Cyber Risk Engineering Report for Carisma Solutions Private Limited

This report provides a detailed overview of key factors of Carisma Solutions Private Limited's overall security posture.

Assessment date

Jul 06, 2026

Generated date

Jul 6, 2026

Report for

Carisma Solutions Private Limited

Issued by

ICICI Lombard

This report has been generated using UpGuard. If you have any questions, please contact support@upguard.com.

Introduction

ICICI Lombard created this report on Carisma Solutions Private Limited on Jul 06, 2026 based on the following assets: {{EvidenceList}}.

These assets are created and stored on the UpGuard platform. UpGuard is a complete third-party risk and attack surface management platform that combines security ratings, security questionnaires, and risk assessments to provide a complete overview of a company’s security posture.

The results are summarized into a security rating, a numeric score for cybersecurity performance. Security ratings make it easy to compare organizations and assess performance over time.

To assist with remediation, the report unpacks the security rating into eleven underlying categories: Questionnaire, Website, IP/Domain Reputation, Encryption, Vulnerability Management, Attack Surface, Network, Email, Data Leakage, DNS, and Brand Reputation. Each category then outlines individual risks, domains & IPs impacted, and provides remediation recommendations. The most severe risks in each category appear first.

To improve Carisma Solutions Private Limited's security rating, focus on Questionnaire, Website, IP/Domain Reputation, Encryption, Vulnerability Management, Attack Surface, Network, Email, Data Leakage, DNS, and Brand Reputation risks.

How are UpGuard's security ratings calculated?

UpGuard uses advanced algorithms to determine the security posture of millions of organizations every day. As noted above, we use threat signals gathered from trusted commercial, open-source, and proprietary sources. We also support the use of targeted security questionnaires to more deeply assess the posture of an organization. These signals are grouped together to identify threats and issues in an attack surface that could result in a security incident. Signals we pay attention to include things like open ports, DNS configuration, known data breaches, and hundreds of other vectors including:

- Susceptibility to man-in-the-middle attacks
- Insecure SSL/TLS certificates
- SPF, DKIM and DMARC settings
- HTTP Strict Transport Security (HSTS)
- Email spoofing and phishing risk
- Vulnerabilities
- Malware susceptibility
- Open admin, database, and file sharing ports
- Exposure to known data breaches and data leaks
- Secure cookie configuration

Our ability to combine these signals in real-time is what makes UpGuard so effective: cybersecurity is a domain where small improvements can make a big difference. By following our suggestions you can reduce the risk of sensitive data exposures, leaked credentials, and other security incidents.

When assessing your security performance, we recommend beginning with your overall security rating. As a general rule of thumb, here is how our A-F ratings correspond to your security posture:

Our security ratings range from A to F:

A **801-950**
Organization has a robust security posture and good attack surface management.

B **601-800**
Organization has reasonable security controls in place but could have gaps in their security posture.

C **401-600**
Organization has poor security controls and has serious issues that need to be addressed.

D **201-400**
Organization has severe security issues and should not process any sensitive data.

F **0-200**
Organization has not invested in basic security controls and should not be used.

Any risks we find are given a severity rating from low to critical:

!!!! **Critical risks**
Critical risks or vulnerabilities that place the business at immediate risk of data breaches.

!!! **High risks**
Severe risks that should be addressed immediately to protect the business.

!! **Medium risks**
Unnecessary security risks that could lead to more serious vulnerabilities.

! **Low risks**
Areas of improvement to reduce risks and improve the business' security rating.

