Conducting a Privacy Assessment

Privacy and HIPAA Compliance Training

October 24, 2001

Brendon Lynch

Senior Manager, Privacy Solutions

p w c

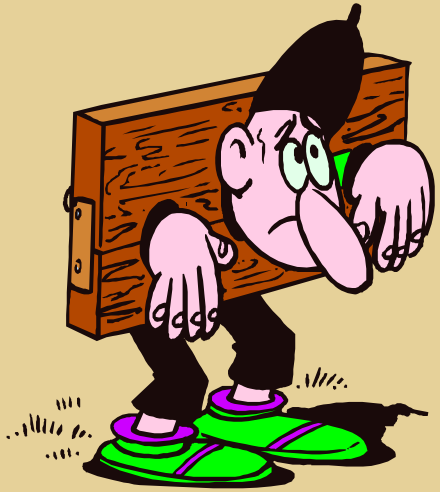
Agenda

- **The Role of Privacy Assessments**
- **Generic Privacy Assessment Approach**
- **HIPAA Privacy Considerations**
- **eHealth Privacy Considerations**
- **Technologies to Aid Assessment**
- **Questions & Answers**

The Role of Privacy Assessments

P w C

Assessments are central to compliance



- Establishing a good privacy policy is not enough…
- Comprehensive business processes are not enough..
- Deploying leading technology solutions and systems controls is not enough…

Regular assessments are crucial in establishing and maintaining effective compliance

