January 2019

ETHISPHERE
GOOD. SMART. BUSINESS. PROFIT.
6991 E. Camelback Rd. Ste. B-350
Scottsdale, AZ 85251
p: 888.229.3207

Frequently Asked Questions about the *Cybersecurity Essentials Assessment*

How the *Cybersecurity Essentials* Service Works

1. What is the *Cybersecurity Essentials Assessment*?

The Cybersecurity Essentials Assessment is a service to measure the maturity of an organization's cybersecurity approach. It is based on leading cybersecurity practices outlined by the U.S. National Institute of Standards and Technology (NIST) with input from information security experts and senior cybersecurity leaders from companies around the world. The assessment aligns to key controls in the NIST Cybersecurity Framework first issued in 2014 and broadly deployed by organizations in the U.S. and around the world. The Framework incorporates and references leading standards and guidance, including ISO 27001, and NIST 800-53 and 800-171, among others.

The service includes an **Online Self-Assessment** providing insights into the maturity of the processes and practices your company currently has in place and is benchmarked against 25 subcategories or controls out of the 98 subcategories in the NIST Cybersecurity Framework. These 25 were chosen because our experts view these as foundational and generally companies of all sizes should understand their application of these controls, the maturity in their approach and focus on improving in these areas. You will receive a **Summary Report** of your results. The assessment offers a way to understand the strengths and gaps in your cybersecurity approach so that you can make improvements for better management of cyber risks. If you are interested in understanding your organizations maturity with respect to all 98 subcategories or controls in the NIST Cybersecurity Framework, please contact your TechSpark contact or support@ethisphere.com.

2. Will I need to agree to Terms of Use to access the *platform*?

As part of your registration on the platform and enrollment in your assessment, you will be asked to review and agree to the provided Terms of Use, which applies to all users of the *Cybersecurity Essentials* service. Access and use of the services, platform and assessments offered by Ethisphere are subject to the Terms of Use. By accessing or using the service, you represent and agree that you and your organization have read, understand, accept, and agree to be bound by the Terms of Use.

3. Why should my organization participate in the *Cybersecurity Essentials Assessment*?

Cyber attacks can put companies at financial, reputational and legal risk. *The Cybersecurity Essentials* service helps your organization mitigate these risks by assessing current systems in place to prevent data breaches, and identifying areas where improvement is needed.

An organization that develops an effective cybersecurity program can avoid costly litigation, penalties, and reputational harm, while enhancing its position as an organization that places the protection of its sensitive and private information as a top priority, differentiating itself from competitors, making the organization more attractive to investors, business partners, potential employees, and customers alike.

6991 E. Camelback Rd. Ste. B-350
Scottsdale, AZ 85251
p: 888.229.3207

4. Who is The Ethisphere Institute, the organization behind the service?

Ethisphere defines and advances business practices in high risk areas that fuel corporate character, marketplace trust, and business success. We have deep expertise in defining, measuring and implementing effective controls using data-driven insights.

Our services help organizations embed a cycle of measurement, monitoring and improvement to build and strengthen effective compliance and risk management programs. These services include assessments for ethics and compliance, corporate culture, cybersecurity, anti-corruption, and the protection of trade secrets and intellectual property.

Our assessment methodology and technology platform combine to provide an efficient workflow, a high-level of quality control, and deep insight into the controls of organizations.

5. What do you mean by a 'cybersecurity program'?

Every organization should have a cybersecurity program or "management system" consisting of controls to prevent, detect and mitigate adverse cyber events. The *Cybersecurity Essentials* service offers organizations the ability to assess their current policies, processes and technology (controls) against leading guidance to determine what gaps, if any, they have in their policies, processes and technology to protect its information security systems and data.

6. What languages are available for the *Cybersecurity Essentials* service?

The *Cybersecurity Essentials* service is available in English and Japanese.

7. How long does it take to go through the *Cybersecurity Essentials Assessment*?

The *Cybersecurity Essentials* Assessment takes some initial preparation and document compilation, and then less than 60 minutes to complete.

