data to Third Countries	Use Limitation (including disclosure limitation)
Security for Privacy	Data Security	Safeguards	Confidentiality and Security of Processing	Security Safeguards
Quality	Data Quality	Accuracy	Principles Relating to Data Quality	Data Quality
Monitoring and Enforcement	Enforcement by the Office of the Privacy Commissioner	Challenging Compliance	Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	Individual Participation (including challenging compliance)

AICPA Privacy Tool

Based on GAPP

- Scores risk for 73 GAPP criteria based on
  - Likelihood of control failure
  - Business impact
  - Effort/cost to mitigate
- Not intended as a “plug-and-play” tool
- Requires understanding of
  - Entity’s privacy programs and initiatives
  - Privacy environment in which entity operates
  - Legislative, regulatory, industry, jurisdictional privacy requirements

AICPA Privacy Tool

Sample Input Template

Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk

GAPP - 73 Criteria	Criteria Description	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
1.0 MANAGEMENT (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.			
Privacy Policies (1.1.0)	Policies are defined for: notice, choice/consent, collection, use/retention/disposal, access, disclosure, security, quality, and monitoring/enforcement.	2	8	2
Communications to Internal Personnel (1.1.1)	Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	2	5	2
Responsibility and Accountability for Policies (1.1.2)	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	2	5	2

AICPA Privacy Tool

Sample Criteria Summary

Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk

1.0 Management	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
14 Criteria	Average Score - 14 Criteria	4.4	5.1	3.9
Privacy Policies (1.1.0)	Policies are defined for: notice, choice/consent, collection, use/retention/ disposal, access, disclosure, security, quality, and monitoring/enforcement.			
Input 1		2	8	2
Input 2		2	2	5
Input 3		0	0	0
Input 4		0	0	0
Input 5		0	0	0
Input 6		0	0	0
Input 7		0	0	0
Input 8		0	0	0
Input 9		0	0	0
Input 10		0	0	0
	Average Score	2.0	5.0	3.5