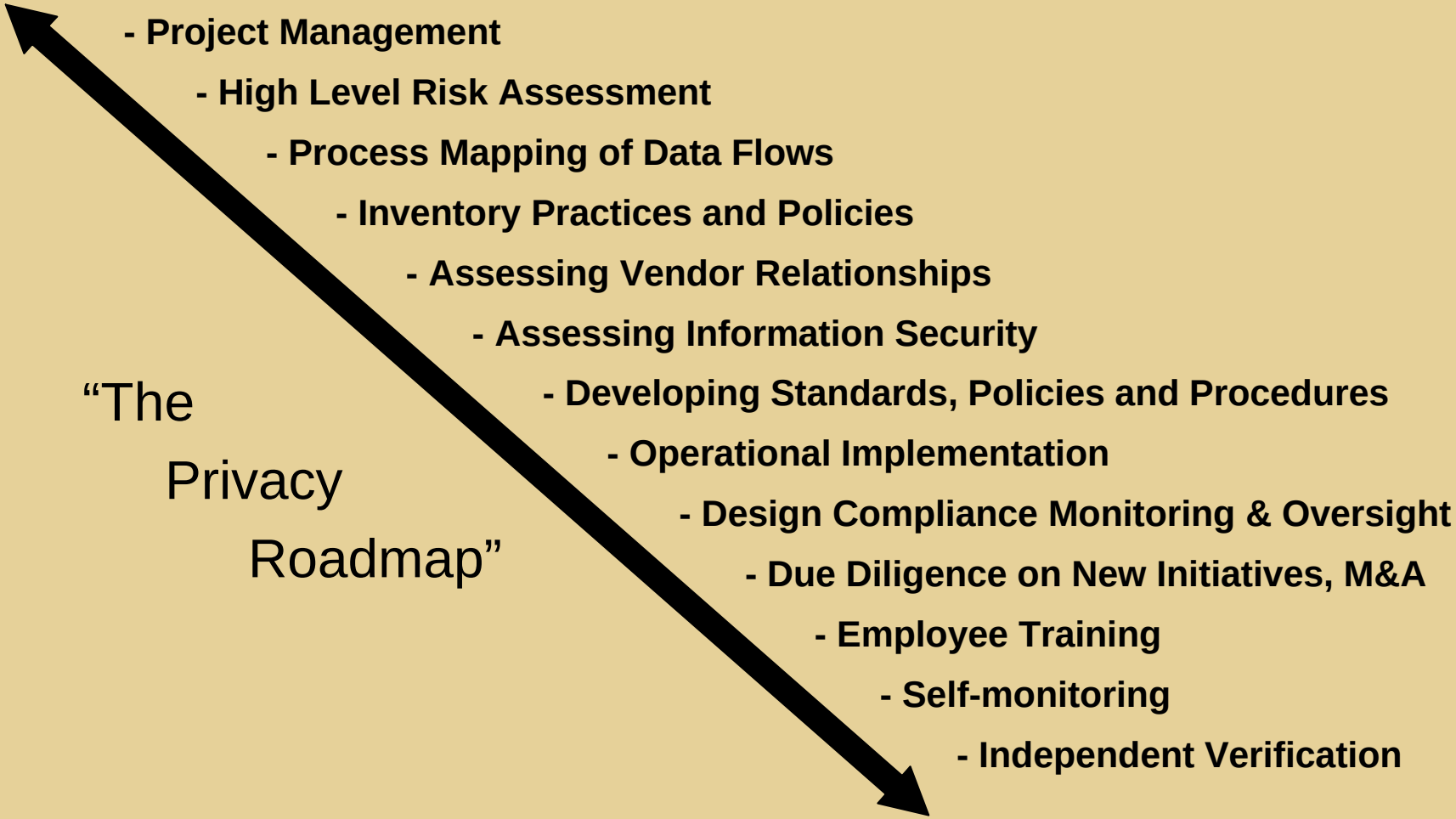
Assessments are central to compliance

- Assessments influence design
  - assist prioritization of activities
  - result in a well designed privacy compliance program
- Design for assessments
  - need for ongoing assurance should be considered all design decisions
  - auditability and audit trails are often needed

Three Types of Assessments

- Risk Assessment
  - what is our exposure and what do we need to do?
- Readiness Assessment
  - have we implemented adequate privacy assurance controls?
- Compliance Assessments
  - how well are we achieving ongoing compliance as our business model changes?

Assessments should cover the full scope of a privacy compliance program



PwC

Generic Privacy Assessment Approach

P w C

Generic Privacy Assessment Approach

Providing assurance and confidence at every stage in the compliance process and ongoing operation of the business

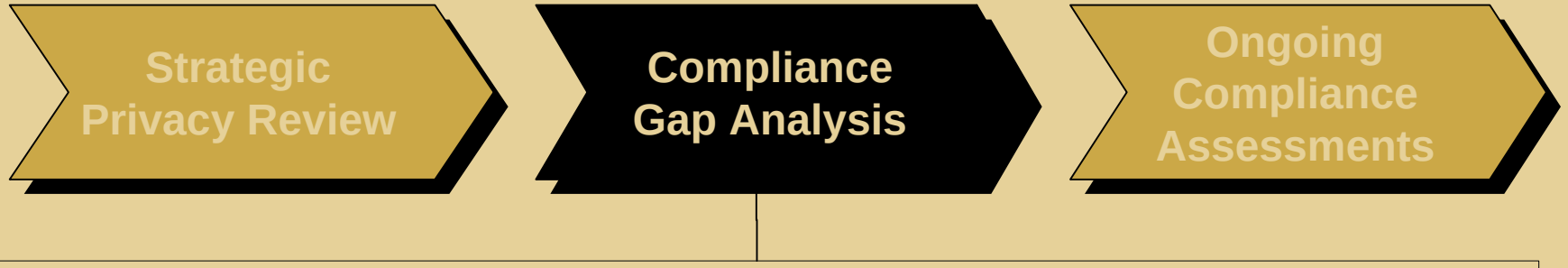
PwC

Strategic Privacy Review

- Work program
  - End-to-end review of the business model to identify patient, employee and consumer information collection, use and sharing
  - Identify key policies, processes and controls in place
  - Benchmark these practices in relation to legislation, industry norms, competitor practices, high sensitivities, etc.
- Outputs
  - Mapping of data flows and associated policies & procedures
  - Recommended enhancements to business and compliance practices

