Qualsys

ISO 27001 – Its all about the CIA

Why?

Remember the benefits:

- ✓ Keeps confidential information secure
- ✓ Provides customers with confidence in how you manage risk
- ✓ Allows for secure exchange of information
- ✓ Ensure you are meeting legal obligations
- ✓ Manages and minimises exposure to risk
- ✓ Brings a culture of security
- ✓ Protects the company, assets, shareholders and directors.
- ✓ Provides a competitive advantage
- ✓ Enhanced customer satisfaction
- ✓ Consistency in delivery of service
- ✓ Enhances cyber security

What?

Information security management is about preserving the confidentiality, integrity and availability of information and any associated information processing facilities.

It ensures business continuity by minimizing business damage by preventing and reducing the impact of security incidents.

- Confidentiality – Information is not made available or disclosed to unauthorised individuals, entities or processes.
- Integrity – safeguarding the accuracy and completeness of information.
- Availability – ensuring the accessibility and usability of information upon demand by an authorised entity.

Confidentiality
Integrity
Availability

What are your biggest challenges??

Common challenges

- Cultural change
- Lack of buy-in from Senior Management
- Understanding the concepts
- Overcomplicating the process
- ‘its not relevant to us’
- Staff competence
- Risk Assessment and Treatment

Do you have these data management processes?

New policies

- Over the next couple of weeks the following policies will be published. Please remember that these relate to the security of information,
  - Acceptable Use Policy
  - Access Control Policy
  - Backup Policy
  - Change Management Policy
  - Data Protection Policy
  - Encryption Policy
  - Equipment Security Policy
  - Exchange of Information Policy
  - Hiring and Termination Policy
  - Information Classification, labelling and handling Policy
  - Management of Removal Media Policy
  - Network Management and Security Policy
  - Patch Management and Software Update Policy
  - Physical Security Policy

How mature is your data management strategy?

Top tips

- Increased awareness around information security:
  - Clear desk and Lock screen
  - Encrypted laptops
  - No tailgating
  - Train, communicate and re-train
- Enhanced management of changes:
  - Infrastructure changes
  - Access changes New starters, leavers and role changes
  - Operational changes
- Management of Security Incidents:
  - Potential and nr miss – Security Incident Issue; tie in with GDPR
- Strict Supplier Management:
  - New or changing suppliers
- Use building blocks

Any questions?

Qualsys