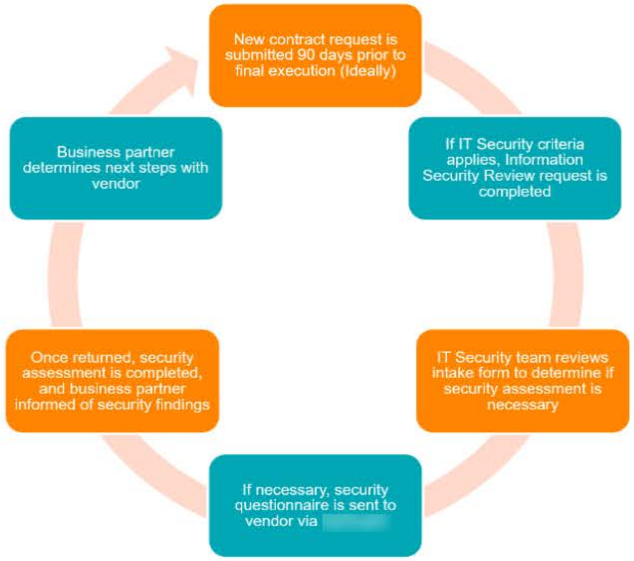
IT Security Assessment Process

ZW Owned by Zshaquel Walker •••
Last updated: Mar 10, 2022 • 8 min read • 3 people viewed • Attachments • Legacy editor

Overview of Third-Party Risk Assessment at [redacted]


New contract request is submitted 90 days prior to final execution (Ideally)
If IT Security criteria applies, Information Security Review request is completed
IT Security team reviews intake form to determine if security assessment is necessary
If necessary, security questionnaire is sent to vendor via [redacted]
Once returned, security assessment is completed, and business partner informed of security findings
Business partner determines next steps with vendor

This Policy defines high-level requirements for protecting information and technology systems, which in turn help support [redacted] overall performance as a leader in chemical distribution and services.

[redacted] Information Security & Protection Policy and Standards)

This Policy defines high-level requirements for protecting information and technology systems, which in turn help support [redacted]' overall performance as a leader in chemical distribution and services.

When will a Security Assessment Be Warranted?

When new contracts, renewals for existing contracts or new integrations with existing vendors are required, requesters are expected to complete the "Information Security Review" form if the following criteria applies:

- The contract is for a third party hosted service (used to store, process, and/or transmit data)
- [redacted] information will be stored or processed on third party systems
- Third party's networks or systems will be connected to [redacted]' corporate systems
- The service will be used to send emails to [redacted] employees or to others on the company's behalf

If yes, requester will receive an email from the IT Security team directing them to the "Information Security Vendor Risk Review" form in IT Store.

Note: *The Information Security Review form should be completed by someone familiar with the proposed technical architecture and classification or sensitivity of the scoped data. Vendor contact information is required to complete the Information Security Review form.*

[redacted]' IT Security team will review the form to determine if a full assessment is required of the vendor. If the security review concludes a full assessment is required, the vendor will receive a Security Assessment Questionnaire via [redacted].

Personally Identifiable Information (PII)

Personally Identifiable Information: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Please visit [redacted]' Privacy Policy for more details.

Safeguarding Sensitive Personally Identifiable Information

PII Escalation Process

If PII or SPI is in scope of the security assessment, the IT Security Team will escalate to the Legal Privacy Team.

Example of Security Assessment Questionnaire to Vendor

Properly vetting potential vendors requires asking the right questions:

- What type of policies, procedures, and processes do you have in place to secure data and follow compliance regulations? Do you follow the best practices for all infosec domains, including robust risk assessment, access management, data privacy, encryption, and incident response programs?
- For cloud service providers or SaaS: Is your security architecture designed using the highest industry standards like FedRAMP?
- Do you test your security systems with both internal and accredited external audits?
- Do you have any regulatory compliance verification, such as a SOC report or a PCI Level-1 certification?
- Can you disclose with which regulatory standards your organization complies?
- Can you provide evidence of due diligence mapping of your existing controls, architecture, and processes to these regulatory standards?
- Do you have agreements in place with your supply chain holding them to your exact security and privacy standards? Can you provide documentation of these agreements?
- Does your organization have a disaster recovery and business continuity plan in place?
- Do you have multiple providers or other fail-safes for each service you rely on to maintain operations?
- If using on-premise infrastructure, do you have adequate physical security controls in place to protect all media and information systems?
- If using virtual infrastructure, does your cloud provider have sufficient security mechanisms in place, including individual hardware restoration and recovery capabilities?

