

Assessor Name : Mathieu Crosby  
Business Name : Potted Coffee  
Business Industry : Food services Annual

Name of Contact : Travis  
Email/Phone : Travis@pottedcoffee.com Date : 0  
2 . 1 3 . 2 0 2 5

## Digital Risk Checkup

Each year, it's crucial to assess your digital vulnerabilities. This involves a thorough review to identify potential weaknesses and strengthen your digital defenses. Just like an annual health checkup keeps you in good physical shape, a digital risk assessment ensures your online presence remains secure.

*Have you recently assessed the digital or cybersecurity risks to your business, people, and/or processes?*

1= not implemented, 5 = implemented. **1**

## Access Check and Minimal Permissions

Regularly inspect and limit who has access to your sensitive data and systems. This practice ensures that only those who truly need access can get it. It's like giving keys to your most trusted employees while keeping the rest of the keys locked away securely.

*Have you recently done an access review of who in your company have access to what systems or information?*

1= not implemented, 5 = implemented. **5**

## Backup Data and Software, then Test

Make sure to regularly save copies of your important data and systems, and don't forget to test

them to ensure they're working as expected. It's like creating a safety net for your digital world.

*Do you back up information? Have you recently tested those back-ups to make sure they work?*

1= not implemented, 5 = implemented. **3**

### **Double Layer Protection Shield**

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring two or more verification steps before granting access. It's like having both a key and a fingerprint to unlock your digital door, making it much harder for unauthorized users to get in.

*Do all of your critical business systems require two or three factors to log into them?*

1= not implemented, 5 = implemented. **5**

### **Digital Perimeter Guard**

A firewall acts as a virtual barrier, protecting your digital assets from unauthorized access and online threats. Think of it as a protective shield that filters out potential dangers and keeps your digital space safe.

*Do you have a network firewall to block unauthorized personnel from accessing your company computer network?*

1= not implemented, 5 = implemented. **3**

### **Draft a Digital Playbook**

Create a set of clear and comprehensive guidelines for how to protect your digital assets. Just like a playbook in sports, these policies and procedures ensure everyone on your team knows the game plan for cybersecurity and can follow it effectively.

*Do you have a cybersecurity incident response plan? Or an Information Security Policy?*

1= not implemented, 5 = implemented. **1**

### **Employee Bootcamp**

Equip all users with the knowledge and skills they need to navigate the digital landscape safely. This

training should start before they gain access and continue as they use digital resources. Think of it as preparing your team with the right tools and skills to face the challenges of the online world.

*Have you trained your personnel on cybersecurity threats in the past 12 months?*

1= not implemented, 5 = implemented. 1