Assessment summary

OVERALL SECURITY RATING

B 735 / 950

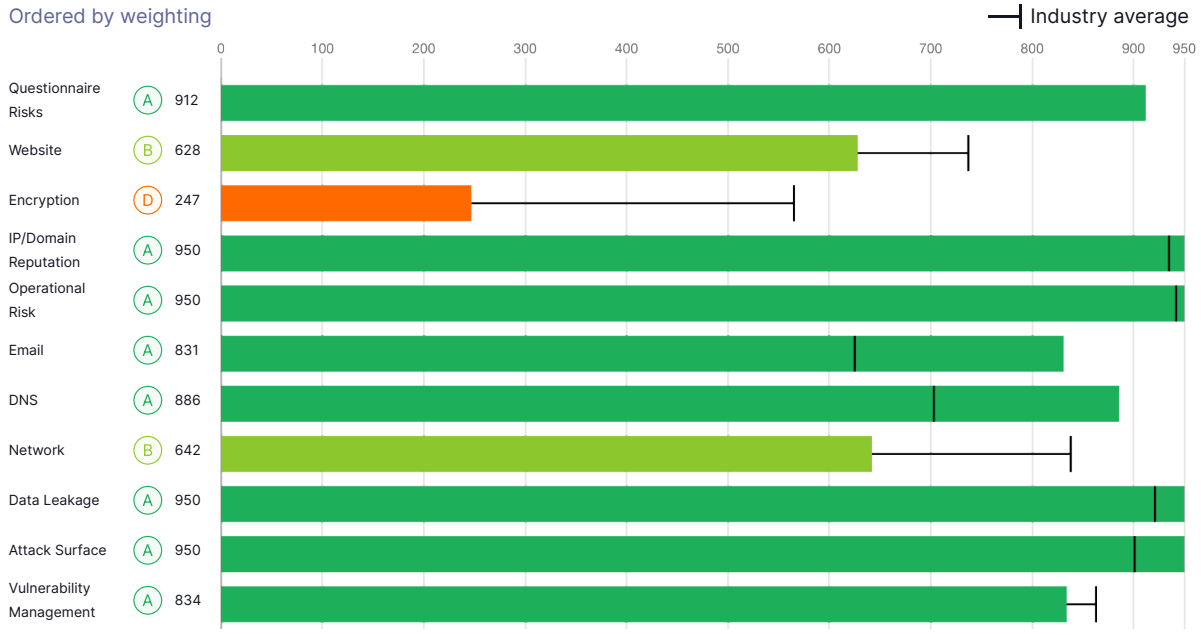
Carisma Solutions Private Limited has reasonable security controls in place but could have gaps in their security posture.

INDUSTRY AVERAGE

B 703

The average rating for companies in the Computer Hardware & Software industry.

Security rating by category



Security rating (last 12 months)



Key risks

These risks were highlighted as part of the risk assessment conducted on 06 Jul, 2026

Risk finding	Risk details
'FTP' port open Network	The 'FTP' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed. We recommend that the 'FTP' port be closed to reduce the attack surface.
SSL not available Encryption	SSL is the standard encryption method for browsing websites. Enabling SSL requires installing an SSL certificate on the site. Install valid SSL certificates on affected domains. Websites without valid SSL certificates are shown as 'non-secure' in modern browsers and will rank worse in Google and other search engines.
End-of-life version of WordPress detected Vulnerability Management	The detected version of WordPress is end of life. The product will likely not receive security updates from the vendor moving forward. Review the product and plan the necessary updates.
HTTP does not redirect to HTTPS Encryption	The domain is still accessible over HTTP. All HTTP requests should be redirected to HTTPS. Redirect users and search engines to the HTTPS page or resource with server-side 301 HTTP redirects. This ensures all communications are encrypted, preventing certain man-in-the-middle attacks.
Hostname does not match SSL certificate Encryption	The site's hostname does not match the SSL certificate. The domain name should be added to the certificate, either as a Subject Alternative Name or as the Common Name. Add the hostname to the SSL certificate, as a Subject Alternative Name or as Common Name, to ensure the website remains secure and does not expose errors to visitors through their browser.
SSL expired Encryption	SSL certificate has expired. The certificate will need to be renewed for connections to your domain to be trusted. Renew expired SSL certificates to ensure that the connections to the domain are secure and trust by modern browsers. This keeps your customers secure and ensures visitors don't bounce from your site.