AICPA Privacy Tool

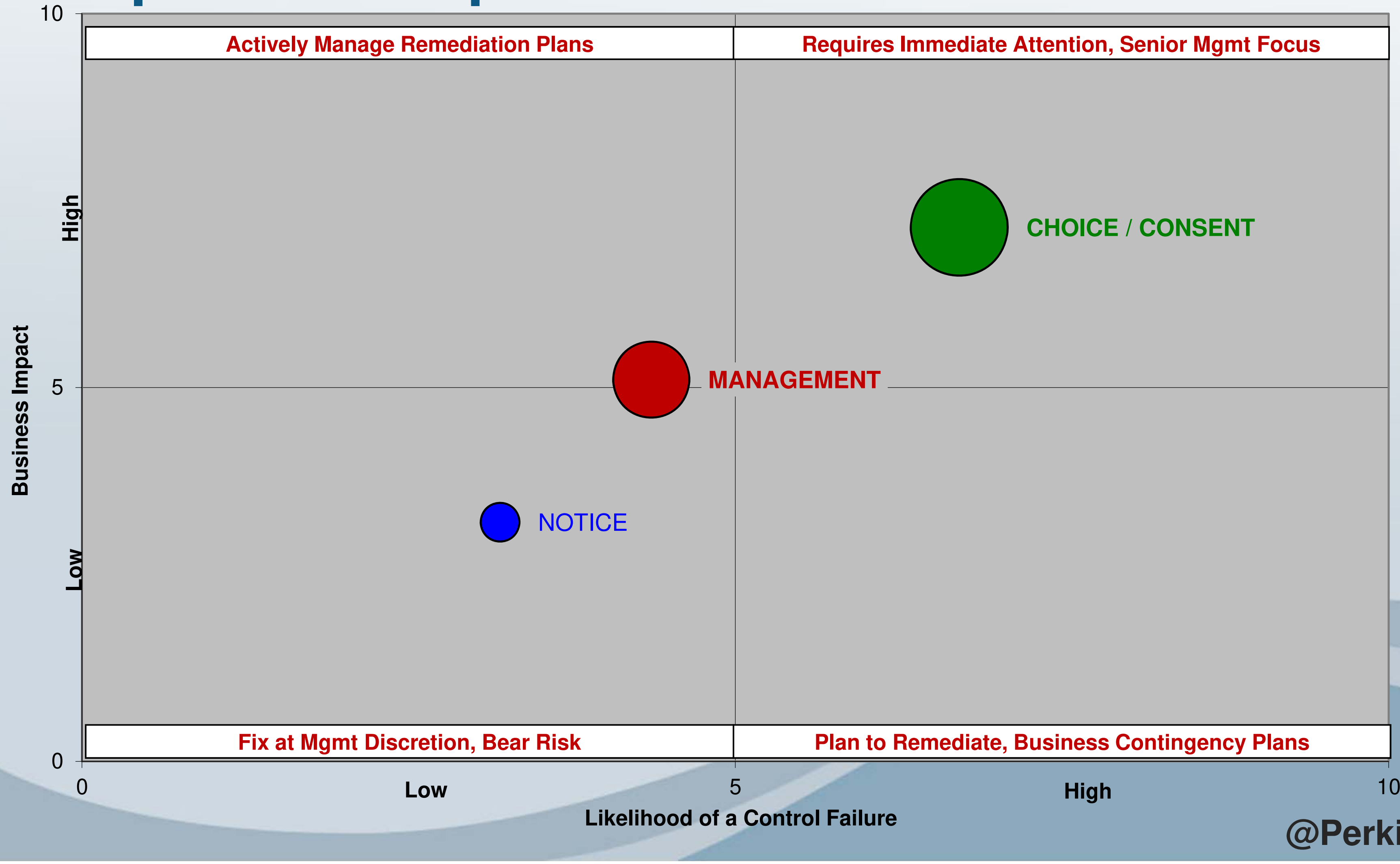
Sample summary of results

Summary of Results

GAPP - 10 Principles		Likelihood of a Control Failure	Business Impact	Size of Marker
MANAGEMENT	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.	4.4	5.1	3.9
NOTICE	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.	3.2	3.2	2.0
CHOICE / CONSENT	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.	6.7	7.1	5.0

AICPA Privacy Tool

Sample Heat Map



@PerkinsCo

Privacy Maturity Model

Based on GAPP

- AICPA/CICA Privacy Task Force
  - Input from ISACA
- Requires understanding of GAPP and entity-specific privacy requirements
- Designed for organizations that have existing privacy program
- Useful for measuring progress against initial maturity (baseline) and desired maturity (goal)

Privacy Maturity Model

Follows Capability Maturity Model (CMM)

- Five Maturity Levels
  1. Ad hoc
  2. Repeatable
  3. Defined
  4. Managed
  5. Optimized
- Recognizes not all privacy initiatives need to reach highest level of maturity
- Facilitates measurement of progress over time and identification of next steps for continuous improvement

Privacy Maturity Model

To be effective, PMM must consider:

- Maturity of the entity’s privacy program
- Ability to obtain complete and accurate information on the entity’s privacy initiatives
- Agreement on the Privacy Maturity assessment criteria
- Level of understanding of GAPP and the PMM

