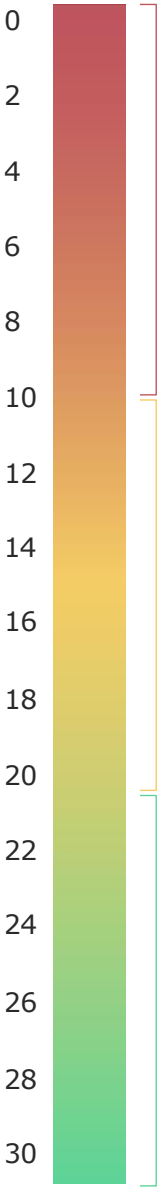
Cybersecurity Risk Assessment

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

0	1	2	3
What's this?	**Considered but not implemented or does not exist**	**Partially implemented or partially exists**	**Fully implemented and operational**

Statement	Score
We educate our employees about the risks of cybersecurity, including regularly scheduled phishing awareness simulations.	
An IT asset inventory exists and is up to date. Data has been classified and procedures exist to protect data access.	
In the last three years, we have engaged in a cybersecurity risk assessment.	
Our systems use multi-factor authentication (i.e., the use of a password and a second factor such as a one-time use code).	
We enforce a strong password policy and require password changes on a regular basis across all applications and systems.	
A cybersecurity strategy exists and is currently exercised.	
Administrative or elevated privileges are assigned based on role or business need and reviewed regularly.	
Endpoints are protected against malware and signature files are updated regularly.	
A vulnerability and patch management solution exists and is in use.	
Backup and restore procedures exist and are tested on a schedule consistent with our Information Security Risk Policy.	
TOTAL	0

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



High Risk

Your organization lacks many of the essential cybersecurity tools, services, and best practices and is at high risk for a catastrophic cybersecurity event.

Moderate Risk

Your organization has some cybersecurity controls in place but is lacking in some key areas. Risk for a cybersecurity event is moderate, and impact may still be serious.

Reduced Risk

Your organization has a mature security posture to reduce but not fully prevent a cybersecurity event. Opportunity may still exist to further reduce risk and limit exposure.

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.

Request an Introductory Discovery Call to Assess Your Cybersecurity Needs.

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 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