netdocuments®

VENDOR SECURITY VALIDATION CHECKLIST

Why should I evaluate vendors or potential vendors, SaaS providers, and other third parties based on security best practices?

Cyber attacks against businesses represent one of the top three threats to the US economy, which means that keeping your data safe should be a major priority. But when you rely on third parties to support your business, you can open your company (and even your customers) to risk. For this reason, it's incredibly important to ensure that your third-party partners are up to par with security best practices.

While some vendors and other partners may open you up to risk, reputable third-party partners can provide additional security capabilities and controls as part of their service, so you don't have to manage security requirements by yourself. This allows you to leverage your vendor's expertise with the comfort that they're complying with best practices (and helping you stay compliant as well). For example, the NetDocuments platform provides state-of-the-art security infrastructure and comprehensive governance protocols so our clients can rest easy knowing their data is backed up, secured, and protected.

What are the risks of ignoring security best practices, especially with vendors, SaaS providers, and other third parties?

New security threats are always evolving, which means your company is already potentially vulnerable to a wide range of risks: hacking, employee mistakes, phishing, malware, etc. When you partner with vendors and other third parties who are not implementing and following appropriate security guidelines, you open the door to their security weaknesses as well. Any data, content, or other material they touch could be at risk. Because of this, it's critical that you hold your vendors to the highest standards of security and ensure that they're following industry best practices for the types of services they offer.

What security practices should I ask about when talking with vendors, SaaS providers, etc.?

When discussing security with vendors, SaaS providers, and other third parties, there are four major areas you'll want to discuss: (1) Platform architecture and encryption, (2) application security, (3) application certification, and (4) operations. Best practices for each of these areas are as follows:

	Best Practice	Value
Platform Architecture and Encryption	Implementing industry best practices	*Increased stability, better security protections, faster innovation rates*
	Multi-Level Encryption	*More keys is more protection, with control for specific client mandates of the firm*
	Hardware Security Module (HSM)	*Maximize encryption key security and minimize risk of compromise*
	Virus, Malware, and Ransomware Protection	*Industry experts recognize that Data Isolation is safer than detection*
Application Security	Federated Identity to reduce user authentication risk	*Default configuration should follow industry standards to reduce misconfiguration risk*
	Application Integration Authentication	*Confirms secure connections and shared data security*
Application Certification	Independent audits and certifications	*Reduced risk and improved responsiveness to client and government compliance requirements*
	Regular testing	*Validation of implemented controls and processes*
Operations	Separation of duties	*Reduce risk from personnel*

Review these best practices with your existing vendors, and always include them as part of your evaluation of new third party partners.

What should I do if a vendor doesn't meet these standards?

Ideally, every vendor would comply with security best practices. However, that's not always the case. If a vendor is not current with security best practices, it's up to you to determine whether you want to begin or continue your working relationship. Follow-up questions to ask to help with this decision might include:

- How does this vendor impact my security position? What data, content, or other materials do they have access to?
- What would happen to my organization if they were compromised? How would my clients, reputation, etc., be impacted?
- What security practices, capabilities, and controls have they implemented?
- Do they have a disaster recovery plan?
- Do they have plans to become compliant with security best practices? If so, when?
- Are they willing to work towards compliance with best practices?

Tactical Checklist for Validating Security Standards

Use this form to evaluate vendors, SaaS providers, and other third parties for security best practices.

Vendor: ____________________

	Best Practice	Vendor Response
Platform Architecture and Encryption	Implementing industry best practices	
	Multi-Level Encryption	
	Hardware Security Module (HSM)	
	Virus, Malware, and Ransomware Protection	
Application Security	Federated Identity to reduce user authentication risk	
	Application Integration Authentication	
Application Certification	Independent audits and certifications	
	Regular testing	
Operations	Separation of duties	

