


Simple Security and Compliance Checklist for Sitecore Websites

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.



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	<input type="checkbox"/>	<input type="checkbox"/>
		Encryption At Rest	At rest – TDE	<input type="checkbox"/>	<input type="checkbox"/>
		Secure key / cert management	Key Vault	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>
		Isolate PII Data	Isolated Customer Data	<input type="checkbox"/>	<input type="checkbox"/>
		Advanced Identity	Azure AAD for CM with 2FA	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>
		Ongoing Review	Regular Control Review	<input type="checkbox"/>	<input type="checkbox"/>
		WAF	WAF Policies	<input type="checkbox"/>	<input type="checkbox"/>
		DDOS/BOT	BoT and DDOS Protection	<input type="checkbox"/>	<input type="checkbox"/>

 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	<input type="checkbox"/>	<input type="checkbox"/>
		Solution Auditing	SQL Auditing	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>
		Filtering	Intelligent Filtering	<input type="checkbox"/>	<input type="checkbox"/>
		Ongoing Scans	Defender for Cloud	<input type="checkbox"/>	<input type="checkbox"/>
		SIEM	Central NOC & Tooling	<input type="checkbox"/>	<input type="checkbox"/>



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 Digital Roadmap Assessment to unlock your potential.

[Get Started](#)

