DOCUMENT MANAGER

Dm

www.document-manager.com

DOCUMENT MANAGEMENT
IMAGING & CAPTURE
WORKFLOW/BPM
CONTENT MANAGEMENT

BPM Strategies:

Trusting the process

Management:

Vendor compliance

Data privacy:

Protecting sensitive content

Enterprise Content Management:

8 best practices for 2024

OPINIONS • REVIEWS • CASE STUDIES • INTERVIEWS

ISSN 1351-3222 Vol 32 No 2 March/April 2024

Non-compliance is not an option

Vendor compliance isn't just about meeting standards; it's about protecting your business and stakeholders, explains Daniel Clark, Quality and Compliance Manager at Storetec

Vendor compliance is a vital consideration for businesses entrusting their document management needs to external providers. At Storetec, we understand the balance between cost efficiency and maintaining uncompromised quality, security, and compliance standards.

In this guide, we delve into the intricacies of evaluating vendor compliance and provide a detailed checklist to aid in your decision-making process.

WHY VENDOR COMPLIANCE MATTERS

Before delving into the checklist, it's crucial to understand why vendor compliance is non-negotiable. In an era where data breaches and compliance failures can have far-reaching consequences, entrusting critical business information to a non-compliant vendor poses significant risks.

Compliance ensures that vendors adhere to industry standards, legal regulations, and best practices, safeguarding your data and reputation. In the event of a legal dispute, this could prove crucial in protecting your business by demonstrating that you have carried out the necessary due diligence. The following points are all key compliance considerations when choosing a provider.

1. Certifications

One of the primary indicators of vendor compliance is certifications. However, not all certifications hold equal weight. It's essential to look beyond surface-level claims and verify the legitimacy of certifications. Certifications such as BS10008, ISO9001 and ISO27001 signify adherence to authenticity and admissibility, quality, and security. Many companies may claim to work in line with these standards but do not hold formal certification. Ensure that these certifications are formally issued and validated by a reputable organisation governed by

the United Kingdom Accreditation Service (UKAS).

The following certifications represent the bare minimum standards to look for in a digital provider, encompassing quality, security, and legal admissibility.

ISO9001 Quality Management - This certification signifies adherence to quality management systems. It ensures that the provider follows stringent quality control processes, resulting in consistent service delivery and customer satisfaction.

ISO27001 Information Security - This certification focuses on information security management systems. It demonstrates the provider's commitment to safeguarding sensitive information both physically and digitally, including data confidentiality, integrity, and availability.

BS10008 Legal Admissibility of Electronic Information - This certification requires strict adherence to procedures, particularly concerning data authenticity. In the event of legal proceedings, authenticity becomes vital. It's crucial for buyers to conduct due diligence and demand proof of formal certification rather than mere 'alignment with' BS10008 standards with no formal validation of compliance.

ISO22301 Business Continuity - Outsourcing critical processes necessitates assurance that the vendor possesses resilient systems. Business continuity and resilience are vital aspects, especially considering the potential risks of disasters. Robust procedures must be in place to minimise risks and have appropriate backup measures in case of emergencies, whilst ensuring continuity of service with the protection of client information and data the main priority.

Cyber Essentials Plus - This certification is essential for any vendor handling sensitive data. While Cyber Essentials involves self-assessment without third-party validation, Cyber Essentials Plus includes audits and system checks to validate security measures via a reputable third-party auditor. It includes robust scans and testing of our external facing IP addresses to identify potential vulnerabilities and ensure best practice security measures are in place to safeguard against cyber threats.

2. Independent penetration testing

Independent penetration testing is a critical step in evaluating the security measures of a digital provider. Unlike standard compliance certifications, this testing involves professional hackers attempting to breach the system using advanced methods, providing a comprehensive assessment of vulnerabilities.

This rigorous evaluation, conducted by government approved third-party cyber firms, ensures that any potential weaknesses are identified and addressed promptly, demonstrating the vendor's confidence in their system, commitment to safeguarding client data, and upholding the highest standards of security.

3. Operational site visits

Before entrusting sensitive information to a third-party provider, it's necessary to conduct operational site visits to assess their onsite security measures. While certifications and assurances may tick certain boxes, physically inspecting the premises provides invaluable insights into the provider's security protocols.

At Storetec, we advocate for due diligence audits on supplier premises prior to contract awarding. Websites can be misleading, and first-hand observation is essential to ensure alignment with security standards. We welcome and encourage site visits to showcase our facility, operations, and dedicated employees. Our commitment to transparency underscores our dedication to providing clients with peace of mind regarding the security of their data.

