

## IT Security Baseline Assessment Checklist

IT security is a critical issue for any organization. Increased access to information and the ever-changing threat landscape has placed even more emphasis on all organization's ability to reduce their risk profile and proactively anticipate risks from both internal and external entities. The potential impact of an incident or breach can cause irreparable damage to an organization and its clients or supply chain.

Information Technology Departments, including Security and Risk roles, play a unique role as the managers and caretakers of some of the largest collections of critical systems, applications, and data. These systems, applications, and data often house information which is subject to strict controls and protections by law, including the data collected, stored, shared, and transmitted that was once very difficult to obtain.

Risk assessment tools, like this checklist, can assist in determining the gaps in an Information Security Program and provide guidance and direction for improvement.

### IT Security Baseline Assessment Checklist Questions

Item	Question	YES/NO
1	Are any changes in your organization's IT and business processes documented?	
2	Do you train your staff on security at least once a year?	
3	Does your organization have a documented and operational Incident Detection and Response (IDR) and Management Program?	
4	Does your organization have a Written Information Security Program (WISP) and Policy?	
5	Does your organization have an Incident Detection, Prevention and Recovery Controls, including Incident Playbooks to protect against incidents and threats?	
6	Does your organization have a Security Information and Event Management (SIEM) solution and program?	
7	Does your organization monitor, review or audit its Cloud services providers?	
8	Has your organization implemented a Third-Party Risk Management (TPRM) Assessment program?	
9	Has your organization implemented a Vulnerability Management (VM) solution and program?	
10	Is any of your organization's regulated or sensitive information stored on end points or other non-sanctioned locations without being encrypted?	

Disclaimer: The information in this document is intended for use as a guideline and does not constitute legal or professional advice. The information and suggestions have been developed from sources believed to be reliable. However, ASMGi accepts no legal responsibility for the correctness or completeness of this material.

## IT Security Baseline Assessment Checklist

11	Is your security program built around a formal framework such as CIS, ISO, NIST, etc.?
12	Are backups of your organization's data tested regularly in accordance with the backup policy in the event of a ransomware or malware incident?
13	Does your organization classify information assets in terms of sensitivity or criticality and a corresponding Data Loss Prevention (DLP) capability?
14	Does your organization have a documented and operational Business Continuity Plan (BCP)?
15	Does your organization have a documented and operational Disaster Recovery (DR) Plan?
16	Does your organization have documented user registration, user access procedures, and an Identity Access Management (IAM) solution?
17	Does your organization have Information Security Policies that are communicated to employees and vendors on a regular basis along with frequent training programs?
18	Does your organization keep an inventory of hardware and software assets that access and are accessible within the organization?
19	Does your organization maintain a current list of security policies, processes and procedures?
20	Does your organization test the security of your applications on a regular basis via Application Vulnerability Assessments and Penetration Testing?
21	Has your organization documented its compliance and contractual requirements, and its approach to meeting these requirements and conduct audits of these requirements?
22	Has your organization implemented rules for the acceptable use and sharing of confidential information?
23	Does your organization have a Cyber Insurance Policy?
24	Do you know the limitations and requirements of your Cyber Insurance Policy?

### ASMGi IT Security Baseline Assessment

As you work diligently to mitigate the myriad of threats to IT security, a Baseline Assessment can provide the critical insight and data you need to develop the most holistic strategy and road map.

Disclaimer: The information in this document is intended for use as a guideline and does not constitute legal or professional advice. The information and suggestions have been developed from sources believed to be reliable. However, ASMGi accepts no legal responsibility for the correctness or completeness of this material.



## IT Security Baseline Assessment Checklist

Performing a Baseline Security Assessment not only requires proven methodologies but an extensive and in-depth understanding of the security and information technology space. When your IT team lacks the expertise, resources or bandwidth to manage your security assessment initiatives, the security and IT professionals at ASMGi have the know-how and expertise to fill the gaps.

### **Security Assessment Services from ASMGi can help you to:**

- Understand your current risk posture as compared to leading practices and compliance requirements
- Document existing controls and security efforts
- Identify and quantify risks to your information assets
- Understand the strengths and weaknesses of your current defenses
- Examine weaknesses from the perspective of the attacker
- Align your IT risk management programs with your security and business goals
- Identify operational areas with high risk

Disclaimer: The information in this document is intended for use as a guideline and does not constitute legal or professional advice. The information and suggestions have been developed from sources believed to be reliable. However, ASMGi accepts no legal responsibility for the correctness or completeness of this material.



## IT Security Baseline Assessment Checklist

Email completed form to [info@asmgi.com](mailto:info@asmgi.com)

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Company: \_\_\_\_\_

Email Address: \_\_\_\_\_

Phone: \_\_\_\_\_

**An ASMGi representative will be in touch within 2 business days to qualify  
you for our**

***FREE Cyber Security Health Check and Assessment.***

Disclaimer: The information in this document is intended for use as a guideline and does not constitute legal or professional advice. The information and suggestions have been developed from sources believed to be reliable. However, ASMGi accepts no legal responsibility for the correctness or completeness of this material.

ATW-052019