






# SOC2 compliance overview


## CC3.3: Consider the potential for fraud

100% 

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	complying

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	failing

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	complying


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

100% 

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	complying






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

 99% 






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



{DB}	Cloud SQL db not enforcing SSL	complying
{DB}	Azure Storage Accounts does not enforce latest TLS version	complying
{DB}	AWS ElastiCache Replication Group should encrypt data in transit	complying
{DB}	Outbound Ansible connections are not encrypted	complying
{DB}	Outbound Ansible connections are not encrypted	complying
{DB}	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
{JS}	Azure Network Security Rule allows plaintext HTTP connections	complying
{PYTHON}	Azure Storage Account allows plaintext HTTP connections	complying
{JS}	Azure Storage Account allows plaintext HTTP connections	complying
{PYTHON}	Azure Network Security Rule allows plaintext HTTP connections	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
<b>Type</b>	<b>Prevents the exposure of sensitive data</b>	<b>Status</b>
	Currently there are no exposed secrets	complying
<b>Type</b>	<b>Has measures against SQL injection attacks</b>	<b>Status</b>
{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
{RUST}	NoSQL injection attack possible	complying
{RUBY}	Potential SQL injection via string-based query concatenation	complying
{APEX}	Potential SQL injection via string-based query concatenation	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	complying

{JAVA}	HTTP request might enable SSRF attack	complying
{JAVA}	HTTP request might enable SSRF attack	complying
{SCALA}	HTTP request might enable SSRF attack	complying
{NET}	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	complying
{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
{JS}	Potential XSS due to enabling bypassSecurityTrustUrl	complying

<b>{RUBY}</b>	Disabling JSON HTML Escaping in ActiveSupport may lead to XSS	complying
<b>{GO}</b>	Directly writing unsanitized input to http.ResponseWriter can lead to XSS	complying

### CC6.1: Consider network segmentation



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
	S3 bucket grants public access to all contents	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



This section is available on any paid plan. [Upgrade Now](#)


Type	Has secured load balancer access points	Status
	Firewall rule prevents SSH access from anywhere	disabled

	Drupal access not secured	disabled
	Drupal access not secured	compliant

### 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
	User's not secured	compliant

### CC6.1: Use encryption to protect data

100% 

This section is available on any paid plan. [Upgrade Now](#)

Type	Encrypts data at rest	Status
	Data not encrypted	compliant
	Backup not encrypted	compliant
	S3 not encrypted	compliant
	EBS not encrypted	compliant
	API not encrypted	compliant


Type	Enforces encryption of data in transit	Status
	SQS not encrypted	compliant
	Load balancer not encrypted	compliant
	Load balancer not encrypted	compliant
	EBS not encrypted	compliant

<input type="checkbox"/>	CRISIS or emergency	<input type="checkbox"/>
<input type="checkbox"/>	Load issues or server issues and reply	<input type="checkbox"/>
<input type="checkbox"/>	Client not on the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	App not working on the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	API issues or server issues and the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	API issues or server issues and the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Outbound issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Outbound issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Signatures issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Log issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	SSL issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Export or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	User issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Temp issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Node issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Dev issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	SSL issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Cookie issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	App issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	App issues or the correct SSL	<input type="checkbox"/>
<input type="checkbox"/>	Node issues or the correct SSL	<input type="checkbox"/>








	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	

Type	Use up to date cryptography libraries	Status
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	
	Use up to date cryptography libraries	

### CC6.6: Restrict Access

100% 

This section is available on any paid plan. [Upgrade Now](#)

Type	Prevents public access to cloud resources	Status
	Prevents public access to cloud resources	disabled
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	disabled
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant
	Prevents public access to cloud resources	compliant

### 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



User's are secure on everything

complying

### CC6.6: Implement boundary protection system

100%

This section is available on any paid plan. [Upgrade Now](#)

Type	Applies the least privilege principle for cloud resource	Status
	Enforce least privilege on IAM roles	disabled
	Data encryption on S3 buckets	complying
	Disable IAM user access keys	disabled
	Disable IAM user MFA	complying
	User's are secure on everything	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
	Enforce TLS 1.2 on all connections	complying
	Load balancers use TLS	complying
	API's are secure on everything	complying

Type	Uses up to date cryptography libraries	Status
	Use up to date crypto libraries	complying
	User's are secure on everything	complying

[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant

### CC6.8: Restrict application and software installation

100% 

This section is available on any paid plan. [Upgrade Now](#)

Type	Protects unauthorized runtime access	Status
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant

Type	Prevents container orchestration takeover	Status
[icon]	[blurred text]	compliant
[icon]	[blurred text]	compliant

### 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
	Logg... on ...	complying
	Logg... on ...	complying

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



This section is available on any paid plan. [Upgrade Now](#)

Type	Aikido Malware Scanner is enabled	Status
	Malw... on ...	complying

### CC7.1: Monitor infrastructure and software



This section is available on any paid plan. [Upgrade Now](#)

Type	Enabled security logging for cloud instances	Status
	Logg... on ...	complying
	Logg... on ...	complying

Type	Configured SLAs to resolve issues	Status
	Conf... SLAs	not

Type	Connected code repositories	Status
	Conn... reposit...	complying

Type	Connected cloud environment	Status
	Conn... env...	complying

Type	Connected public facing domain	Status
	Connected public facing domain	complying

### CC7.1: Implement change detection mechanism



This section is available on any paid plan. [Upgrade Now](#)

Type	Alerting is enabled	Status
	Alerting is enabled	complying

### CC7.1: Detect unknown or unauthorized components



This section is available on any paid plan. [Upgrade Now](#)

Type	Does not have risky scanners	Status
	Does not have risky scanners	complying

### CC7.1: Conduct vulnerability scans



This section is available on any paid plan. [Upgrade Now](#)

Type	Uses Lockfiles to pin code dependencies	Status
	Uses Lockfiles to pin code dependencies	fail
Type	Does not have any issues outside of their SLA	Status
	Does not have any issues outside of their SLA	fail
Type	Connected code repositories	Status
	Connected code repositories	complying

Type	Connected public facing domain	Status
	Connected public facing domain	compliant

### CC7.1: Implement filters to analyze anomalies

100%

This section is available on any paid plan. [Upgrade Now](#)

Type	Connected code repositories	Status
	Connected code repositories	compliant

### CC7.1: Restores the affected environments

100%

This section is available on any paid plan. [Upgrade Now](#)

Type	Runtimes are up to date	Status
	Runtime is up to date	compliant
	Runtime is up to date	compliant
	Runtime is up to date	compliant
	Runtime is up to date	compliant
	Runtime is up to date	compliant
	No CVEs	compliant
	AWS	compliant

Type	Has no critical open source dependency issues	Status
	Has no critical open source dependency issues	compliant

### CC8.1: Protect confidential information



This section is available on any paid plan. [Upgrade Now](#)

Type	Prevents the exposure of sensitive data	Status
	Customer access via an access policy	compliant

### CC8.1: Track system changes



This section is available on any paid plan. [Upgrade Now](#)

Type	Tracks progress via an issue tracker	Status
	Customer access via an access policy	not compliant

### CC10.3: Tests integrity and completeness of backup data



This section is available on any paid plan. [Upgrade Now](#)

Type	Has backups for stateful cloud resources	Status
	Customer access via an access policy	compliant
	Customer access via an access policy	compliant