Third Party Vendor Security Assessment Output

Once the vendor has completed the Security Assessment Questionnaire via [redacted] IT Security team reviews the vendor's responses and risk rating. [redacted] generates security risk ratings through proprietary algorithms that take in and analyze trusted commercial and open-source data sets to non-intrusively collect data that can quantitatively evaluate cybersecurity risk. The IT Security findings are returned to the business partner to determine next steps (see Appendix).

Appendix

Information Security Vendor Risk Review Form (Security Intake)

Required Fields

- Project Name - Project or initiative associated with request
- Project Description - Details of intended product use and vendor name
- Project Manager - Product owner/Lead
- Estimated Go-Live Date - Anticipated implementation date
- Vendor's Technical Contact
    - Name/Phone/Email
- **Data Assessment** - Will the product access [redacted] data?
    - Potential Regulatory Impact
        - None
        - GDPR – employee privacy
        - PCI – credit card privacy
        - DHS – chemicals of interest
        - SOX – financial regulations
        - Other
    - Will [redacted] information be stored or processed on third party systems?
        - Yes/No
    - Type of information stored, processed or transmitted on the third party system
        - Personal User Information
        - Credit Card Information
        - Sensitive Product Information
        - Sensitive Financial Information
        - Sensitive Customer Information
        - Other
    - Data Classification (refers to the classification of the type of information stored, processed or transmitted)
        - Public - Any data accessible in public domain
        - Private - Customer & Sales data, bank account information, user names and passwords
        - Regulated - Personally Identifiable Information, Social Security Numbers, Personal Health Information, Cardholder Data
    - Data Owner - Business owner responsible for data being stored, processed or transmitted on third-party system
    - Will the data be encrypted, both in transit and on disk?
        - Yes/No
- **Platform & Network Connectivity** - Details about vendor's product platform/service. Will third party's network or system require connectivity to [redacted] corporate systems?
    - Project Platform
        - Not Applicable
        - On-Premise
        - Hybrid
    - Cloud Service
        - Not Applicable
        - AWS
        - Azure
        - SalesForce
        - Other
    - Service Provider Website / URL
    - Will data be transferred between the service and [redacted] systems?
        - Yes/No
    - How will data be transferred between the service and [redacted] corporate systems?
        - Not Applicable
        - Manual
        - Integration
        - VPN
        - SSL/TLS
        - Other
    - How will users access the service?
        - Not Applicable
        - Web
        - VPN
        - Other
- **Email Whitelisting**
    - Will emails be sent from this service to [redacted] employees?
        - Yes/No
    - Will emails be sent from this service to external recipients?
        - Yes/No
    - Is there a need for the service to impersonate internal senders (i.e. will emails be sent as @[redacted] or other internal email domains?)
    - Yes/No
    - List email addresses or domains that will be used to send emails from this service

SLA

Security Team expected to acknowledge New Information Security request within 2 days of TASK creation by moving status to "Work in Progress" and sending a security questionnaire via [redacted], to the vendor contact.

The vendor is expected to return the completed assessment within 30 days. If the questionnaire has not been returned to [redacted] within 30 days, the [redacted] Business Sponsor will be informed of request being closed as "Incomplete." IT Security team will contact vendor weekly until questionnaire is returned or request is closed as "Incomplete."

Upon receipt of the completed questionnaire, the Information Security team is responsible for reviewing the questionnaire and any additional documents, (SOC, ISO etc.) and returning the [redacted] findings to the Business Sponsor within 3 days of receipt.

Note: This timeline may be impacted if the vendor is asked to remediate any critical or high risks findings.