Risk category breakdown

Questionnaire Risks

Security questionnaires help identify potential weaknesses that are not observable from outside of the organization. This could include identity and device management, data protection, and information governance controls like single sign-on, audit logs, and retention policies. Security questionnaires are notoriously labor-intensive to administer which is why organizations invest in tools like UpGuard to automate the process.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 4

Questionnaire Risks Breakdown

Risk	Details
Third-Party Dependency	When organizations depend on third-party providers, they may inadvertently expose themselves to risks associated with those providers, including data breaches, compliance issues, and service outages. To mitigate this risk, organizations should conduct thorough due diligence before engaging third-party vendors, including assessing their security practices, compliance with relevant regulations, and incident response capabilities. Additionally, organizations should establish clear contractual agreements that define security expectations and responsibilities and implement regular assessments or audits of third-party service providers to ensure ongoing compliance and risk management.
Inherent Risk - Dependency on Primary URL / Online operations	The assessment score also considers the health of the primary URL through external scans. Therefore, it's crucial to continuously maintain a strong security posture for your primary URL, as it represents your organization and can serve as an entry point for attackers.
Inherent Risk - Nature of Business	Inherent risk refers to the level of risk present in a process or activity before any controls or mitigation measures are applied.This option indicates a risk due to the nature of the industry the organization operates in.
Inherent Risk - Region of Operation	Detection and escalation cost, Notification cost, Forensic and investigative activities, Assessment and audit services, Post data breach response, Help desk activities/inbound communications, Credit report monitoring and identity protection services, Legal expenditures Regulatory interventions, Lost business cost. This option indicates a risk due to the region in which the organization operates.

Risk category breakdown

Website

Website security identifies issues with the controls that allow websites to safely be exposed to the untrusted network of the internet. Many of these controls are server security headers that help ensure a site is only serving trusted content.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 5	! 3

Website Risk Breakdown

Risk	Affected	Overview	Recommendation
!! Secure cookies not used	1 asset	Cookies are data sent from websites that are stored on your computer. They contain information about your preferences, history and other details. Cookies are used by websites to track users over time, target advertising and personalize the user experience. Some cookies are used in authentication, allowing sessions to be established without re-entering credentials. The Secure cookies attribute restricts the cookie's usability to encrypted channels only, ensuring that cookies are always passed over HTTPS connections.	Applications and web servers that distribute cookies should be configured to include the Secure attribute. The specifics of how to do this differ by technology. For example in ASP.NET, you add <httpCookies requireSSL="true" /> to the web.config file. In Java, you add <secure>`true`</secure> to the cookie-config session of web.xml. Because the Secure attribute requires SSL connections to work, it is important to verify that SSL is properly configured before enabling it.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	`[all set-cookie headers include 'secure']`	`Set-Cookie: ASP.NET_SessionId HttpOnly;`

Risk	Affected	Overview	Recommendation
!! Server information header exposed	1 asset	HTTP response headers pass additional information about the web server being contacted to the client contacting it. Such information can include the age of cached information, any redirection targets, and descriptions of currently running software. These headers are configured on the server, and depending on the platform, may contain default values for these fields. The Server header is specifically used to describe the type and version of web server software, e.g. Server: Apache/2.4.1 (Unix).	The Server header should be removed, blanked out or minimized. The method for doing so differs based on technology. In IIS, a URL rewrite rule can be used to replace the server header with a blank string. In Apache, however, the Server header cannot be blanked out, but can be configured to display only "Apache" by setting "ServerTokens Prod" in the Apache config file. Monitoring or auditing of exposed headers on all systems is recommended to ensure information about servers is not being shared.

Asset	Expected	Actual
candidatesentry.carisma-solutions.com.au	`[does not contain version number]`	`Microsoft-HTTPAPI/2.0`

Risk	Affected	Overview	Recommendation
!! X-Frame-Options is not deny or sameorigin	6 assets	X-Frame-Options is a server header that dictates whether a page is allowed to be rendered using the <frame>, <iframe>, <embed> or <object> tags. This measure prevents attackers from rendering a page within a frame they control, where they can then gather inputs to the page like login credentials.	Add a server header for X-Frame-Options with an option of "deny" if there is no need for the site to appear in a frame, or "sameorigin" to restrict this option to other pages on the same domain.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	`[deny or sameorigin]`	`[not set]`
auditandassurance.carisma-solutions.com.au	`[deny or sameorigin]`	`[not set]`
blog.carisma-solutions.com.au	`[deny or sameorigin]`	`[not set]`
candidatesentry.carisma-solutions.com.au	`[deny or sameorigin]`	`[not set]`
clientportal.carisma-solutions.com.au	`[deny or sameorigin]`	`[not set]`

Website Risk Breakdown (continued)

elevatesmsf.carisma-solutions.com.au	[deny or sameorigin]	[not set]

CSP implemented unsafely — 1 asset

A Content-Security-Policy (CSP) header defines directives for what resources can be used by the site as a measure to prevent cross site scripting attacks. The implementation of the CSP for this site uses a directive that potentially allows unsafe content.