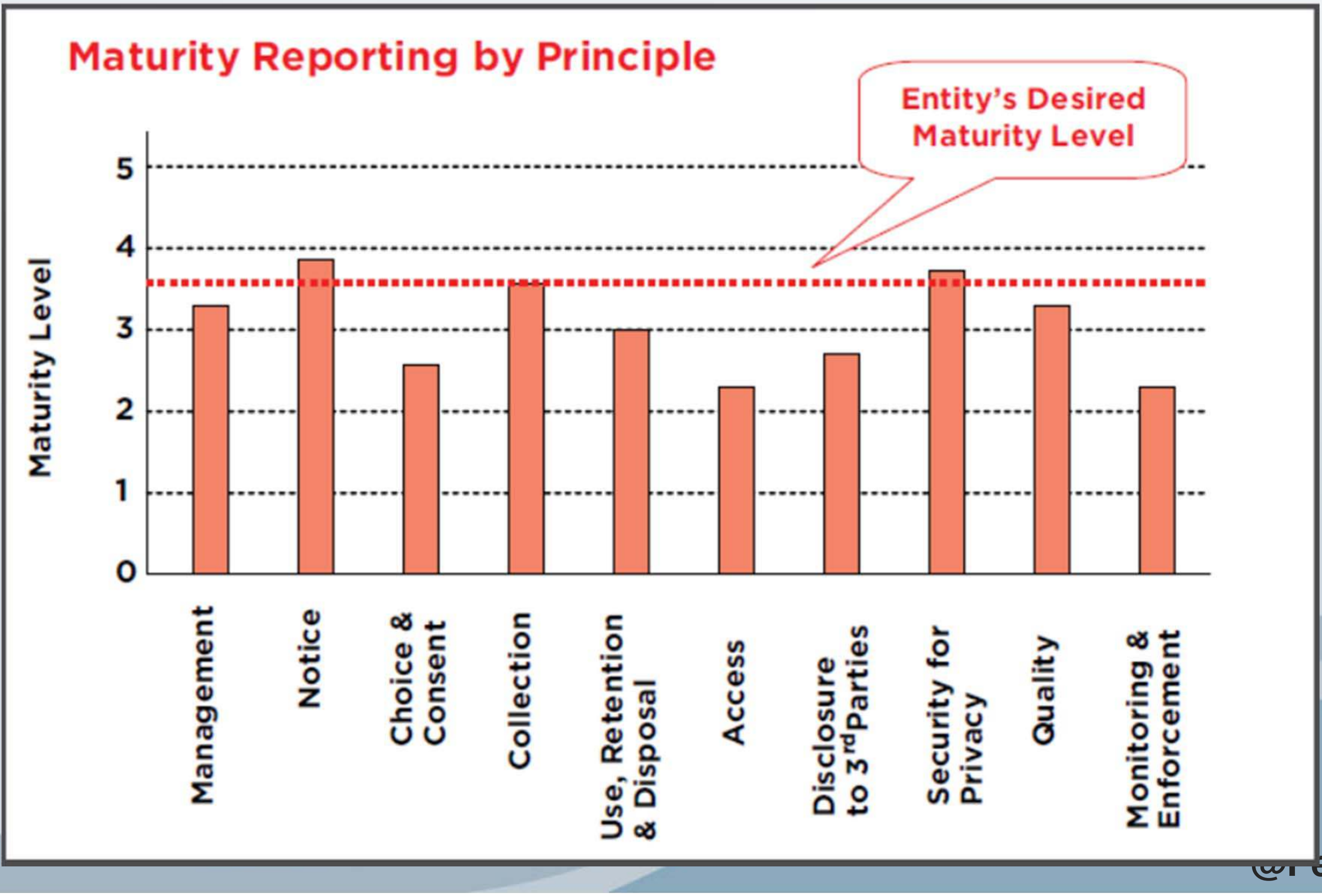
Privacy Maturity Model

Sample PMM Criteria Maturity

GAPP – 73 Criteria	Criteria Description	Maturity Levels				
		Ad HOC	Repeatable	Defined	Managed	Optimized
Management (14 criteria	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Policies (1.1.0)	The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement .	Compliance with privacy policies are monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely manner.

Privacy Maturity Model

Sample PMM Report



Other Resources

AICPA

http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx

IAPP https://www.privacyassociation.org/

FTC http://business.ftc.gov/privacy-and-security

ISACA

http://www.isaca.org/Groups/Professional-English/privacy-data-protection/Pages/Overview.aspx

Summary

Privacy laws and risks will continue to evolve

Privacy programs can be effective at reducing risks

A privacy risk assessment can identify risks and facilitate mitigation

Numerous resources are available to support the practitioner in performing a privacy risk assessment

Questions:

Michael Hulet mhulet@perkinsaccounting.com

503-221-7533

LinkedIn/Michael Hulet

Perkins & Co perkinsaccounting.com

503-221-0336

@PerkinsCo

PerkinsCo

LinkedIn/perkins & co