8. Will my organization be required to produce documents? Where do I upload my organization's documents?

You will not be required to upload documents. TechSpark is providing you an opportunity to assess against the NIST Cybersecurity Framework. When Ethisphere provides this service generally, its experts review a respondent's answers, any uploaded documents provided for verification and also conduct an interview of key people to discuss each of the controls included in the self-assessment. A list of suggested documents is available in the platform if you want to see what types of documents are usually provided for verification. All information and documentation you provide to Ethisphere will be treated as confidential.

9. Who in my organization should be involved in *CREATe Leading Practices for Cybersecurity Essentials*?

6991 E. Camelback Rd. Ste. B-350
Scottsdale, AZ 85251
p: 888.229.3207

Typically, one person will manage your organization's involvement in the *Cybersecurity Essentials* service. That person should be primarily responsible for the organization's cybersecurity and/or information security program. Knowledge of the organization's information security policies, processes and controls is critical to an accurate assessment and completion of the service. As needed, and as suggested below, that person can draw on the experience of others in the organization to answer specific questions.

For completing the Self-Assessment, you should strive to include key people from different areas of the organization who contribute to building and implementing your cybersecurity program, including:

- Information Technology
- Security
- Compliance
- Legal (if separate from the compliance team or function)
- Finance
- Human resources/training
- Marketing/sales/business development
- Sourcing/procurement/supply chain

How Your Organization is Evaluated

10. How does the online Self-Assessment work?

The online Self-Assessment asks a series of specific questions about the policies, processes and controls that an organization has in place to manage cyber risk and to protect private and sensitive data. All 25 questions in the assessment are aligned to key subcategories in the NIST Cybersecurity Framework. A maturity score from 1 to 5 is automatically generated based on the organization's score for each category and function.

11. What kind of information or report will Ethisphere provide once my organization has completed the Self-Assessment?

After completing the Self-Assessment, your organization will receive the following:

- Maturity scores in each of the functions and categories that comprise the Self-Assessment;
- An overall score; and,
- A Summary Report that benchmarks your scores against blinded, aggregated scores from other participating organizations.

How the *Cybersecurity Essentials* Service Addresses Cyber Readiness

12. Is the *Cybersecurity Essentials service* intended to cover all aspects of cyber risk?

6991 E. Camelback Rd. Ste. B-350
Scottsdale, AZ 85251
p: 888.229.3207

The *Cybersecurity Essentials* service is focused on improving the management systems that organizations have in place to deal with cyber risk and to help ensure compliance. It is designed to be flexible enough to deal with various kinds of cyber risk in different sectors and situations. While each cybersecurity program must be designed with an organization's unique circumstances, attributes, risk profile, and access to and use of sensitive data in mind, the *Cybersecurity Essentials* service can help you gain insight into the strengths and weaknesses of your program. While our full Cybersecurity assessment aligned to the 98 subcategories of the NIST Cybersecurity Framework is more comprehensive, the Essentials service will provide key insights on foundational issues that every organization should understand about its approach to cyber risk management.

Security for *Cybersecurity Essentials* Participants

13. How will Ethisphere keep organization information secure?

The Self-Assessment responses, any information you provide within your Self-Assessment including documents and comments, and information Ethisphere provides to you are kept on a secure, password protected server. You will be required to enter a unique multi-factor authentication to access. Only you, the Ethisphere evaluator(s), Ethisphere administrative personnel will have access to it on a "need-to-know" basis. You will have access to the assessment results and report through a unique user ID and password.

The *Cybersecurity Essentials* online service is hosted on Microsoft Azure servers (Azure). Azure is a world-class enterprise-level hosting service provider with data centers around the world, mirrored services in the USA, EU, Asia, and South America and an immense focus on protecting data. Through Azure, bandwidth, security, redundancy, system capacity, backup and concurrent usage issues are managed automatically.

All data used for internal analysis to generate metrics and reports will be stored on a single machine in a secure server room. The data will be stored in MySQL tables on this machine. MySQL has sophisticated security schemes to protect data. Without direct physical access to the data files, defeating this security is very difficult. Remote access over IP will be limited to Ethisphere administrative personnel and specific remote IP addresses. All actual data will be encrypted at rest and in transit utilizing AES 256 and SSL certificates.

14. Who do I contact if I need help?

Contact support@ethisphere.com.