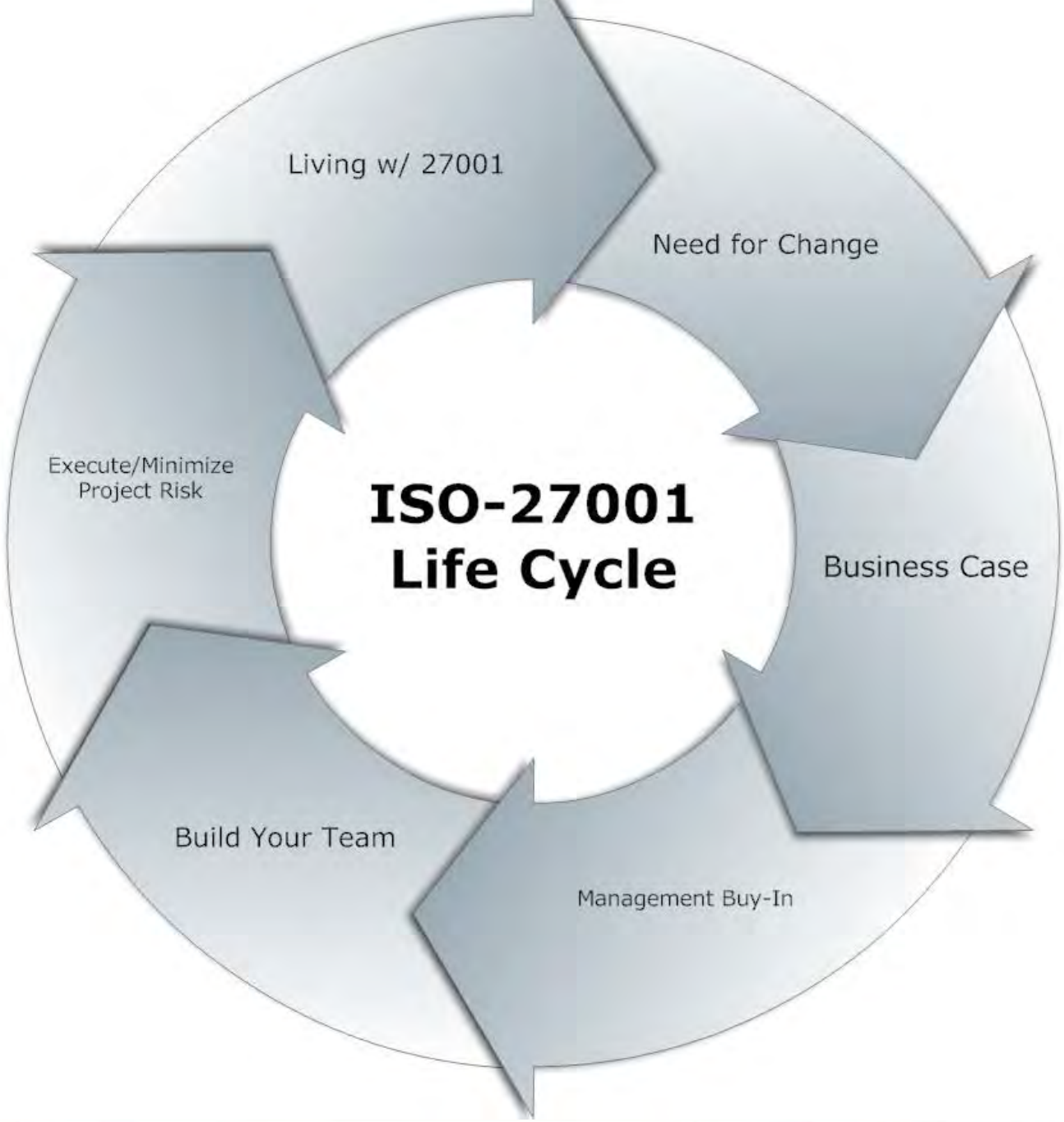
Pivot Point SECURITY

Developing Your Company's ISO-27001 RoadMap

27K Summit May 12, 2015

John Verry, Pivot Point Security

Pivot Point SECURITY



Pivot Point SECURITY

Should We Pursue ISO-27001?

