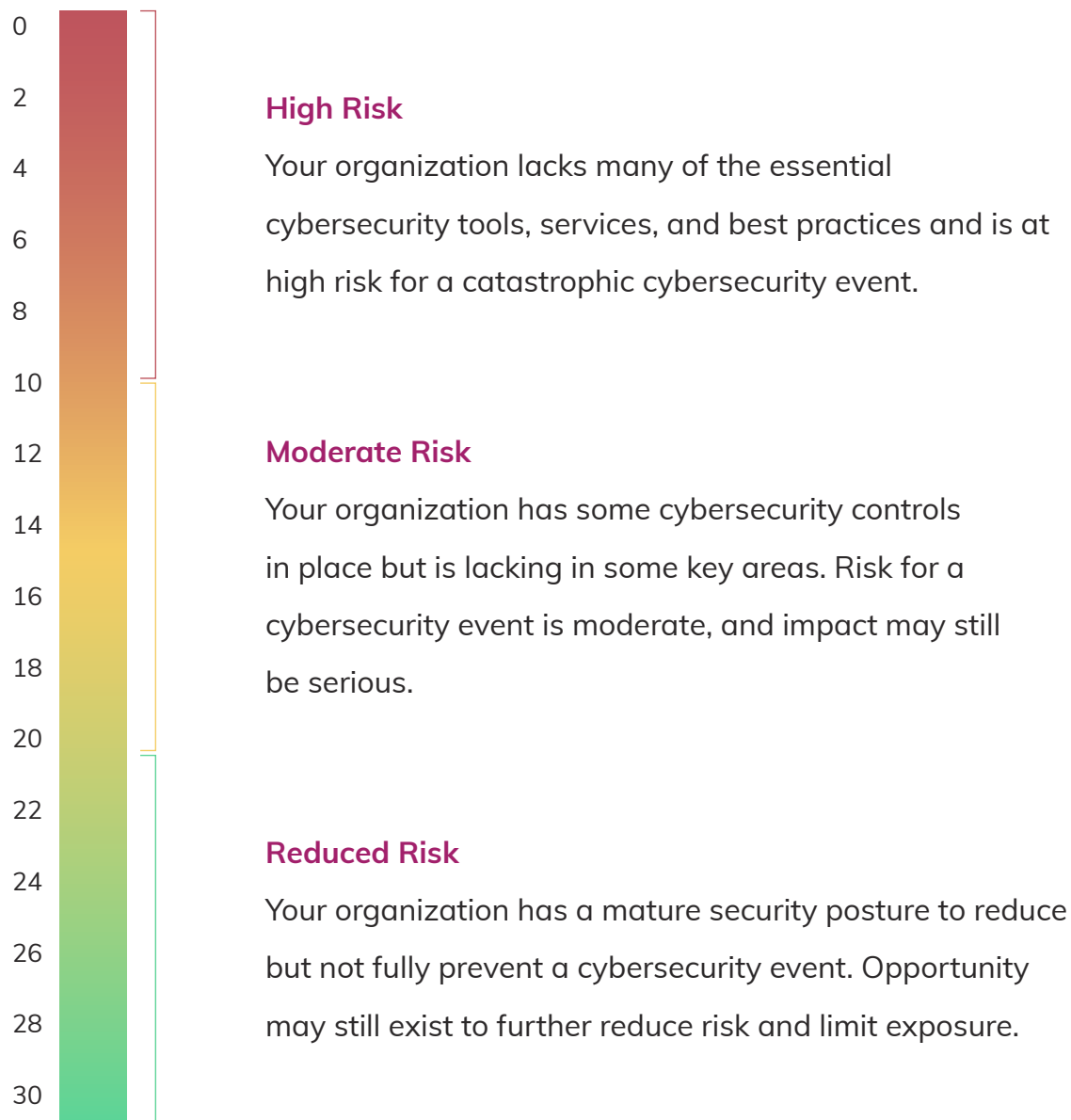


Cybersecurity Risk Assessment

Rank each statement below to complete a quick cybersecurity risk assessment on your business.

0 What's this?	1 Considered but not implemented or does not exist	2 Partially implemented or partially exists	3 Fully implemented and operational
Statement			Score
We educate our employees about the risks of cybersecurity, including regularly scheduled phishing awareness simulations.			<input type="checkbox"/>
An IT asset inventory exists and is up to date. Data has been classified and procedures exist to protect data access.			<input type="checkbox"/>
In the last three years, we have engaged in a cybersecurity risk assessment.			<input type="checkbox"/>
Our systems use multi-factor authentication (i.e., the use of a password and a second factor such as a one-time use code).			<input type="checkbox"/>
We enforce a strong password policy and require password changes on a regular basis across all applications and systems.			<input type="checkbox"/>
A cybersecurity strategy exists and is currently exercised.			<input type="checkbox"/>
Administrative or elevated privileges are assigned based on role or business need and reviewed regularly.			<input type="checkbox"/>
Endpoints are protected against malware and signature files are updated regularly.			<input type="checkbox"/>
A vulnerability and patch management solution exists and is in use.			<input type="checkbox"/>
Backup and restore procedures exist and are tested on a schedule consistent with our Information Security Risk Policy.			<input type="checkbox"/>
TOTAL			<input type="checkbox"/>

Total your score and compare it to the chart below. Where does your organization stand?



Note that a person or organization should never consider themselves fully protected from cybersecurity risk. Implementation of cybersecurity tools, services, and best practices serves to reduce the likelihood and impact of an event.

Reach out to Axians for a FREE consultation with an IT professional.

[Contact Us](#)

How Can Axians Help?

The primary purpose of a cyber-risk assessment from [Axians](#) is to help inform decision makers and support proper risk responses. An assessment will also provide an executive summary to help your organization make informed decisions about security.

Keeping information and assets safe from attack, damage, or unauthorized access requires implementing smart cybersecurity services, such as:

- ✓ Threat detection
- ✓ Threat prevention
- ✓ Intrusion protection
- ✓ Incident remediation
- ✓ Detailed forensics

Each service brings unique, tangible benefits to your business and bolsters your overall security posture. Fortunately, although the deck is stacked against the average business, your company does not have to be a statistic.

By partnering with Axians, you will have access to industry experts ready on day one to identify, implement, and [continuously improve your cybersecurity program](#), no matter the scope or scale of your business.



axians

READY TO LEARN MORE?

Contact the team at Axians to [schedule a free consultation](#).

Let a cybersecurity risk assessment from Axians help transform you from a reactive organization to a proactive one.

As we always say, IT is in our DNA—and this could be the single most important decision you make this year.

Contact Axians for your cybersecurity risk assessment today.

[**Contact Us**](#)

www.axians.us