PwC

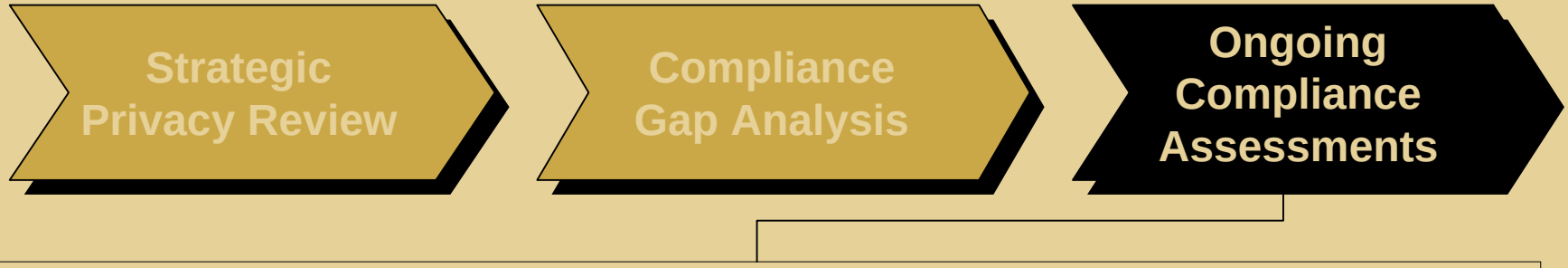
Compliance Gap Analysis



- Work program
  - Establish assessment criteria that will address all components of privacy compliance process
  - Review current implementation of processes and controls to support the standards
- Outputs
  - Gap analysis and recommended improvements to privacy compliance infrastructure

PwC

Ongoing Compliance Assessments



- Work program
  - Review of significant changes to business model since previous assessment
  - Detailed review and testing of the relevant privacy compliance controls over the period of the assessment
- Outputs
  - Report indicating sufficient internal control
  - If applicable, secondary gap analysis of significant control weaknesses – for re-examination at a subsequent date

PwC

HIPAA Privacy Considerations

P w C

HIPAA Privacy Considerations

- Document internal and external flows and uses of Personal Health Information (PHI) – written, spoken, faxed, electronic – to identify risk points
- Evaluate departmental physical as well as IT security practices
- Review information retention policies and procedures
- Evaluate required privacy program elements – privacy official, written policies and procedures
- Following early assessments, recommend rapid rollout projects, longer term remediation projects with high-level work plans and budget estimates

eHealth Privacy Considerations

P w C

Online Privacy Challenges

- The Web provides unprecedented ability to conduct interactive business
- The main benefits of the Internet - high visibility and readily accessible and transferable information - can clash with the basic premise of personal privacy
- Highly publicized online privacy breaches have resulted in lack of trust and lost revenue
- Web privacy assessments are complex – there is much to look for spread over thousands of pages

eHealth Privacy Assessment Considerations

- Identify capture of sensitive personal information (especially PHI)
- Online privacy policies – are they clear, conspicuous and accessible to the user at the point of information collection?
- Are there adequate security protections (e.g. 128bit SSL) at point of collecting sensitive personal information?
- Use of cookies and ‘invisible’ web beacons used for consumer tracking purposes – are they appropriate and disclosed?
- Is there potential for “inadvertent data-spillage” as a result of glitches in website design – e.g. the ‘GET’ method for web forms?
- Use of syndicated content and affiliate integration - is it clear who is receiving information and what privacy policy applies?

Technologies to Aid Assessment

P w C

Technologies to Aid Assessment

- Privacy Permissions Management Technologies
  - Zero-Knowledge Systems PRM Center
  - PrivacyRight TrustFilter
  - IBM Enterprise Privacy Architecture
- Web Privacy Assessment Technologies
  - PwC/Watchfire WebCPO
  - IDcide PrivacyWall

Summary

- Assessments are an important tool to manage risk and ensure compliance activity is in line with compliance objectives
- Begin assessments early in the process – they are value-adding
- Be wary of online privacy issues
- Consider the use of assessment technologies for effectiveness and efficiency

Q&A