Specific Industry Standards

	Regulatory Domain	Value to Customer	Vendor Response
Broadly Applicable	ISO 27001	*Ensures that controls are in place to protect customer data in compliance with the de facto international standards for Information Security Management, managing PII in the cloud, and the implementation of controls for cloud-based service organization.*	
	ISO 27018		
	ISO 27017		
	U.S. Privacy Shield	*Required for legal data transfers between U.S. and EU.*	
	Type 2 SOC 2 | SOC 2+	*Ensures that controls for one or more of the Trust Service Criteria (Security, Availability, Processing Integrity, Confidentiality, or Privacy) are in place and effective over time.*	
	FIPS 140-2 Level 3	*Ensures that cryptographic keys are held in physically secure mechanisms that meet U.S. Government standards for ability to detect and prevent access or modification attempts.*	
United States Government	FedRAMP	*Ensures that cloud computing services meet a single consistent U.S. Government standard for security.*	
Industry Specific	HIPPA / HITECH	*Ensures that controls are implemented to protect personal and health information.*	
	FINRA/SEC 17a-4	*Ensures compliance with SEC regulations for data retention, indexing, and accessibility*	
Region or Country	EU GDPR	*Facilitates and ensures compliance with EU regulations governing the data privacy rights of personal data subjects.*	
	EU Model Clauses	*The EU model clauses are optionally available in GDPR processing addenda, and ensure that data transfers meet the requirements of the EU Data Protection Directive.*	
	Australia CCSL	*Recognizes compliance with Australian Government Information Security Policies.*	

[1] SOC 2+ is a specific set of additional security controls identified by a U.S. Financial Services working group including Goldman Sachs, Citibank, JP Morgan, AMEX, and others.

[2] FedRAMP audit starts with assessment in 2019 and w full audit in 2020.

Tactical Checklist for Validating Security Standards

NetDocuments' Responses

How NetDocuments is addressing security best practices.

Vendor: netdocuments®

	Best Practice	Vendor Response
Platform Architecture and Encryption	Implementing industry best practices	NetDocuments actively monitors evolving security standards and regularly implements improved controls and procedures, validated by independent audits
	Multi-Level Encryption	Each file stored in the NetDocuments Service is automatically protected by two separate AES 256 encryption keys and optionally by a third, customer-controlled, AES 256 encryption key
	Hardware Security Module (HSM)	Master encryption keys and customer managed keys are securely stored in HSMs
	Virus, Malware, and Ransomware Protection	All endpoint devices have active virus, malware, and ransomware protection; all production environments have multiple re-enforcing security controls protecting against viruses, malware, and ransomware
Application Security	Federated Identity to reduce user authentication risk	The NetDocuments Service fully supports SAML 2.0 so customers may implement their own federated identity solutions
	Application Integration Authentication	Robust API for authenticated integration
Application Certification	Independent audits and certifications	Annual Type 2 SOC 2 audits for Security, Availability, and Privacy; current ISO 27001 certification; see full list below
	Regular testing	Independent audits take place each year
Operations	Separation of duties	Developers do not have access to I.T. Production environments; I.T. does not have access to development services

Specific Industry Standards

	Regulatory Domain	Value to Customer	Vendor Response
Broadly Applicable	ISO 27001	*Ensures that controls are in place to protect customer data in compliance with the de facto international standards for Information Security Management, managing PII in the cloud, and the implementation of controls for cloud-based service organization.*	Certified
	ISO 27018		Certified
	ISO 27017		Certified
	U.S. Privacy Shield	*Required for legal data transfers between U.S. and EU.*	Certified
	Type 2 SOC 2 | SOC 2+	*Ensures that controls for one or more of the Trust Service Criteria (Security, Availability, Processing Integrity, Confidentiality, or Privacy) are in place and effective over time.*	Annual Audit
	FIPS 140-2 Level 3	*Ensures that cryptographic keys are held in physically secure mechanisms that meet U.S. Government standards for ability to detect and prevent access or modification attempts.*	Certified
United States Government	FedRAMP	*Ensures that cloud computing services meet a single consistent U.S. Government standard for security.*	Assessment in 2019
Industry Specific	HIPPA / HITECH	*Ensures that controls are implemented to protect personal and health information.*	Attestation
	FINRA/SEC 17a-4	*Ensures compliance with SEC regulations for data retention, indexing, and accessibility*	Attestation (self)
Region or Country	EU GDPR	*Facilitates and ensures compliance with EU regulations governing the data privacy rights of personal data subjects.*	Attestation
	EU Model Clauses	*The EU model clauses are optionally available in GDPR processing addenda, and ensure that data transfers meet the requirements of the EU Data Protection Directive.*	Available
	Australia CCSL	*Recognizes compliance with Australian Government Information Security Policies.*	Evaluating

[1] SOC 2+ is a specific set of additional security controls identified by a U.S. Financial Services working group including Goldman Sachs, Citibank, JP Morgan, AMEX, and others.

[2] FedRAMP audit starts with assessment in 2019 and w full audit in 2020.

Ready to learn more?

netdocuments.com/demo

nd

netdocuments®