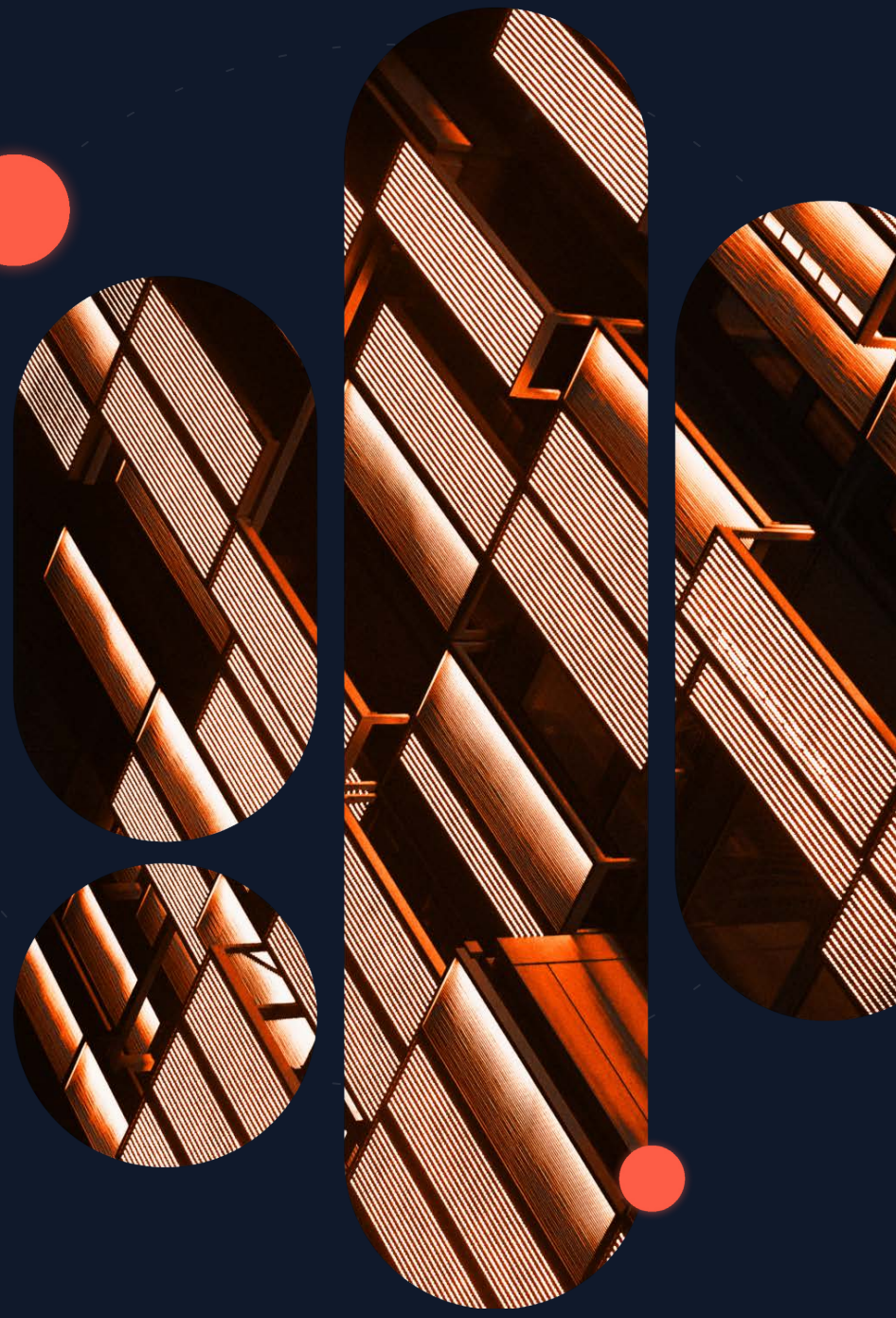
Dataweavers

Simple Security and Compliance Checklist for Sitecore

A multi-layered security posture for Sitecore is one step to building an effective platform. To uncover your potential risks, use our checklist to dive deeper on encryption, access controls, risk management, auditing & monitoring.



www.dataweavers.com

Key Requirement	Description	Approach (How to)		Have you implemented?	
				Yes	No
Encryption	Is the data used in the solution specifically PII data, encrypted in transit and at rest. Are they keys appropriately controlled.	**Transport Encryption**	In transit – SSL	☐	☐
		Encryption At Rest	At rest – TDE	☐	☐
		Secure key / cert management	Key Vault	☐	☐
Access Controls	Does the solution have suitable access controls in the application where roles and responsibilities are mapped. Does the solution at the infrastructure level have the appropriate access controls. Are enhanced identity solutions used including the use of MFA, to protect user credentials and access.	**Rolebased**	Extensive RBAC	☐	☐
		Isolate PII Data	Isolated Customer Data	☐	☐
		Advanced Identity	Azure AAD for CM with 2FA	☐	☐
Risk Management	Appropriately implemented Risk management framework, including assessment, controls, monitoring, improvement, training, and response. Alignment with Applicable Standards ISO27001 and/or SOC2 .	**Multilayer Network**	Defence in Depth	☐	☐
		Ongoing Review	Regular Control Review	☐	☐
		WAF	WAF Policies	☐	☐
		DDOS/BOT	BoT and DDOS Protection	☐	☐

This is a simple check list designed to help identify areas you may need to address in your Sitecore ecosystem. This does not replace a full assessment and you may need to evaluate your organizational compliance with specific industry standard you are looking to achieve.

Key Requirement	Description	Approach (How to)		Have you implemented?	
				Yes	No
Auditing	Application-level auditing / logging to record which users performed which actions. Infrastructure auditing to identify which processes or operational team members access and or modify infrastructure configuration. Data access auditing.	**Infrastructure Auditing**	Azure Auditing	☐	☐
		Solution Auditing	SQL Auditing	☐	☐
Monitoring	Suitable monitoring platforms and observability platforms that can provide advanced warning of security incidents and alerting, that can be actioned. This should cover the application layer, the underlying infrastructure layer, the network, and the ingress points.	**Application Alerts**	Application Insights	☐	☐
		Filtering	Intelligent Filtering	☐	☐
		Ongoing Scans	Defender for Cloud	☐	☐
		SIEM	Central NOC & Tooling	☐	☐

This is a simple check list designed to help identify areas you may need to address in your Sitecore ecosystem. This does not replace a full assessment and you may need to evaluate your organizational compliance with specific industry standard you are looking to achieve.

Did you answer “No” or you’re Not Sure?

If you answered “No” or you’re not sure about 3 or more questions in our checklist, it’s time to better understand your platform and its compliance requirements.

Discover how Dataweavers’ **Platform Operations** can help

Get started with our WebOps Assessment to unlock your potential.

Get Started

Dataweavers

www.dataweavers.com