SOC2 compliance overview

CC3.3: Consider the potential for fraud

83%

Type	Applies the least privilege principle to cloud resources	Status
	Firewall rule prevents SSH access from anywhere	disabled
	Databases only allows trusted connections	complying
	Droplet prevent SSH from anywhere	disabled

Type	Applies the least privilege principle for cloud resource	Status
	Droplet firewall set up	failing

Type	Enabled security logging for cloud instances	Status
	Logging is enabled for resources	complying

Type	Requires MFA for cloud users	Status
	Users are logging in securely	complying

CC3.2: Estimate Significance of Risks Identified

88%

Type	Properly manages the identity of cloud users	Status
	Users are logging in securely	complying

Type	Does not have any severe surface monitoring issues	Status

	No active critical surface monitoring issues	complying
	No active high severity surface monitoring issues	complying

Type	Does not have any severe open source dependency issues	Status
	No active critical open source dependency issues	complying
	No active high severity open source dependency issues	complying

Type	Configured monitoring for code repositories	Status
	Configured monitoring for all code repositories	complying

Type	Configured monitoring for container images	Status
	Configured monitoring for all container images	complying

Type	Configured monitoring for domains	Status
	Configured monitoring for domains	failing

CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives

86%

Type	Properly manages the identity of cloud users	Status
	Users are logging in securely	complying

Type	Applies the least privilege principle for cloud resource	Status
	Firewall rule prevents SSH access from anywhere	disabled
	Databases only allows trusted connections	complying

	Droplet prevent SSH from anywhere	disabled
	Droplet firewall set up	failing

Type	Does not have any severe infrastructure as code issues	Status
	No active critical infrastructure as code issues	complying
	No active high severity infrastructure as code issues	complying

CC6.1: Restricts logical access

96%

Type	Requires MFA for cloud users	Status
	Users are logging in securely	complying

Type	Applies the least privilege principle to cloud resources	Status
	Firewall rule prevents SSH access from anywhere	disabled
	Databases only allows trusted connections	complying
	Droplet prevent SSH from anywhere	disabled

Type	Enforces encryption of data in transit	Status
	Load balancer SSL redirect enabled	complying
	Load balancer allows invalid HTTP headers	complying
	Elasticsearch domain might have outdated TLS version	complying
	DNSSEC is disabled	complying
	Load balancer is using outdated TLS policy	complying

{}	Cloud SQL db not enforcing SSL	complying
{}	Azure Storage Accounts does not enforce latest TLS version	complying
{}	AWS ElastiCache Replication Group should encrypt data in transit	complying
{}	Outbound Ansible connections are not encrypted	complying
{}	Outbound Ansible connections are not encrypted	complying
{}	Signature validation for dnf packages is off	complying
{PHP}	Laravel cookies can be sent unencrypted	complying
{PHP}	SSL certificate verification turned off during requests	complying
{JS}	Express is not emitting security headers	complying
{PHP}	Using potentially unsafe FTP connections to move data	complying
{JAVA}	Turning off TLS verification enabled MITM attacks	complying
{.NET}	Use of broken or outdated encryption	complying
{TS}	NodeJS talks to database without encryption	complying
{TS}	Insecure gRPC connection can lead to remote code execution	complying
{PY}	SSL certificate verification turned off during requests	complying
{JAVA}	Cookie missing HttpOnly flag	complying
{JAVA}	App uses an outdated TLS protocol	complying
{JAVA}	App does not validate SSL certificates properly	complying
{JS}	NodeJS talks to database without encryption	complying
{JS}	Insecure gRPC connection can lead to remote code execution	complying

{PY}	Using potentially unsafe FTP connections to move data	complying
{SWIFT}	Insecure TLS configuration detected	complying
{SWIFT}	Usage of deprecated or broken encryption detected	complying
{PYTHON}	Insecure usage of `requests` sends data over cleartext	complying
{.NET}	TLS Certificate Validation Disabled	complying
{.NET}	Deprecated SSL Protocol Usage Detected	complying
{JS}	Insecure websocket connection sends data over cleartext	complying
{C++}	Weak SSL/TLS protocols used	complying
{C++}	Server certificates are not verified during SSL/TLS connections	complying
{C++}	Server hostnames not verified during SSL/TLS connections	complying

Type	Encrypts data at rest	Status
	SQS queue data is not encrypted	complying
	Databases have encryption at rest	complying
	Docker image repository not encrypted at rest	complying
	SNS topics are not encrypted at rest	complying
	Elasticsearch domain is not encrypted at rest	complying
	AWS ElastiCache Redis cluster should have encryption at rest enabled	complying

