CLOUDICA
Be sure of IT

Visit our Website | Contact us

# Calculate the Cyber Security Maturity Index

By conducting a cybersecurity maturity assessment using the outlined model, you gain valuable insights into your security capabilities. It allows you to identify gaps, allocate resources effectively, and prioritize cybersecurity initiatives.

## How to use?

Assign a score of 1-5 to each question based on your demonstrated level of maturity. For instance, a score of 1 indicates a basic level of maturity, while a score of 5 represents an advanced level of maturity.

Next, calculate the average score for each category by summing the scores for all questions in that category and dividing it by the total number of questions in that category. This will provide the maturity level for each category.

Finally, calculate the overall cybersecurity maturity index by averaging the maturity levels across all categories. This index will give you a comprehensive view of your cybersecurity posture.

## Levels of maturity

**Level 1: Basic**
You have minimal cybersecurity processes in place and face a high risk of cyberattacks. Immediate attention and significant improvements are necessary to enhance your security posture.

**Level 2: Developing**
You have some cybersecurity processes in place but require substantial improvements to reach a mature state. You should focus on strengthening your policies, procedures, and security controls.

**Level 3: Mature**
You have a solid cybersecurity posture, but there is still room for improvement. You should continue enhancing your processes, monitoring capabilities, and incident response practices.

**Level 4: Advanced**
You have a strong cybersecurity posture and are well-prepared to address potential threats. However, you should remain proactive and stay abreast of emerging threats and technologies to maintain your advanced level of security.

**Level 5: Leading**
You have a comprehensive and mature approach to cybersecurity. You are a leader in cybersecurity best practices and continually innovate to stay ahead of

## Why is this important?

Assessing your cybersecurity maturity is crucial for evaluating your current security posture and identifying areas for improvement. By considering governance and risk management, access control and identity management, threat detection and response, and infrastructure and data protection, you can determine your cybersecurity maturity level.

The calculated cybersecurity maturity index provides a clear roadmap for enhancing your security capabilities, reducing vulnerabilities, and safeguarding your valuable assets from cyber threats. Embracing a proactive approach to cybersecurity maturity assessment is an essential step toward building a robust and resilient security foundation for your organization.

## 1. Governance and Risk Management:

A score of 1 indicates a basic level of maturity, while a score of 5 represents an advanced level of maturity.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Does the organization have a cybersecurity strategy and policy that aligns with business goals and objectives? | ○ | ○ | ○ | ○ | ○ |
| Is there a clear process in place for identifying and assessing cybersecurity risks? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for regularly reviewing and updating cybersecurity policies and procedures? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for reporting cybersecurity incidents to relevant authorities? | ○ | ○ | ○ | ○ | ○ |

## 2. Access Control and Identity Management:

A score of 1 indicates a basic level of maturity, while a score of 5 represents an advanced level of maturity.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Is there a process in place for managing user access to IT systems and data? | ○ | ○ | ○ | ○ | ○ |
| Are users authenticated and authorized in accordance with policies and procedures? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for managing user credentials, including password management? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for regularly reviewing and updating access control policies and procedures? | ○ | ○ | ○ | ○ | ○ |

## 3. Threat Detection and Response:

A score of 1 indicates a basic level of maturity, while a score of 5 represents an advanced level of maturity.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Is there a process in place for monitoring IT systems for security events and incidents? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for responding to security incidents? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for testing and validating incident response plans? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for learning from past incidents and improving incident response processes? | ○ | ○ | ○ | ○ | ○ |

## 4. Infrastructure and Data Protection:

A score of 1 indicates a basic level of maturity, while a score of 5 represents an advanced level of maturity.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Is there a process in place for regularly patching and updating IT systems? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for monitoring and managing network and system security? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for protecting sensitive data, including encryption and data masking? | ○ | ○ | ○ | ○ | ○ |
| Is there a process in place for regularly testing and validating backup and recovery processes? | ○ | ○ | ○ | ○ | ○ |

**Your Cyber Security Maturity Index:** .....