To remediate the unsafe conditions in the CSP, identify which of the conditions in the risk details applies. If possible, remove unsafe-inline scripts, or add a hash or nonce to validate its integrity. Review the "object-src" and "script-src" directives and include specific trusted origins.

Asset	Expected	Actual
carisma-solutions.com.au	[implemented safely]	frame-ancestors 'self'

CSP is not implemented — 7 assets

A Content-Security-Policy header defines directives for server governance on website behaviors through the HTTP header, though you can also supply HTML meta tags with a string-matching attribute that sets a CSP for the page. With your CSP, you define the approved origins for content that browsers will load on your website, such as JavaScript, CSS stylesheets, images, and more.

To create the Content Security Policy for your website, you will need to update the configuration file containing your HTTP Response header. Different server setups and hosting platforms require different approaches to your configuration files. For example, you update the .htaccess or .httpd.conf files for Apache web servers, whereas NGINX servers require modification in the server block.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	[valid policy]	[not set]
auditandassurance.carisma-solutions.com.au	[valid policy]	[not set]
blog.carisma-solutions.com.au	[valid policy]	[not set]
candidatesentry.carisma-solutions.com.au	[valid policy]	[not set]
carisma-solutions.com.au	[valid policy]	[not set]
clientportal.carisma-solutions.com.au	[valid policy]	[not set]
elevatesmsf.carisma-solutions.com.au	[valid policy]	[not set]

Specific ASP.NET version exposed via header — 2 assets

HTTP response headers pass additional information about the web server being contacted to the client contacting it. Such information can include the age of cached information, any redirection targets, and descriptions of currently running software. Default installations of Microsoft IIS web servers often include an HTTP response header called X-AspNet-Version. This can contain the version of ASP.NET that is currently running.

The entire X-AspNet-Version header should be removed. It can be found and removed under HTTP Response Headers in the IIS GUI. Just clearing the value of the header is not enough. Even the presence of the X-AspNet-Version header reveals that some version of ASP.NET and likely IIS is running on the server. Monitoring or auditing of exposed headers on all systems is recommended to ensure information about servers is not being shared.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	[not set]	4.0.30319
candidatesentry.carisma-solutions.com.au	[not set]	4.0.30319

Use of ASP.NET exposed via header — 2 assets

HTTP response headers pass additional information about the web server being contacted to the client contacting it. Such information can include the age of cached information, any redirection targets, and descriptions of currently

The X-AspNet-Version header should be removed. It can be found and removed under HTTP Response Headers in the IIS GUI. Monitoring or auditing of exposed headers on all systems is recommended to ensure information about servers is not being

Website Risk Breakdown (continued)

		running software. Default installations of Microsoft IIS web servers often include an HTTP response header called X-AspNet-Version. This can contain the version of ASP.NET that is currently running.	shared.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	[not present]	[present]
candidatesentry.carisma-solutions.com.au	[not present]	[present]

X-Content-Type-Options is not nosniff	7 assets	The X-Content-Type-Options header is not set to "nosniff," an option that prevents MIME type sniffing. This header ensures that the content types defined in the Content-Type header are used and not changed.	In the file that configures your server headers, add the header X-Content-Type-Options: nosniff. You should also ensure that the Content-Type is set correctly for the content you are expecting to server, and test that the site renders as desired after the change.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	nosniff	[not set]
auditandassurance.carisma-solutions.com.au	nosniff	[not set]
blog.carisma-solutions.com.au	nosniff	[not set]
candidatesentry.carisma-solutions.com.au	nosniff	[not set]
carisma-solutions.com.au	nosniff	[not set]
clientportal.carisma-solutions.com.au	nosniff	[not set]
elevatesmsf.carisma-solutions.com.au	nosniff	[not set]