Type	Prevents the exposure of sensitive data	Status
	Currently there are no exposed secrets	failing

Type	Has measures against SQL injection attacks	Status
{PHP}	Potential SQL injection via string-based query concatenation	failing
{PHP}	Potential SQL injection via string-based query concatenation using AuraSQL framework functions	complying
{PHP}	Potential SQL injection via string-based query concatenation	complying
{RUBY}	Potential SQL injection via string-based query concatenation	complying
{PHP}	Potential SQL injection via Laravel function	complying
{PHP}	Potential SQL injection via Drupal database functionality	complying
{PHP}	Potential SQL injection when bypassing Doctrine ORM with raw query	complying
{PHP}	Potential NoSQL injection via string-based query concatenation	complying
{JAVA}	Potential NoSQL injection via string-based query concatenation	complying
{JAVA}	Potential SQL injection via string-based query concatenation	complying
{TS}	Potential SQL injection via string-based query concatenation	complying
{JAVA}	Potential SQL injection via string-based query concatenation	complying
{JAVA}	Potential SQL injection through JDBC via string-based query concatenation	complying
{SCALA}	Potential SQL injection via string-based query concatenation	complying
{.NET}	Potential NoSQL injection via string-based query concatenation	complying
{TS}	NoSQL injection attack possible	complying
{JS}	NoSQL injection attack possible	complying
{JS}	Potential SQL injection via string-based query concatenation	complying
{JS}	Potential SQL injection in sqlite3 via string-based query concatenation	complying

{.NET}	Potential SQL injection via string-based query concatenation	complying
{PY}	Potential SQL injection when bypassing Django ORM with extra()	complying
{PY}	Potential SQL injection when bypassing Django ORM with RawSQL()	complying
{PY}	Potential SQL injection via string-based query concatenation	complying
{KOTLIN}	Potential SQL injection via string-based query concatenation	complying
{DART}	Potential SQL injection via string-based query concatenation	complying
{GO}	Potential SQL injection via string-based query concatenation	complying
{RUST}	Potential SQL injection via dynamic raw query construction	complying
{C}	Potential SQL injection via dynamic raw query construction	complying

Type	Is protected against SSRF attacks	Status
	EC2 IAM roles vulnerable to SSRF attacks	complying
	GCP Kubernetes engine clusters vulnerable to SSRF attacks	complying
{PHP}	HTTP request might enable SSRF attack	failing
{JAVA}	HTTP request might enable SSRF attack	complying
{JAVA}	HTTP request might enable SSRF attack	complying
{SCALA}	HTTP request might enable SSRF attack	complying
{TS}	Potential file inclusion attack via reading file	complying
{TS}	Potential file inclusion attack via file path construction	complying
{TS}	A timing attack might allow hackers to bruteforce passwords	complying
{TS}	User data used in Puppeteer methods can result in SSRF	complying

{JS}	HTTP request might enable SSRF attack	complying
{JS}	Potential file inclusion attack via reading file	complying
{JS}	Potential file inclusion attack via file path construction	complying
{JS}	User data used in Puppeteer methods can result in SSRF	complying
{PY}	Potential user input in HTTP request may allow SSRF attack	complying
{GO}	Simple DOS attack possible due to http.server misconfiguration	complying
{GO}	HTTP request might enable SSRF attack	complying
{GO}	Potential file inclusion attack via reading file	complying
{RUST}	Potential user input in HTTP request may allow SSRF attack	complying

Type	Is protected against command injections attacks	Status
{.NET}	Possible command injection via Process.Start	complying
{.NET}	Xpath injection attack could lead to information extraction	complying
{YAML}	Use of vulnerable ingress-nginx controller	complying
{GO}	Possible command injection via shell script	complying
{RUST}	Potential command injection via Command API	complying

Type	Prevents XSS attacks	Status
{PY}	Rendering unescaped input can lead to XSS attacks	complying
{PHP}	Rendering unescaped input can lead to XSS attacks	failing
{JS}	Using dangerouslySetInnerHTML in React can lead to XSS attacks	complying
{JAVA}	HttpServletRequest output can be used for XSS attacks	complying

{.NET}	Rendering unescaped input can lead to XSS attacks	complying
{JS}	Using v-html in Vue templates can lead to XSS attacks	complying
{JS}	Rendering unescaped input in EJS template can lead to XSS attacks	complying
{JS}	Rendering unescaped input in handlebar/mustache template can lead to XSS attacks	complying
{JS}	Rendering unescaped input in HTML template can lead to XSS attacks	complying
{JAVA}	Unsanitized user input leads to cross-site scripting (XSS)	complying
{JAVA}	Rendering unescaped input can lead to XSS attacks	complying
{PY}	Jinja2 template config can lead to XSS attacks	complying
{JS}	Using document write methods can lead to XSS attacks	complying
{ELIXIR}	Using raw on potential user input can leads to XSS	complying
{GO}	Rendering unescaped input can lead to XSS attacks	complying
{GO}	Directly writing unsanitized input to http.ResponseWriter can lead to XSS	complying

