FORTRA™

CHECKLIST (DIGITAL GUARDIAN)

Digital Guardian Security Audit Checklist

12 Most Common Questions in a Client Data Protection Audit

Sophisticated cybercriminals have identified third party suppliers as a lucrative back door to steal sensitive information of major corporations. Consequently, all companies are face increasing pressure to button

up their cybersecurity presence from their corporate clients as well as regulators. Federal and state authorities are now recommending or requiring that major corporations do complete security audits of their third-party vendors. Companies that have trouble with the audits and can't demonstrate that they are adequately monitoring and protecting the sensitive data of their corporate customers run the real risk of losing those customers.

This checklist is based on our experience with wide a range of our customers who have been required to meet stringent partner or supplier data protection requirements and data protection security audits. It is designed to help your organization understand your "audit readiness."

Question	Question Why is it important?	Are you prepared?
1. Where is sensitive client data located?	Clients will want to be certain that you understand where their data will reside within your organization and what controls you have in place to track its movement. Data is not static; it may be stored on local servers, moved to individual desktops, and integrated with other data types. Expect clients to ask whether you have controls in place to prevent sensitive information from all possible egress channels, including email, cloud services, and removable drives.	☐ Yes ☐ No
2. Who in your organization will use client data?	Clients will want to know how widely their sensitive data is distributed and what controls are in place to limit access to it. Questions about data distribution can include how data is accessed, transmitted, shared, the screening processes used in hiring, and if any contractors or other non-employees will require access. This can extend to not only people, but also systems that use the data.	☐ Yes ☐ No
3. What do your users do with the data?	The core question in many audits is; "How will my data be handled?" While access control measures may limit information availability, users with legitimate access can copy data, incorporate it in other files, and move it to storage devices. Audit questions will focus on your ability to track data continuously, in any format. This includes use cases where sensitive data files are compressed, embedded in spreadsheets, or pasted as images into documents.	☐ Yes ☐ No

4. Which applications will access and use the data?	Once a client's information is within your systems, you need to demonstrate how you protect that data while in use, including its interaction with other applications that use the data to deliver information or products. For example, a design document may be entered into an inventory control system to ensure the necessary parts are available. Questions about application control will probe your ability to block unauthorized applications and processes from accessing, manipulating, and using data. This can include unknown applications which may be malicious, and legitimate applications which may put data at risk (e.g., peer to peer networking, file sharing).	☐ Yes ☐ No
5. When is the data at risk?	While static data can be encrypted, clients recognize that their sensitive information must also be used to deliver goods and services back to the client. Data is typically most at risk when it is used on endpoints. Here, users may take actions such as opening decrypted copies, copy data, send documents to others, or move sensitive data to other locations. Clients will ask for information about how you control your endpoints from external threats, such as malicious software and advanced threats, as well as internal threats, whether purposeful or inadvertent.	☐ Yes ☐ No
6. What controls can you provide to mitigate risks?	Knowledge workers have many demands on their time, relying on a policy document to protect sensitive client information is not enough. Clients will require evidence that you have controls in place to prevent the loss of the data for each use case and risk identified by you or the client. Controls should be automated and enforce policies in real time, allowing legitimate business processes to be conducted securely. Clients will need information on how you address insider and outsider threats, without requiring human judgment or intervention.	■ Yes ■ No
7. Can you monitor and provide an audit trail with respect to data transmissions?	"Trust but verify." Clients want to trust their business partners, but also require verification in the form of tamper-proof reports. Stringent policies are not enough; evidence of controls must be demonstrable. Questions about logging and auditing will include how you track all data access, use, and actions. This will include appropriate use, but may also show incidents when inappropriate were blocked. The latter can build confidence that the controls in place are effective.	☐ Yes ☐ No
8. Can you control or inhibit inappropriate data use?	A client can't be onsite at all times to protect their data, but want to know that you are constantly reminding your employees to be careful with sensitive information. Simply blocking an action, such as copying data to a removable drive or printing documents, may not reinforce to the user why the action could not occur. Be prepared for questions about real time controls that help reinforce the policies you have in place. This may be as simple as providing a prompt when blocking an action, or requiring auditable justification for approval prior to allowing an action.	☐ Yes ☐ No

9. Can you ensure that data is only accessed on a need to know basis?	Clients want assurances that access to their sensitive information is limited to those who require it and that it can't be shared without permission. Questions about access control are typically simple to answer. However, be prepared to demonstrate your controls for privileged users, such as system administrators. These employees possess elevated device privileges (root access). Clients will ask how you manage privileged users' ability to manage devices, while preventing access to the client's data on those devices.	☐ Yes ☐ No
10. What happens if one of your systems is compromised?	Attacks are inevitable; clients want to understand what controls are in place to contain a compromise. Audit questions will focus on how you recognize Indicators of Compromise (IoC), redundancy in IoC signatures, and threat intelligence used. If you have security solutions to detect external, network attacks, be prepared to demonstrate how that information is used to protect endpoints.	☐ Yes ☐ No
11. Can you expose any anomalous activity on devices that contain client data?	Sensitive data on endpoints is at risk of misuse, but also inadvertent errors. Clients will need information on how you recognize these actions and address common vectors such as phishing attacks. Be prepared to answer questions about controls for anomalous endpoint activity. Examples will include automated responses from common attack vectors such as phishing where an executable can be embedded in a seemingly benign attachment. The ability to detect, control, and block unauthorized processes and outbound network communications will be important.	☐ Yes ☐ No
12. What is your process for revoking usage privileges for users who are no longer authorized to access data?	As client teams add and lose members, it is necessary to demonstrate change control procedures that ensure former privileged users do not retain residual access to data.	☐ Yes ☐ No

How We're Different

Cloud-Delivered Date Protection

Cross Platform Coverage

Flexible Controls

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.