What are the 10 most common non-conformances identified at an annual ISO 27001 surveillance audit?

Have you put the right policies, procedures and controls in place to protect your organisation against information security risks? Everyday valuable data is at risk of being hacked, corrupted, lost or accessed by the wrong personnel. Here are the top 10 information security failings identified by ISO 27001 in today's business:

1. **Implement a process for monitoring Information Security risks** – To ensure risks are identified, managed and ideally avoided it is important that you create either a Risk Register or a similar formalised process to enable evidence-based decisions to be made in response to the risks that are identified.

2. **Conduct training and provide evidence of staff competency** – For an organisation to demonstrate staff competency and reduce internal risks they should consider introducing Role Specifications and/or Job Descriptions, Induction Checklists and Staff Handbooks. These can help to outline your Organisation's expectations for staff to demonstrate appropriate levels of Information Security awareness, training and/or experience, in accordance with role.

3. **Ensure you have a robust recruitment process** – The Recruitment Process should determine the selection of new recruits based on appropriate education, training, or experience to include Information Security responsibilities of that role.

4. **Put a process in place for the secure destruction of information and data** – An organisation that takes Information Security seriously should have a defined process for the secure destruction of information and data that includes electronic media, physical media, confidential documentation and records of the disposals that have taken place.

5. **Introduce regular and structured training programmes** – Although some staff may have received training within your Organisation, this is usually not specific to the subject and can be provided using various sources that are not approved. Therefore, it is very important that Information Security awareness training is carried out in a structured way.

6. **A Business Continuity Plan and/or Disaster Recovery Plan** – Having one of these plans developed and approved, that references the continuity of Information Security processes in the event of a disruptive incident, can be critical to the ongoing security of information and data in today's business.

7. **A system that records Information Security failings** – The recording of Information Security failings is critical if you want to identify, overcome and prevent future threats to your Organisation and avoid any result and damage to your brand's reputation. An Incident Reporting system can be used to record responses to Information Security events, incidents and non-conformances during operation of an Information Security system.

8. **Establish an Information Exchange agreement** – Increase customer confidence in your Organisation's handling of their private data with an Information Exchange agreement. The agreement governs the transmission of information and data between your Organisation and your customers. In particular it specifies what, why and how customer information is collected and processed, how long it is kept for and how it is securely removed from your records.

9. **Develop Information Security Management System policies** – A set of policies that match your Organisation's intentions towards the management of Information Security make it clear what your customers and employees can expect. These policies should be made available both internally and externally.

10. **Define and Document legal requirements** – Using either a Legal Register or an approved provider document any relevant legal, regulatory, statutory and other requirements that your Organisation must follow.

Don't struggle alone, let QMS help you implement an ISO 27001 Management System to manage all of these areas and protect your business' reputation.