CC6.1: Consider network segmentation

86%

Type	Prevents unauthorized public access to file storage	Status
	S3 Buckets should have block public access globally	complying
	Azure Storage Account allow public access	complying
	Azure Storage blobs do not restrict public access for nested items	complying

Type	Prevents unauthorized access via ssh	Status
	Firewall rule prevents SSH access from anywhere	disabled

	Droplet prevent SSH from anywhere	disabled
	Firewall rules allow SSH from any public IP	complying

Type	Has separate production and test environments	Status
	No cloud environment used for mixed purposes (eg production and staging)	failing

CC6.1: Restrict access to information assets

100%

This section is available on any paid plan. Upgrade Now

Type	Has secured load balancer access points	Status
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]

CC6.1: Manages credentials for infrastructure and software

100%

This section is available on any paid plan. Upgrade Now

Type	Has secured load balancer access points	Status
	[illegible]	[illegible]

CC6.1: Use encryption to protect data

100%

This section is available on any paid plan. Upgrade Now

Type	Encrypts data at rest	Status
	[illegible]	[illegible]

[S]	Dock** ***** ***** *** ***** ** rest	complying
[S]	SNS ***** *** *** ***** ** rest	complying
[S]	Elas***** ***** ** *** ***** ** rest	complying
[S]	AWS ***** ***** ***** ***** **** ***** ** **** ***pted	complying

Type	Enforces encryption of data in transit	Status
[S]	SQS ***** **** ** *** *****pted	complying
[cloud]	Load ***** *** ***** ***pted	complying
[S]	Load ***** ***** ***** **** ***ders	complying
[S]	Elas***** ***** ***** **** ***** *** ***sion	complying
[S]	DNSS** ** ****pted	complying
[S]	Load ***** ** ***** ***** *** **tcy	complying
[S]	Clou* *** ** *** ***** SSL	complying
[S]	Azur* ***** ***** **** *** ***** ***** *** ***sion	complying
[S]	AWS ***** ***** ***** ***** ***** **** ** ***mit	complying
[S]	Outb**** ***** ***** *** *** *****pted	complying
[S]	Outb**** ***** ***** *** *** *****pted	complying
[S]	Sign***** ***** *** *** ***** ** oft	complying
[new]	Lang*** ***** *** ** **** *****pted	complying
[new]	SSL ***** ***** ***** *** ***** ****ests	complying
[w]	Expi*** ** *** ***** ***** ***ders	complying

[new]	Union* ***** ***** *** ***** ** **** data	complying
[secr]	Turn*** *** *** ***** ***** **** ***acks	complying
[ex]	Node** ***** ** ***** ***** *****tion	complying
[ex]	Inse**** **** ***** *** **** ** ***** **** *****tion	complying
[ex]	SSL ***** ***** ***** *** ***** ****ests	complying
[secr]	Cook** ***** ***** flag	complying
[secr]	App **** ** ***** *** ****ocol	complying
[secr]	App **** *** ***** *** ***** ****erly	complying
[ex]	Node** ***** ** ***** ***** *****tion	complying
[ex]	Inse**** **** ***** *** **** ** ***** **** *****tion	complying
[ex]	Union* ***** ***** *** ***** ** **** data	complying
[secr]	Inse**** *** ***** ****cted	complying
[access]	Inse**** ***** ** ***** ***** **** **** *****text	complying
[secr]	TLS ***** ***** ****sted	complying
[secr]	Depe***** *** ***** ***** ****cted	complying
[ex]	Inse**** ***** ***** ***** **** **** *****text	complying
[---]	Weak ***** ***** used	complying
[---]	Serv** ***** *** *** ***** ***** ***** *****ions	complying
[---]	Serv** ***** *** ***** ***** ***** *****ions	complying

Type	Uses up to date cryptography libraries	Status

[redacted]	Use ** ***** ** ***** *****tion	complying
[redacted]	Usag* ** ***** ** ***** ***** ****cted	complying
[redacted]	Usin* ***** ***** ****ary	complying
[redacted]	Hash** ***** ***** ** ***** salt	complying

