# Take the assessment

Implementing a robust cyber-resilience strategy is not difficult, but it takes a thoughtful approach. Understand where you are today so you can identify the biggest gaps and work toward eliminating them.

| | Scores | | |
|---|---|---|---|
| **About your data** | **5** points | **3** points | **1** point |
| a. Name all your corporate workloads and applications where your data is housed today.<br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| b. Identify all your cloud applications (note: many enterprises have 500+ cloud solutions in use that are not authorized or purchased through IT).<br>**5 points** if you conduct regular surveys with all business users to list what non-IT-endorsed cloud applications they are using<br>**3 points** if you have some of your non-IT cloud applications documented<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| c. Where is all your data located?<br>i. Public cloud<br>ii. Collocation facility<br>iii. Data center<br>iv. Edge<br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| d. Identify all your devices (including phones, laptops, network equipment, and BYO) as well as how data is accessed.<br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| e. Do you have identity management and access controls?<br>**5 points** if fully implemented<br>**3 points** if partially implemented<br>**1 point** if not implemented | ☐ | ☐ | ☐ |
| f. Have you identified risk factors down to the transaction level and have you implemented single-factor/multi-factor strategies to mitigate them?<br>**5 points** if fully implemented<br>**3 points** if partially implemented<br>**1 point** if not implemented | ☐ | ☐ | ☐ |

NetApp

| About your company | Scores | | |
|---|---|---|---|
| | **5** points | **3** points | **1** point |
| a. Do you have written current data security policies?<br><br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| b. What industry are you in and what regulatory or compliance requirements do you need to meet that are unique to your industry? **This is a bonus question**<br><br>**5 points** if you know the industry you are in (😉we know you know this already) and **3 extra points** if you know your specific compliance and regulatory requirements | ☐ | ☐ | |
| c. Do you have a well-documented and current business continuity plan?<br><br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| d. How frequently do you test your business continuity plan?<br><br>**5 points** for once a quarter<br>**3 points** for twice a year<br>**1 point** if you don't know | ☐ | ☐ | ☐ |
| e. How frequently do you communicate your data security policies to your entire organization?<br><br>**5 points** for once a quarter<br>**3 points** for twice a year<br>**1 point** if you don't know (or rarely) | ☐ | ☐ | ☐ |
| f. How frequently do you train your employees and contractors in your data security policies?<br><br>**5 points** for when onboarding and then twice a year<br>**3 points** for when onboarding and then once a year<br>**1 point** for I'm not sure | ☐ | ☐ | ☐ |
| g. How frequently do you test employees and contractors in security awareness through random practice incidents?<br><br>**5 points** for once a quarter<br>**3 points** for twice a year<br>**1 point** if you don't know (or rarely) | ☐ | ☐ | ☐ |

NetApp

| | Scores | | |
|---|---|---|---|
| **About the business** | **5** points | **3** points | **1** point |
| a. Have you defined clear roles and responsibilities for data security?<br>**5 points** if you have this in place for all your business units<br>**3 points** if you have this in place for some but not all business units<br>**1 point** if this is not well documented or in place | ☐ | ☐ | ☐ |
| b. Do your business leaders understand the implications of these SLAs?<br>Trick question – they may say "yes" but during an outage, you may realize it's "no" | | | |
| c. How quickly can you recover from any form of business disruption? Includes:<br>i. Malicious intent<br>ii. Natural disaster<br>iii. Device failure or loss<br>**5 points** if you have 15-minute RTO & RPO<br>**3 points** if you have 24-hour RTO & RPO<br>**1 point** if you need to call your tape storage provider to find out how fast they can restore backups | ☐ | ☐ | ☐ |
| **Roles and responsibilities** | | | |
| a. Do you have SLAs in place across the business?<br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| b. Do you have a policy in place to inform internal and external stakeholders in the event of a breach?<br>**5 points** if you have this already documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| c. Do you understand your legal and regulatory requirements with respect to privacy?<br>**5 points** if you have this clearly documented<br>**3 points** if you are in the process of documenting this<br>**1 point** if this is not well documented | ☐ | ☐ | ☐ |
| d. Are you able to respond quickly to changing regulatory or compliance requirements and modify policies as a result?<br>**5 points** if you can modify processes in 24 hours<br>**3 points** if you can modify processes in 7 days<br>**1 point** if this is a Herculean and manual effort | ☐ | ☐ | ☐ |