Example Email: Completed Third Party Vendor Security Assessment

The security assessment for XXX Vendor is complete. As you know, we run passive vulnerability scans on a vendor's public facing servers using [redacted] to gauge how well [redacted] data is being protected. As shown below, strong scores indicate this vendor has a robust security posture and good attack surface management. Overall, there were NO Missing Software Patches reported. Equally impressive, there were NO Critical or High severity vulnerabilities reported. While this email is classified as Internal Distribution Only, you are encouraged to share the attached reports with the vendor as an informational aid to assist with any remediation efforts they undertake. Let me know if you have any questions.

VULNERABILITIES

***NO CRITICAL OR HIGH SEVERITY RISKS WERE REPORTED

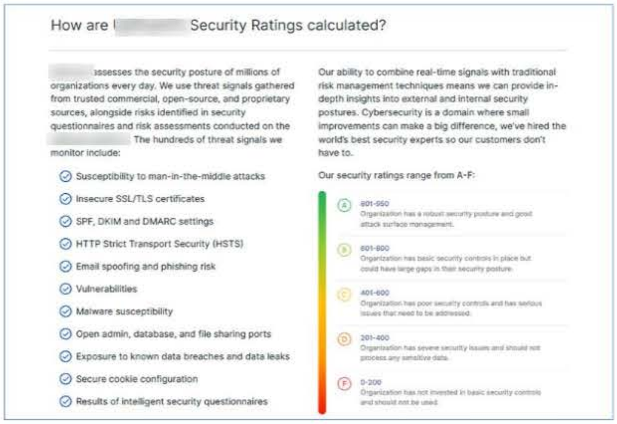
Severity/Finding/Risk	Domains Impacted

Critical	**0**
High	**0**
Medium	4
HttpOnly cookies not used	3
Vulnerable to cross-site attacks	3
Secure cookies not used	1
Susceptible to man-in-the-middle attacks	1
Low	6
DNSSEC not enabled	1
DNS is susceptible to man-in-the-middle attacks	1
Domain was not found on the HSTS preload list	4
Susceptible to man-in-the-middle attacks	4
HSTS header does not contain includeSubDomains	1
Susceptible to man-in-the-middle attacks	1
Grand Total	10

MISSING SOFTWARE PATCHES

***NO MISSING PATCHES WERE REPORTED

Severity/Patch	Patch Instances
Critical	0
High	0
Medium	0
Low	0
Grand Total	0



How are [redacted] Security Ratings calculated?

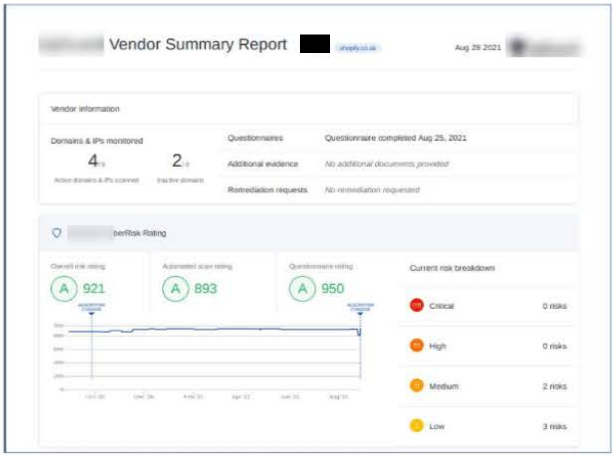
[redacted] assesses the security posture of millions of organizations every day. We use threat signals gathered from trusted commercial, open-source, and proprietary sources, alongside risks identified in security questionnaires and risk assessments conducted on the [redacted] The hundreds of threat signals we monitor include:

- ✓ 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
- ✓ Results of intelligent security questionnaires

Our ability to combine real-time signals with traditional risk management techniques means we can provide in-depth insights into external and internal security postures. Cybersecurity is a domain where small improvements can make a big difference, we've hired the world's best security experts so our customers don't have to.

Our security ratings range from A-F:

A	801-950 Organization has a robust security posture and good attack surface management.
B	601-800 Organization has basic security controls in place but could have large 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.