- Typical Drivers
  - Client contracts/RFPs, target market requirements, competitive issues, current risk
- Alternatives (or Additions)
  - What other frameworks/attestations should we consider (instead or in addition)?
    - FedRAMP, SOC1/2, HITRUST, NIST/FISMA, NCSF, 27002 Alignment
- Getting up to Speed
  - Challenging as bulk of meaningful/relevant information is by registrars/consultants
  - Much of it is great content (look for secondary validation)
- Get Conversational
  - To pitch it to management you need to be conversational; speak with key players in the industry to validate your research and build your business case & potential team

Pivot Point SECURITY

Building Your Business Case: Drivers & ROI

- Client Contract (or RFP(s))
- Risk Management
  - PII/PHI Breach Costs (Ponemon Institute)
  - 10K Names = $2M
- Marketing Value
  - Timeline: Competitive Advantage/Evolving Market Requirement/Playing Catch-Up
- Attestation Reduction (time savings)
  - Fewer questionnaires
  - Less Entertaining Auditors
  - Higher security perception yields additional business

Pivot Point SECURITY

Gaining Management Approval: Cost & Impact

- Preparation: $0 (internal resources) – $120K+ (consultant(s))
  - Drivers are Scope/Gap/Speed/Resource Availability
  - Control short-term cost and complexity with initial scope control
- Certification (Registrar): Certification Audit: $15K – 50K+
  - Driver is scope (e.g., ISMS complexity, number of locations)
- Ongoing 27K Maintenance
  - ISMS Internal Audit: $0 (internal) – $10K+ (consultant(s))
  - Surveillance Audit: ~70% of the cost of Certification Audit
- Other “Hard Costs” are generally minimal

Pivot Point SECURITY

Gaining Management Approval: Cost & Impact

- Impact on IT, Infosec, and Other Functions
  - Project Lead Impact is notable at points, additional work effort is pretty distributed cross organizationally. Minor impact on sporadic basis.
- Minor impact on Management - risk management and governance -"Tone at the Top" is critical
- Additional InfoSec Staffing not typically required as work effort is relatively distributed and savings often offset ISMS overhead
- Impact on Employees & Clients
  - Generally minor, ISO is non-prescriptive so there is flexibility

Pivot Point SECURITY

Project Execution: Building Your Team

- Key Decision Points for Registrars
  - FTE's versus 1099's, vertical experience, additional attestation requirements (e.g., SOC2, PCI, FedRAMP, ISO-9001, HITRUST), cost, experience of the auditor assigned to your project, familiarity with selected consultant
- Key Decision Points for Consulting Companies/Consultants
  - FTE's versus 1099's, vertical experience, additional security/attestation requirements (e.g., pen testing, code review, SOC2, PCI, FedRAMP, ISO-9001, HITRUST), cost, experience/cultural fit of the consultant(s) assigned to your project, familiarity with selected registrar and auditor
- Key Decision Points for Internal Team
  - Experience implementing ISMS's, operations expertise, risk assessment experience, open-minded, likeable, ability to communicate at a business and technical level

Pivot Point SECURITY

Project Execution: Minimize Risk

- Timeline
  - Typically 6 – 18 Months; under-promise and over-deliver, it will take longer than you think (urgent trumps important)
  - If necessary, develop an interim attestation strategy (e.g., pen test, AUP, engagement letter)
- Scope
  - Only as broad as absolutely necessary to satisfy stakeholder request (boiling the ocean isn't a good option). Think scope expansion during surveillance audits from the start
- Integration
  - 27K is the superset of all regulatory compliance frameworks
  - Factor in other attestation that may be needed (SOC2, FedRAMP, PCI HIPAA)
- Participation is Important
  - If using consultants, ensure that you are integral to the project – it's important that your culture and current processes are reflected in your ISMS

Pivot Point SECURITY

Success Post Certification

- Risk is Everything
  - Evolve your Risk Management capacity; your ISMS is only as good as your risk assessment
- Operations Trumps Security
  - Support your “CSO” with strong operations capability; 27001 is an ongoing process
- Optimize Your ISMS Scope
  - Opportunistically extend scope in accordance with evolving client/business objectives
- Monitor, Respond, Improve
  - Ideally your ISMS Internal Audit isn’t something you do because you have to …. It’s something you do to improve your ISMS and more effectively manage risk
  - Make Incidents meaningful – learn from each one
- Do We Have Related Information/Business Risks That Are Not Well Managed?
  - IT Continuity, Business Continuity, Service Delivery Management, etc.

Where to turn.

John Verry, Principal
john.verry@pivotpointsecurity.com
732.267.6324
www.pivotpointsecurity.com

PivotPoint SECURITY