CC6.6: Restrict Access

100%

This section is available on any paid plan. Upgrade Now

Type	Prevents public access to cloud resources	Status
[redacted]	Fire**** **** ***** *** ***** **** ****here	disabled
[redacted]	Dele***** **** ***** ***** *****tions	complying
[redacted]	Drop*** ***** *** **** ****here	disabled
[redacted]	Fire**** ***** ***** *** **** *** *****c IP	complying
[redacted]	S3 B***** ***** **** ***** ***** ***** ****ally	complying
[redacted]	Kube***** ***** ***** ** ****cyed	complying
[redacted]	Azur* ***** ***** ***** ***** ***** **cess	complying
[redacted]	Azur* *** ***** ***** ***** ***** **cess	complying
[redacted]	AKS *** ***** **** *** ***** ***** ** ** **nges	complying
[redacted]	Azur* ***** ***** ***** ***** **cess	complying
[redacted]	Azur* ***** ***** ** *** ***** ***** ***** *** ***** *tems	complying
[redacted]	Prof***** ***** ***** ***** ** *****prof	complying

CC6.6: Require additional authentication or credentials

100%

This section is available on any paid plan. Upgrade Now

Type	MFA is enforced for cloud users	Status
	[illegible]	complying

CC6.6: Implement boundary protection system

80%

This section is available on any paid plan. Upgrade Now

Type	Applies the least privilege principle for cloud resource	Status
	[illegible]	disabled
	[illegible]	complying
	[illegible]	disabled
	[illegible]	failing
	[illegible]	complying

CC6.7: Use encryption technologies or secure communication channels to protect data

100%

This section is available on any paid plan. Upgrade Now

Type	Enforces latest TLS version	Status
	[illegible]	complying
	[illegible]	complying
	[illegible]	complying

Type	Uses up to date cryptography libraries	Status
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying

CC6.8: Restrict application and software installation

100%

This section is available on any paid plan. Upgrade Now

Type	Protects unauthorized runtime access	Status
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying

Type	Prevents container orchestration takeover	Status
[redacted]	[redacted]	complying
[redacted]	[redacted]	complying

CC6.8: Detect unauthorized changes to software and configuration parameters

100%

This section is available on any paid plan. Upgrade Now

Type	Enabled security logging for cloud instances	Status
	[illegible]	complying
	[illegible]	complying

CC6.8 Use anti-virus and anti-malware software

100%

This section is available on any paid plan. Upgrade Now

Type	Akido Malware Scanner is enabled	Status
	[illegible]	complying

CC7.1: Monitor infrastructure and software

67%

This section is available on any paid plan. Upgrade Now

Type	Enabled security logging for cloud instances	Status
	[illegible]	complying
	[illegible]	complying

Type	Configured SLAs to resolve issues	Status
	[illegible]	failing

Type	Connected code repositories	Status
	[illegible]	complying

Type	Connected cloud environment	Status
	[illegible]	complying

Type	Connected public facing domain	Status
	[illegible]	failing

CC7.1: Implement change detection mechanism

100%

This section is available on any paid plan. Upgrade Now

Type	Alerting is enabled	Status
	[illegible]	complying

CC7.1: Detect unknown or unauthorized components

100%

This section is available on any paid plan. Upgrade Now

Type	Does not have risky licenses	Status
	[illegible]	complying

CC7.1: Conduct vulnerability scans

25%

This section is available on any paid plan. Upgrade Now

Type	Uses Lockfiles to pin code dependencies	Status
	[illegible]	failing

Type	Does not have any issues outside of their SLA	Status
	[illegible]	failing

Type	Connected code repositories	Status
	[illegible]	complying

Type	Connected public facing domain	Status
	[illegible]	failing

CC7.1: Implement filters to analyze anomalies

100%

This section is available on any paid plan. Upgrade Now

Type	Connected code repositories	Status
	[illegible]	complying

CC7.1: Restores the affected environments

100%

This section is available on any paid plan. Upgrade Now

Type	Runtimes are up to date	Status
	[illegible]	complying
	[illegible]	complying
	[illegible]	complying
	[illegible]	complying
	[illegible]	complying
	[illegible]	complying
	[illegible]	complying

Type	Has no critical open source dependency issues	Status
	[illegible]	complying

CC8.1: Protect confidential information

0%

This section is available on any paid plan. Upgrade Now

Type	Prevents the exposure of sensitive data	Status
	[illegible]	failing

CC8.1: Track system changes

0%

This section is available on any paid plan. Upgrade Now

Type	Tracks progress via an issue tracker	Status
	[illegible]	failing

CC10.3: Tests integrity and completeness of backup data

100%

This section is available on any paid plan. Upgrade Now

Type	Has backups for stateful cloud resources	Status
	[illegible]	complying
	[illegible]	complying