[redacted] Vendor Summary Report [redacted] shopify.co.uk Aug 28 2021 [redacted]

Vendor information

Domains & IPs monitored

4 Active domains & IPs scanned

2 Inactive domains

Questionnaires	Questionnaire completed Aug 25, 2021
Additional evidence	*No additional documents provided*
Remediation requests	*No remediation requested*

[redacted] berRisk Rating

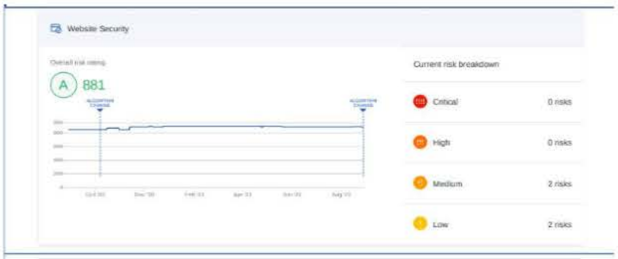
Overall risk rating A 921

Automated scan rating A 893

Questionnaire rating A 950

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	2 risks
Low	3 risks

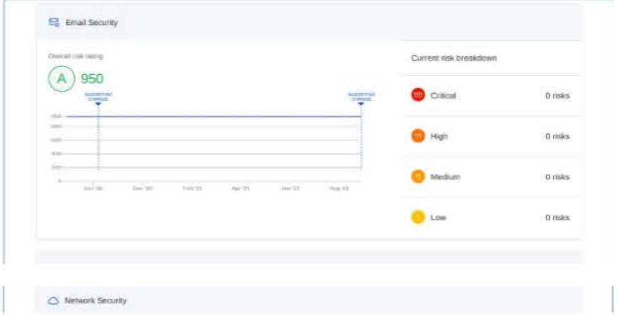


Website Security

Overall risk rating A 881

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	2 risks
Low	2 risks



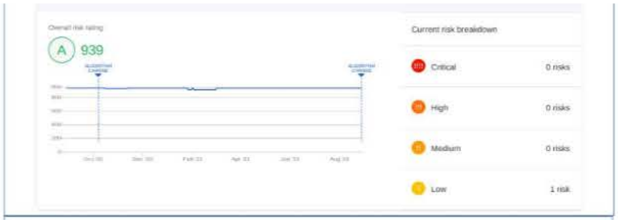
Email Security

Overall risk rating A 950

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	0 risks
Low	0 risks

Network Security

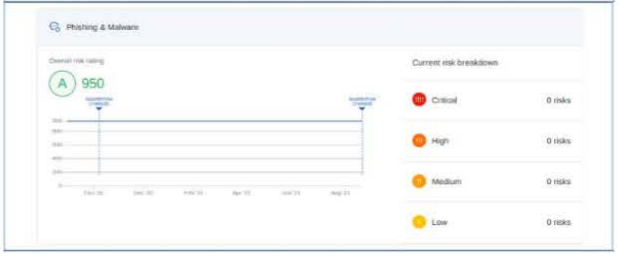


Overall risk rating

A 939

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	0 risks
Low	1 risk



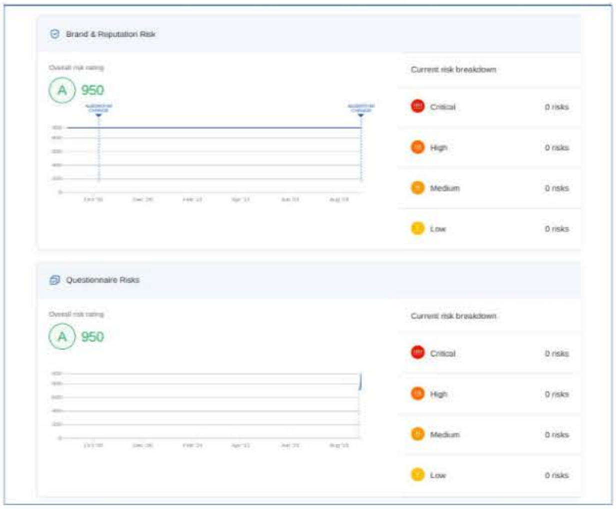
Phishing & Malware

Overall risk rating

A 950

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	0 risks
Low	0 risks



Brand & Reputation Risk

Overall risk rating

A 950

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	0 risks
Low	0 risks

Questionnaire Risks

Overall risk rating

A 950

Current risk breakdown

Critical	0 risks
High	0 risks
Medium	0 risks
Low	0 risks

Q & A:

1. When a new vendor is about to initiate on boarding, does the process involve legal department to determine the specifics on an engagement letter or similar?
   - It is assumed that Legal gets involved in discussions whenever a vendor is on/off boarded.
2. What does the engagement letter allow/forbids?
   - Legal, Contract and H/R teams may all be engaged here to set requirements.
3. Does [redacted] classify vendors only based on their public reputation? (i.e. Does it take into account internal controls, attestations and/or their efficiency?)
   - [redacted] assesses the security posture of millions of organizations every day. They use threat signals gathered from trusted commercial, open-source, and proprietary sources, alongside risks identified in security questionnaires and risk assessments conducted on the [redacted] platform. [redacted] 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.
4. When [redacted] flags a high/critical finding, how do you follow up the remediation plan those findings?
   - Vendors are provided copies of [redacted] reports at the completion of every assessment to assist with their remediation efforts to mitigate Critical and High severity issues as soon as feasibly possible. Whenever further communications are needed, email, voice or video conference meetings are held to answer questions and provide recommendations as needed.
     Are those remediated at all before the engagement with the vendor? Business teams are responsible to ensure risk assessments are completed prior to go-live but are free to accept, transfer or mitigate risks to meet business goals and objectives. Our team sets no requirement to remediate a risk prior to engagement.
5. What kind of documentation do you normally ask from vendors (e.g. annual pentest, soc reports, ISO attestation)?
   - If a full assessment is not warranted, we run and store [redacted] scans on SharePoint. Scan results are shared with whomever requested the assessment. An email is sent to the requestor summarizing our findings and offering guidance to share those results with vendors to assist with their remediation efforts. When responses to the Intake Form indicate a full assessment is warranted, we send the vendor a security questionnaire from within [redacted]. The questionnaires provide opportunity to attach audit reports (SOC2 Type-2 preferred) as well as other relevant documents such as security and privacy policies, bridge/attestation letters and Penetration tests if available). how do you define what to ask from each vendor? The answer is based upon the size and maturity level of an organizations Security Program.
6. How do you classify vendors criticality?
   - The sensitivity of [redacted] information is often a primary driver of scoping vendor engagements. For example, publicly available company data does require the same level of protection as Sensitive, Private or Highly Confidential.
7. Is there a formal PII/CCI/intellectual capital tier classification document?
   - Tier classification may be covered by one or more of the pre-canned security questionnaires such as PCI.
8. Do all vendors get the same questionnaire, no matter their use/level of Confidential Data, PII, and/or Intellectual capital?
   - There are a handful of security questionnaires available. Where less sensitive or publicly available Univar data is involved, a short-form security questionnaire is often sent to vendor for completion. Vendors that handle more sensitive Univar data will generally get a more comprehensive security questionnaire sent to them so we can more fully understand their risk posture and ability to safeguard our data commensurate with its value.
9. How does the risk acceptance process work and how is it documented?
   - The [redacted] platform provides the ability to request remediation for risk issues discovered in scans or through responses documented in questionnaires. Documentation is all stored in the [redacted] platform and is typically exported to PDF or Excel format at the conclusion of an assessment where it is stored in [redacted].
10. How do you handle & record exceptions to the company security policies?
    - As it pertains to vulnerabilities discovered by [redacted], documentation is saved in [redacted] and stored on [redacted]s.

+ Add label

Related pages

Security Assessment Email to User
IT Compliance

Organized together

Measuring Risk
IT Compliance

Organized together

Vulnerability Management and Policy Compliance Dashboards
IT Compliance

Organized together

IT Risk Register
IT Compliance

Organized together

IT Compliance
IT Compliance

Organized together

Information Security
IT Compliance

Organized together

👍 👏 🎉 Be the first to add a reaction

ZW Write a comment...