Risk category breakdown

Encryption

Encryption of data in transit is a security measure that prevents adversary-in-the-middle attacks. Data in transit over the internet should always be encrypted, and the encryption methods should be kept up to date to avoid adversarial decryption techniques.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 1	!!! 3	!! 2	! 2

Encryption Risk Breakdown

Risk	Affected	Overview	Recommendation
!!!! SSL not available	2 assets	Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. Certificates expire after a set period of time and must be renewed to keep SSL/TLS active. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when necessary.	Valid SSL/TLS certificates with strong encryption algorithms should be obtained from a trusted authority and properly installed and configured on all internet facing systems. Every system must have its name on the certificate to prevent mismatch errors in the browser. HTTPS should be made mandatory, with the necessary redirects and enforcement in place to ensure no plain text connections are possible. Processes should be established to ensure certificates are renewed before they expire.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	`true`	`false`
blog.carisma-solutions.com.au	`true`	`false`

Risk	Affected	Overview	Recommendation
!!! HTTP does not redirect to HTTPS	3 assets	The HTTP Still Available check is used to measure whether a server is allowing users to connect to it via HTTP rather than HTTPS. Connecting to a website via HTTPS is more secure as it involves a SSL/TLS-based connection, which encrypts data in transit. Many web browsers will try the HTTP version of a website first before trying the HTTPS version. If you have a proper redirect response on your HTTP port then you will pass this check. You should combine this with proper HSTS settings to ensure browsers always attempt a HTTPS-based connection from the beginning.	All HTTP connections should be redirected to HTTPS connections instead. The method for doing this differs by technology. For some websites, the .htaccess file can be modified to reroute requests to HTTPS. For Microsoft IIS, the URL Rewrite module for IIS will allow you to redirect HTTP requests to HTTPS. HTTPS redirects should always be paired with HTTP Strict Transport Security (HSTS). HSTS will ensure no HTTP connections are allowed.

Asset	Expected	Actual
assessment.carisma-solutions.com.au	`false`	`true`
candidatesentry.carisma-solutions.com.au	`false`	`true`
clientportal.carisma-solutions.com.au	`false`	`true`

Risk	Affected	Overview	Recommendation
!!! Hostname does not match SSL certificate	5 assets	Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. Every certificate should include the preferred hostname(s) for the system that is being protected, so that the certificate can be verified to the address being accessed by the client.	A new certificate should be requested from a trusted authority with the correct hostname(s) listed on it. This will prevent browser errors and reduce certificate complexity across the organization. All existing certificates should be audited to ensure that each one has the proper hostnames. Changes to hostnames or aliases should include steps to update certificates with the new names.

Encryption Risk Breakdown (continued)

Asset	Expected	Actual
auditandassurance.carisma-solutions.com.au	[hostname matches SSL certificate]	auditandassurance.carisma-solutions.com.au does not match any of these Subject Alternative Names in the SSL certificate: *.shr.prod.sin2.secureserver.net, shr.prod.sin2.secureserver.net
blog.carisma-solutions.com.au	[hostname matches SSL certificate]	blog.carisma-solutions.com.au does not match any of these Subject Alternative Names in the SSL certificate: *.shr.prod.sin2.secureserver.net, shr.prod.sin2.secureserver.net
candidatesentry.carisma-solutions.com.au	[hostname matches SSL certificate]	candidatesentry.carisma-solutions.com.au does not match any of these Subject Alternative Names in the SSL certificate: unitedauditsolutions.com.au, www.unitedauditsolutions.com.au
carisma-solutions.com.au	[hostname matches SSL certificate]	carisma-solutions.com.au does not match any of these Subject Alternative Names in the SSL certificate: *.shr.prod.sin2.secureserver.net, shr.prod.sin2.secureserver.net, www.carisma-solutions.com.au does not match any of these Subject Alternative Names in the SSL certificate: *.shr.prod.sin2.secureserver.net, shr.prod.sin2.secureserver.net
clientportal.carisma-solutions.com.au	[hostname matches SSL certificate]	clientportal.carisma-solutions.com.au does not match any of these Subject Alternative Names in the SSL certificate: *.shr.prod.sin2.secureserver.net, shr.prod.sin2.secureserver.net

SSL expired — 2 assets

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when necessary. Certificates expire after a set period of time and must be renewed to keep SSL/TLS active.

