MACPAGE™

Accessible
Approachable
Accountable

CYBERSECURITY CONTROLS REVIEW

A Cybersecurity Controls Review is an evaluation of your organization’s information security on networked systems. The review will result in prioritized recommendations that help identify areas of concern so that management can align controls with industry best practices and requirements.

If networked systems are mission-critical to business operations, then the implementation of Cybersecurity controls is essential to ensuring the confidentiality, integrity and availability of your organization's information. A Cybersecurity Controls Review is recommended every 12 - 24 months, depending on your organization’s level of risk.

WHY TO DO A CYBERSECURITY CONTROLS REVIEW WITH MACPAGE:

- We can help you obtain a more thorough understanding of your Cybersecurity posture.
- We can help you understand your Cybersecurity requirements. Depending on your industry, there are various regulatory and compliance requirements relating to Cybersecurity that Macpage can help you navigate.
- If you know you that you have Cybersecurity risks but don’t know where to start addressing them, Macpage can help you assess the priority of actions needed to be taken and recommendations for implementing each one.
- Macpage is a reputable, established firm, not a pop-up firm that will come and go with the security fad of the day.
- We can help you minimize the risks of a Cybersecurity incident. It is much less expensive to implement preventative controls than the cost of recovering from a Cybersecurity incident.

CYBERSECURITY QUESTIONNAIRE

- Is **all** of the confidential information transmitted or stored by your organization **encrypted**? This includes, but is not limited to, credit card or bank account information, medical or health records, and customer information such as social security numbers.
- Is adequate **vendor due diligence performed** on third party vendors, such as cloud-based services and data processors, **prior** to entering into a business relationship and updated on a **yearly** basis?
- Do you have a **written** Cybersecurity incident response plan that is tested and updated on a **yearly** basis? Does it include data breaches?
- Do you have a **formal** Information Risk Assessment that includes Cybersecurity risks? Is it updated on a yearly basis?
- Are **all employees** aware of their Cybersecurity roles and responsibilities? Are their responsibilities documented in Cybersecurity **policies**? Are employees **trained** on their Cybersecurity roles and responsibilities on a yearly basis?
- Do you regularly **audit** or **test** your Cybersecurity program to ensure that adequate controls are in place?

If you answered *“No”* to any of these questions, you should contact the Macpage Information Assurance Services team today to have a Cybersecurity Controls Review performed.