4. Validation

Ensuring the validity of certifications is vital when selecting a digital provider. Here's how to validate certifications effectively.

In the UK, the United Kingdom Accreditation Service (UKAS) is the government-appointed accrediting body to assess and accredit organisations that provide certification services. UKAS plays a crucial role in auditing certifying bodies to ensure adherence to rigorous standards, however, not all certification bodies are accredited by UKAS, so it's important to question the legitimacy of these organisations.

When evaluating scanning companies' certifications, it's essential to consider how they obtained those certifications. While any company can claim to be an awarding body and provide certifications, the credibility of these certifications lies in the accreditation process. For ISO and British Standards, certification from a UKAS-accredited body holds significant weight due to its government validation, ensuring adherence to internationally recognised standards.

To verify the authenticity of certifications held by scanning companies, public registers serve as valuable resources. Websites such as those provided by BSI Group, UKAS CertCheck, and IASME offer transparency and facilitate the verification process. By utilising these resources, businesses can ensure that their chosen vendor holds valid and reputable certifications.

OTHER CONSIDERATIONS

ISO14001 Environmental Sustainability - Look for suppliers who prioritise environmental sustainability and have obtained ISO14001 certification. A commitment to sustainability, including a Net Zero plan, demonstrates alignment with government initiatives and reflects shared core values.

Frameworks - Assess whether the supplier is accepted onto industry frameworks that impose stringent requirements for security, quality, and other key aspects. Being part of recognised frameworks can indicate a commitment to meeting industry standards and best practices.

> "IN AN ERA WHERE DATA BREACHES AND COMPLIANCE FAILURES CAN HAVE FAR-REACHING CONSEQUENCES, ENTRUSTING CRITICAL BUSINESS INFORMATION TO A NON-COMPLIANT VENDOR POSES SIGNIFICANT RISKS. COMPLIANCE ENSURES THAT VENDORS ADHERE TO INDUSTRY STANDARDS, LEGAL REGULATIONS, AND BEST PRACTICES, SAFEGUARDING YOUR DATA AND REPUTATION. IN THE EVENT OF A LEGAL DISPUTE, THIS COULD PROVE CRUCIAL IN PROTECTING YOUR BUSINESS BY DEMONSTRATING THAT YOU HAVE CARRIED OUT THE NECESSARY DUE DILIGENCE."

Case Studies, Testimonials, Reviews - Evaluate the supplier's credibility by reviewing case studies, testimonials, and reviews from previous clients. Positive feedback and success stories provide valuable insights into the supplier's track record and ability to deliver on promises.

Transparency and Communication - Don't hesitate to ask questions and engage in discussions about the supplier's processes, security measures, and environmental initiatives. A reputable provider should be transparent and willing to address any concerns, demonstrating a commitment to open communication and collaboration.

Consequences of non-compliance
Neglecting to prioritise thorough due diligence and compliance in selecting a document management supplier can have severe consequences for businesses. Some potential outcomes include:

ICO Fines on GDPR Penalties - Non-compliance with GDPR regulations can result in significant fines imposed by the Information Commissioner's Office (ICO). Failure to protect sensitive data adequately can lead to costly penalties that impact financial stability and reputation.

Financial Loss and Risks - Choosing a supplier solely based on cost without considering compliance and security measures may seem like a short-term gain. However, it can expose businesses to substantial financial losses and risks in the long run. Investing in a compliant supplier is an essential strategy to mitigate future financial loss and safeguard business interests.

Data Ransom - Inadequate security measures can leave businesses vulnerable to ransomware attacks, where cybercriminals encrypt sensitive data and demand payment for its release. Many businesses find themselves with no other option but to pay the ransom to regain access to critical information, especially where appropriate backup copies have not been maintained, resulting in financial losses and reputational damage.

Cyber Attacks - Failing to prioritise security measures can increase the risk of cyber-attacks, including malware infections, data breaches, and system compromises. Such attacks can disrupt operations, compromise sensitive information, and lead to legal liabilities and reputational harm.

A LONG-TERM INVESTMENT

In conclusion, vendor compliance is a multifaceted aspect of document management that requires careful consideration and thorough evaluation. By following this comprehensive checklist and prioritising compliance, you can ensure that your chosen vendor meets the highest standards of quality, security, and legal compliance.

Remember, investing in a compliant vendor is an investment in the long-term success and security of your business.

More info: www.storetec.net