Expired certificates must be replaced with valid certificates from a trusted authority. Once a valid certificate has been installed on the system, SSL/TLS functionality will be restored. Validity periods are limited to 398 days. In order to maintain continuity, processes should be established to renew certificates within that time frame before they expire.

Asset	Expected	Actual
auditandassurance.carisma-solutions.com.au	[has not expired]	2025-08-17 23:59:59 UTC
candidatesentry.carisma-solutions.com.au	[has not expired]	2025-07-08 23:59:59 UTC

HTTP Strict Transport Security (HSTS) not enforced — 5 assets

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. SSL/TLS uses the HTTPS protocol, so all client connections

Enable HSTS on the server. This is done by including the Strict-Transport-Security header on the system. The “includeSubDomains” directive should be specified to ensure all subdomains on the system use HTTPS. Submit your domain to Google’s HSTS preload service. This preload list is included in most browsers and will automatically make all connections to the domain use an encrypted channel.

Encryption Risk Breakdown (continued)

must be rerouted from HTTP to HTTPS when necessary. HTTP Strict Transport Security (HSTS) ensures that no HTTP connections will be allowed from the server. This forces the use of HTTPS, which maintains encryption at all times.

Asset	Expected	Actual
auditandassurance.carisma-solutions.com.au	[header set]	[not set]
blog.carisma-solutions.com.au	[header set]	[not set]
candidatesentry.carisma-solutions.com.au	[header set]	[not set]
carisma-solutions.com.au	[header set]	[not set]
clientportal.carisma-solutions.com.au	[header set]	[not set]

Insecure SSL/TLS versions available — 1 asset

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. There are multiple versions of SSL and TLS that can be used. Although each version supersedes the last, many times the older protocols remain enabled for legacy support.

Only TLS 1.2 or higher should be allowed. All older versions should be disabled on the server to prevent malicious actors from trying to connect to these vulnerable protocols.

Asset	Expected	Actual
candidatesentry.carisma-solutions.com.au	[none found]	TLSv1, TLSv1.1

Domain was not found on the HSTS preload list — 1 asset

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when necessary. HTTP Strict Transport Security (HSTS) ensures that no HTTP connections will be allowed from the server. This forces the use of HTTPS, which maintains encryption at all times. Google hosts an HSTS preload list that is used in most browsers. Domains on this list will automatically establish encrypted connections from the browser, giving them the best protection.

Add the domain to the preload list by following the steps at https://hstspreload.org. There are several prerequisites to approval, including the need for a valid certificate, an HTTP to HTTPS redirect and that all subdomains are served over HTTPS as well. Your HSTS header must also be properly configured, containing both the IncludeSubDomains and Preload directives.

Asset	Expected	Actual
elevatesmsf.carisma-solutions.com.au	[entry found]	[no entry found]

HSTS header does not contain includeSubDomains — 1 asset

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when

Update the Strict-Transport-Security header on the system to contain the IncludeSubDomains parameter. Web services may need to be restarted for the change to take effect. Processes should be established to monitor or audit the status of HSTS on all internet-facing systems to ensure HSTS is present and properly configured.

Encryption Risk Breakdown (continued)

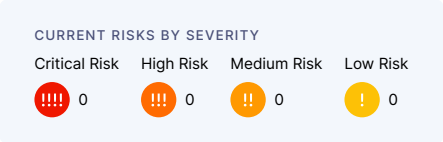
necessary. HTTP Strict Transport Security (HSTS) ensures that no HTTP connections will be allowed from the server. This forces the use of HTTPS, which maintains encryption at all times. The IncludeSubDomains directive enforces HSTS across subdomains as well.

Asset	Expected	Actual
elevatesmsf.carisma-solutions.com.au	`max-age=[anything]; includeSubDomains; ...`	`max-age=63072000`

Risk category breakdown

IP/Domain Reputation

IP/Domain reputation indicates reports that a site is suspected of hosting malware, unwanted software, or phishing pages. These risks can indicate that a system has been compromised and may result in the site being blocklisted by other security administrators.



IP/Domain Reputation Risk Breakdown

No risks detected in this category.

