HyperComply

Instructions:

- Create a copy of this document for each vendor you need to assess. Add the vendor's name to the file name (ex: 2022 Assessment - Mega Corp) so it's easy to find and reference in the future.

- Review the Questionnaire tabs to familiarize yourself with the topics and questions included. These are the most common topics you will likely be reviewing for third party software and data vendors.

- Based on a specific vendor, you may want to add or remove questions to gather more specific information. For example, if a company only provides you with data and does not have an application, you may be able to omit "Application Security" questions.

- Send the questionnaire document to your vendor. After they have fully completed it, review to ensure their responses match up with your own company's security policies and requirements.

Want to automate sending vendor security questionnaires?
HyperComply makes it easy to send security questionnaires to new vendors, track responses, and monitor your network of tools over time. Get started today—for free.

General Information

Company Details

Company name	
Parent company name	

Website URL	
When was the company founded?	
Is the company traded publicly?	
What exchange is the company listed on?	
What is the company's ticker symbol?	
Are there any material claims against the company?	
Please describe in detail what material claims are held against the company	

Product Details

Product name	
Product description	
Product URL	

Compliance Documentation

GDPR

Are you GDPR certified?	
Please provide links to supporting documentation	

SOC2

Are you SOC2 certified?	
Please provide links to supporting documentation	

CCPA

Are you CCPA compliant?	
Please provide links to supporting documentation	

ISO

Are you ISO certified?	
Please provide links to supporting documentation	

SSPA

Are you SSPA compliant?	
Please provide links to supporting documentation	

CMMC

Are you CMMC compliant?	

Please provide links to supporting documentation	

Security Policies and Practices

Other compliance

Do you have additional compliance certifications?	
Please provide links to supporting documentation	

Access Control Policy

Do you have a documented access control policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
How often are entitlements evaluated?	
Are access rights adjusted or revoked on termination of employment, contract, or agreement?	

Asset Management Policy

Do you have a documented asset management policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	

Acceptable Use Policy

Do you have a documented acceptable use policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Are all personnel required to sign an Acceptable Use Policy?	

Application Security Policy

Do you have a documented application security policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Is the application input and output validated?	
Are application network boundaries protected by firewalls?	
Do you perform vulnerability tests?	
How often are vulnerability tests conducted?	

Is the service hosted in the cloud?	
Who is the cloud provider?	
Where are the data centers located?	
Does the provider follow security best practices?	
Do you support any types of Single Sign On (SSO)?	
Please list the types of SSO you support (SAML, OAuth, etc.)	

Backup Policy

Do you have a documented backup policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
How long are system backups retained?	
How often are system backups performed?	
Are backups encryped?	

Business Continuity and Disaster Recovery (BCDR) Policy

Do you have a documented BCDR policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	

Change Management Policy

Do you have a documented change management policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Is automated validation performed on code prior to production deploy?	
Does the policy outline a secure development practice?	
Is code tested on a preproduction environment priort to production deploy?	
Is version control used?	
Are customers notified of significant changes to the product?	

Code of Conduct Policy

Do you have a documented code of conduct policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	

Data Deletion Policy

Do you have a documented data deletion policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
At contract termination, will the customer's data be deleted?	
Do you support secure deletion of data and backups?	
Encryption Policy	
Do you have a documented encryption policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Is data encrypted at rest?	
What method is used to encrypt data in transit?	
How are encryption keys managed?	
Information Security Policy	
Do you have a documented information security policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Are background checks performed?	
Is annual security awareness traning conducted for employees?	
Is role-specific security training performed?	
Incident Response Policy	
Do you have a documented incident response policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Does the incident response policy contain a data classification matrix?	
Password Policy	
Do you have a documented password policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Do you require complex passwords?	
Are passwords required to be rotated periodically?	
How often are passwords rotated?	

Is multi-factor authentication (MFA, 2FA) required to be used where available?	
Does the passwords policy require keeping passwords confidential?	
Physical Security Policy	
Do you have a documented physical security policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Privacy Policy	
Do you have a documented privacy policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Do you collect Personal Health Information (PHI)?	
Terms of Service Policy	
Do you have a documented terms of service policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Third Party Management Policy	
Do you have a documented third party management policy?	
Please provide link to supporting documentation	
How often is your policy reviewed?	
Do third parties have access to customer PII?	
Which third parties have access to customer PII?	
How do third parties comply with your security compliance standards?	