NetApp

| | Scores | | |
|---|---|---|---|
| **Data protection** | **5** points | **3** points | **1** point |
| a. To what level of detail are you able to prescribe data protection?<br>**5 points** if you can protect your data from ransomware with early detection and automated responses to threats<br>**3 points** if you can create an RPO of zero<br>**1 point** if you cannot do this | ☐ | ☐ | ☐ |
| b. Can you quickly identify and block malicious activities?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| c. Can you build protection around your data so that it can "self-protect" in minutes when a threat is identified?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| d. Are you able to monitor suspicious behaviors across your entire network?<br>**5 points** if you can monitor across all of your on-premises and cloud applications<br>**3 points** if you can monitor across some of your on-premises and cloud applications<br>**1 point** if this is not easy to do | ☐ | ☐ | ☐ |
| e. Is your data-at-rest protected?<br>**5 points** if you can protect across all of your on-premises and cloud applications<br>**3 points** if you can protect across some of your on-premises and cloud applications<br>**1 point** if this is not easy to do | ☐ | ☐ | ☐ |
| f. Is your data-in-flight protected?<br>**5 points** if you can protect across all of your on-premises and cloud applications<br>**3 points** if you can protect across some of your on-premises and cloud applications<br>**1 point** if this is not easy to do | ☐ | ☐ | ☐ |
| g. Can you identify and isolate the source of a threat quickly?<br>**5 points** if you can identify and isolate in minutes<br>**3 points** if you can identify and isolate in 24 hours<br>**1 point** if this is not easy to do | ☐ | ☐ | ☐ |

NetApp

| | Scores | | |
|---|---|---|---|
| **Supply chain** | **5** points | **3** points | **1** point |
| a. To what level of detail are you able to prescribe data protection?<br>**This is an awareness question, no answer needed.** | | | |
| b. Do you have extended policies and technologies that your supply chain vendors need to establish and follow?<br>**5 points** if you have extended policies in place and test your supply chain<br>**3 points** if you have extended policies in place but do not test your supply chain<br>**1 point** if you do not have extended policies in place | ☐ | ☐ | ☐ |
| c. Are you able to monitor integration points along your supply chain network to mitigate risk around potential entry threats?<br>**5 points** if you can monitor all integration points<br>**3 points** if you can monitor some integration points<br>**1 point** if this is not easy to do | ☐ | ☐ | ☐ |
| d. Do you have business continuity strategies in place with your supply chain vendors?<br>**5 points** if you have business continuity strategies in place and test them regularly<br>**3 points** if you have business continuity strategies in place and test them occasionally or rarely<br>**1 point** if you do not have this implemented | ☐ | ☐ | ☐ |
| **Technologies** | | | |
| a. Do you have an overall cyber-resilience technology platform that begins at the data layer or are you relying on external point solutions?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| b. Can you restore your mission-critical systems with a 15-minute RTO and a 15-minute RPO window?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| c. Are you able to, without difficulty, identify abnormal user behavior and block access?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |

NetApp

| | Scores | | |
|---|---|---|---|
| **Technologies** | **5** points | **3** points | **1** point |
| d. Are you able to, without difficulty, replicate to other regions to protect against outages and perform non-disruptive DR tests?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| e. Do you have the option of managing your own encryption keys for your assets in cloud storage?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| f. Does your current backup system offer write-once, read-many (WORM) file-locking to protect your data?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| g. Can you detect ransomware attacks in under two minutes and respond by immediately creating a Snapshot recovery point and blocking user storage access?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| h. Are you using AI to monitor the overall health of your systems, as well as abnormal behaviors?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |
| i. Can your current system use pattern-matching to identify sensitive information, such as PII, that should be purged or moved to another region?<br>**5 points** for yes<br>**1 point** for no | ☐ | | ☐ |

## Score yourself

**150-200 Points**
Congratulations, you are well on your way to becoming a fully cyber-resilient organization.

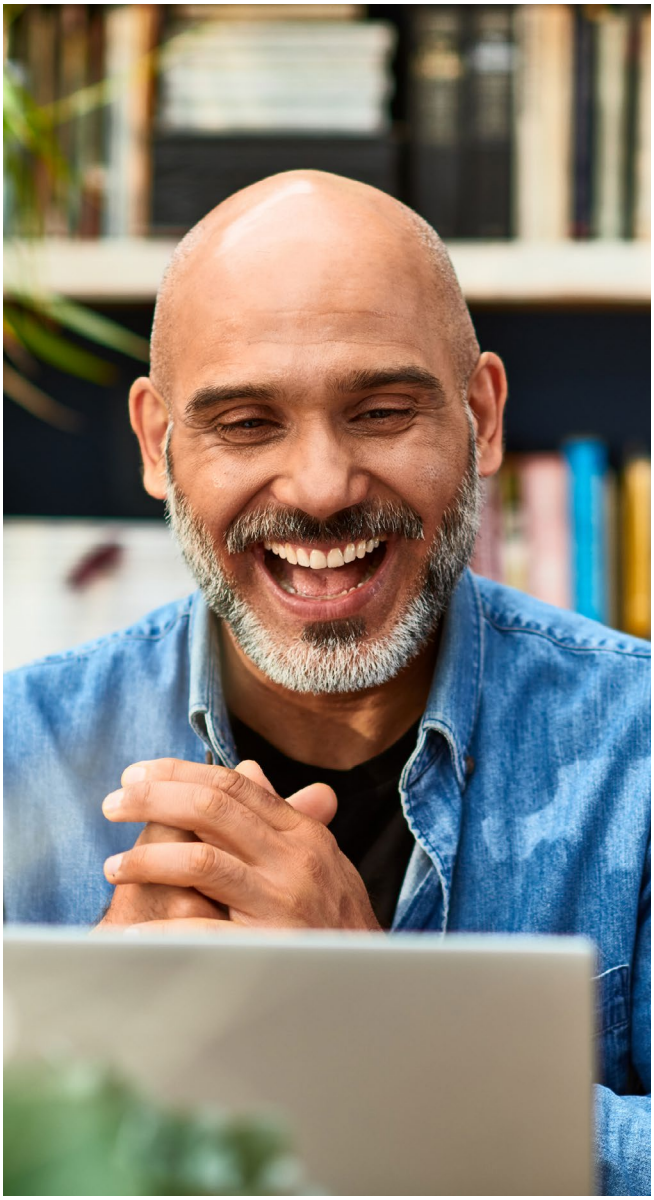
**Next step:** List any gaps and prioritize the most urgent. Speak to a Google Cloud specialist to get additional tips, hacks, and ideas.

**100-149 Points**
Well done. You have started your cyber-resilience journey and have made lots of progress.

**Next step:** Speak to a Google Cloud specialist about how to address the gaps in your cyber-resilience strategy. We have tools and methods available, as well as access to experts, to help you easily get the information you need to make great go-forward decisions.

**Less than 100 Points**
You're off to a good start – every journey needs a great beginning.

**Next step:** Speak to a Google Cloud specialist. We can simplify your journey. A workload analysis can be a great place to start. Learn more about how you can protect and secure your environments with this high-value, no-cost engagement.



NetApp

+1 877 263 8277