Risk category breakdown

Operational Risk

Operational risk highlights factors that indicate a company may face elevated exposure due to how it operates, including use of emerging technologies, links to sanctions, or activity in high-risk regions.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 0

Operational Risk Risk Breakdown

No risks detected in this category.

Risk category breakdown

Email

Email security measures prevent malicious actors from impersonating the sender of an email message. These controls help prevent phishing campaigns against an organization, its vendors, and its customers. Email is a commonly abused method for attempting to gain access to a user's account, and effective email security can reduce this risk.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 1

Email Risk Breakdown

Risk	Affected	Overview	Recommendation
! DMARC policy is p=quarantine	1 asset	Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email security feature that works in conjunction with Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) to ensure that messages actually originate from the organizations claimed in the From: address. It does this by “aligning” the From: address with either the SPF or DKIM policy in the sender domain. If a message’s From: address does not align with either of these policies, DMARC offers options on how to handle the message, including delivering it, quarantining it and blocking it altogether.	The p= value in DMARC provides instructions on what to do with an email that fails DMARC alignment. The p= value should ultimately be set to reject for best security; however, p=quarantine can be used temporarily to monitor DMARC behavior and ensure false positives are not being quarantined. Once this monitoring is complete, the p= value should be set to reject. This helps prevent fraudulent email from reaching end users.

Asset	Expected	Actual
carisma-solutions.com.au	`v=DMARC1; p=reject; ...`	`v=DMARC1; p=quarantine; pct=100`

Risk category breakdown

DNS

DNS security entails the management of settings in DNS records to ensure that organizations remain in control of their domains and the content served on their domains. Poor DNS security can allow attackers to gain control of domains and serve malicious content on sites that appear to belong to the victim organization.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 1

DNS Risk Breakdown

Risk	Affected	Overview	Recommendation
! DNSSEC not enabled	1 asset	Domain Name System (DNS) is the service that translates human-friendly names to IP addresses. When a URL is sent from the browser, it goes to a DNS server that references its database and returns an IP address for the browser to use. Domain Name System Security Extensions (DNSSEC) is an optional feature of DNS that authenticates (but does not encrypt) responses to DNS requests. DNSSEC uses certificates to ensure only authorized DNS translations are returned to a client.	Enable DNSSEC on the domain. This is a three step process that involves creating the necessary DNSSEC records in your domain, activating DNSSEC at your domain registrar and enabling DNSSEC signature validation on all DNS servers. The specifics of each step vary depending on the platforms and vendors in play.

Asset	Expected	Actual
carisma-solutions.com.au	`true`	`false`

Risk category breakdown

Network

Network layer security means restricting access to the services running on an IP address to only those expected to be internet-facing. Services identified as network risks are those intended to run inside a trusted network or where direct access allows attackers excessive opportunity for abuse.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 1	!!! 0	!! 0	! 0

Network Risk Breakdown

Risk	Affected	Overview	Recommendation
!!!! 'FTP' port open	4 assets	File Transfer Protocol (FTP) is a common method for reliably sharing files between networked systems. By default FTP uses port 21. Data transferred in FTP is done so in plain text, including credentials. FTP can require user credentials, or use an anonymous mode that allows all connections. The FTP root is configured on the server to a specific directory, granting remote access to its contents, including subdirectories.	File transfers should be done on an intranet, VPN or other solution that prevents internet-wide exposure. FTP should be replaced with an encrypted solution such as SFTP or FTPS. This will protect data in transit from third party interception. If FTP must be open to the internet, it should be rigorously updated and maintained to ensure it is not vulnerable to any known exploits.

Asset	Expected	Actual
auditandassurance.carisma-solutions.com.au	[closed]	'FTP': [listening on port 21]
blog.carisma-solutions.com.au	[closed]	'FTP': [listening on port 21]
carisma-solutions.com.au	[closed]	'FTP': [listening on port 21]
clientportal.carisma-solutions.com.au	[closed]	'FTP': [listening on port 21]

Risk category breakdown

Data Leakage

Data leakage is the unintentional exposure of potentially sensitive information, including credentials, personal information, and business secrets. Data leakage risks can indicate lapses in best practice that could result in sensitive data being exposed in the future, as well as active exposures of sensitive data.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 0

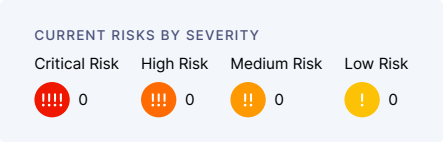
Data Leakage Risk Breakdown

No risks detected in this category.

