

# ISO 27001 for 2020



**Key Steps to Make 2020 a Success**

---

**A third party attested, robust  
Information Security Management System (ISMS)  
built around the  
ISO 27001 framework  
can be the key to success in 2020 and beyond**

---

# Good News 27001 provides Answers to the Issues you're facing in of 2020

- COVID-19
- CMMC & NIST SP 800-171
- The rise of Privacy
- Rising Client Expectations around Privacy/Security (Data Privacy Addendums, Vendor Due Diligence Questionnaires, Business Associate Agreements)

**++ pressure from clients/partners to prove privacy/security**

# Two Common Approaches



## Option #1 – Horse before the cart

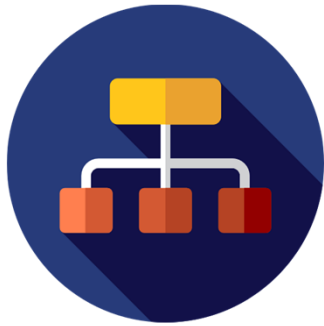
- Implement the Management System
- Gap Assess the Controls
- Close Gaps
- Get Certified



## Option #2 – Cart before the horse

- Gap Assess the Controls (how far am I right now?)
- Close the gaps
- Implement the Management System
- Re-tune the controls to reflect the Management System

# The 2 Elements of ISO 27001

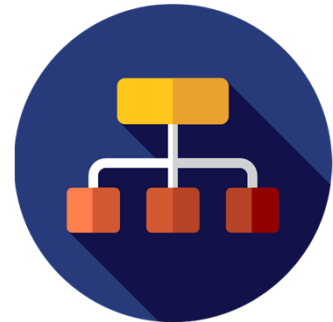


**Management System (ISO-27001)**



**Technical Controls (Annex A – ISO-27002)**

# The Management System



## 7 Clauses of ISO-27001

- **Context:** What info are we protecting? Why?
- **Leadership:** Who is responsible to make it happen?
- **Planning:** What is our plan to manage information related risk? Why/How did we arrive at that plan?
- **Support:** What actions and resources do we need to commit to making the plan a reality?
- **Operation:** Who/How/When/Where are we going to operate it?
- **Performance Evaluation:** How do we know it is working?
- **Improvement:** How do we get better YoY?

# The Controls



## 14 Domains of ISO-27002/Annex A

- **5. Information Security Policies**
- **6. Organization of Information Security ... structure and MDM**
- **7. Human Resource Security – Screening, Security Awareness Training, Term**
- **8. Asset Management – Responsibility, Info Classification, Media handling**
- **9. Access Control – PW's, User Account Management. Needs to know**
- **10. Cryptography – Encryption**
- **11. Physical/Environmental – Locks, utilities, equipment protection on/off**

# The Controls



## 14 Domains of ISO-27002/Annex A

- **12. Operation Security- Malware, Backups, Logging and monitoring, Technical vulnerability & configuration management**
- **13. Communication security – NW security & Information transfer**
- **14. System acquisition, development and maintenance – SDLC**
- **15. Supplier relationships – Vendor Risk Management**
- **16. Information security incident management (your IRP)**
- **17. Information security aspects of business continuity management (your BCP)**
- **18. Compliance – Legal/contractual requirements & Infosec reviews**



# The Process (optimally)



## Typically looks like

- Establish Scope
- Risk Methodology, Risk Assessment, Risk Treatment Plan
- Gap Assess Controls against Plan
- Prioritized Gap Remediation Plan
  - Management System
  - Controls
- ISMS Internal Audit
- Corrective Action Plans & Management Review
- Stage 1 Certification Audit (Management System focused)
- Stage 2 Certification Audit (Controls focused)

# Key Questions

*Do you have the right pieces in place?*



Have clear answers to these questions before you begin your ISO 27001 efforts:

- **Do I have the internal staff to stand up an ISMS?**
  - Expertise?
  - Availability?
- **What is my opportunity cost of remaining uncertified? Will I realize an ROI?**
  - Clients lost
  - Clients gained
  - Breach exposure
  - Other alternatives (SOC2, NIST/FISMA)
- **Is the timing right?**

# Issues you're facing in of 2020

- **COVID-19 – Now? “Post” COVID-19?**
  - **Business Continuity**
  - **Vendor Risk Management/Supply Chain**
- **CMMC & NIST SP 800-171**
  - **Defense Industrial Base**
  - **PROVE you are compliant**
- **The rise of Privacy**
  - **GDPR & CCPA & APAC & XXXX**
  - **Rising Client Expectations around Privacy/Security (Data Privacy Addendums, Vendor Due Diligence Questionnaires, Business Associate Agreements)**
  - **ISO-27701: Convert your Information Security Management System (ISMS) to an Information Security & Privacy Management System (ISPMS)**

# Questions?