Risk category breakdown

Attack Surface

Attack surface risks present attackers with additional points on an organization's externally accessible boundaries for them to target. Attack surface reduction is the practice of increasing security by removing possible targets, either by decommissioning assets or moving them behind a network layer protection like a VPN.



Attack Surface Risk Breakdown

No risks detected in this category.

Risk category breakdown

Vulnerability Management

Vulnerability management requires identifying software vulnerabilities and upgrading to secure versions on a timeline appropriate to the severity of the vulnerability. Software with actively exploited vulnerability should be updated as quickly as possible. End of life software no longer receives security updates, and should be decommissioned or updated to an actively maintained version.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 1	!! 0	! 0

Vulnerability Management Risk Breakdown

Risk	Affected	Overview	Recommendation
!!! **End-of-life version of WordPress detected**	1 asset	The software product used on this site is advertising a version that is past it's end of life (EOL) date. EOL software is at higher risk of having unpatched vulnerabilities leading to exploitation.	The software should be updated to a currently maintained version so that any new security updates can be applied quickly. If the software is running a different version than what is advertised in its server header, updating the server header to the current version can also remediate the detection of an EOL software product.

Asset	Expected	Actual
blog.carisma-solutions.com.au	`[none detected]`	`WordPress: 4.9.8: 2018-12-06 (port: 443)`

Conclusion

In summary, we recommend the following course of action for Carisma Solutions Private Limited

- Follow up to ensure all recommendations have been implemented
- Vendor should be reassessed in 1 year
- *Add further recommendations here*

This Report, including all data, content, analysis, recommendations, and other information provided (the "Report"), is proprietary and confidential to ICICI Lombard General Insurance Company Limited ("ICICI Lombard"). It is intended for the sole use of the Recipient and must be kept private and confidential. The Report shall not be disclosed, circulated, reproduced, or published by the Recipient, in whole or in part, without prior written consent from ICICI Lombard.

The assessment is performed basis on the information and responses provided by the client. UpGuard has prepared this Report only at the Recipient's request and direction. This Report is based on information provided to us without independent verification. UpGuard have not conducted any tool-based vulnerability assessment, penetration testing, or audit as part of this assessment. The findings should be read in conjunction with the specific objectives and scope of this engagement.

ICICI Lombard make no representations or warranties, express or implied, regarding the accuracy, completeness, or reliability of the information herein. This Report does not constitute any legal, financial, or professional advice and should not be used as the sole basis for making any decision.

ICICI Lombard disclaim liability for any direct, indirect, incidental, special, or consequential damages or any claim arising out of the use, reliance, or application of this Report. Any use or reliance on the content is strictly at the Recipient's own risk. Recommendations in the Report do not constitute an offer or invitation or form the basis of any contractual relationship.

ICICI Lombard is responsible for any errors, omissions, or reliance placed on third-party information within this Report. The content, proprietary to ICICI Lombard, may not be copied, distributed, or communicated to any third party without explicit permission from ICICI Lombard.

ICICI Lombard's trade logo belongs to ICICI Bank and is used by ICICI Lombard General Insurance Company Limited under license.

Evidence used to generate this report

This report includes analysis performed as part of a risk assessment.

The overall set of risks included in this report reflect the risk profile at the time that this risk assessment was published.

DATE PUBLISHED
Jul 6, 2026

AUTHOR
Roshni Nagvekar

Questionnaires (1)

Questionnaire name	Sent	Submitted	Rating	Risks detected
ILGIC Haiku - Inherent Risk	Jul 6, 2026	Jul 6, 2026	A 911	4 risks

Automated scanning

This report includes analysis performed on the following domains and IPs as of Jul 6, 2026.

ACTIVE DOMAINS & IPS	INACTIVE DOMAINS & IPS	TOTAL DOMAINS & IPS SCANNED
8	0	8