Frequently Asked Questions about the *Ethisphere Cybersecurity Maturity Assessment*

How the *Ethisphere Cybersecurity Maturity Assessment* Service Works

1. What is the *Ethisphere Cybersecurity Maturity Assessment*?

The *Ethisphere Cybersecurity Maturity Assessment* is a service to assess and improve 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 service aligns to 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, among others.

The service includes:

1) **An Online Self-Assessment** providing insights into the processes and practices currently in place and benchmarked against the 98 controls in the NIST Cybersecurity Framework;
2) **An Independent Evaluation** including a review of the Self-Assessment, any verifying documents, and a discussion conducted by telephone by an Ethisphere expert to further review and benchmark current processes against the 98 controls; and,
3) **A Summary Report** of the results with recommendations and a roadmap for improving the program.

2. Will I need to agree to Terms of Use to access the *Ethisphere 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 *Ethisphere* service, including anyone for your organization or a Referring Company. 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. Who is The Ethisphere Institute, the organization behind the service?

Ethisphere® is the global leader in defining and advancing the standards of ethical business practices that fuel corporate character, marketplace trust and business success. We have a deep expertise in measuring and defining core ethics standards using data-driven insights that help companies enhance corporate character and believe integrity and transparency impact the public trust and the bottom line of any organization.

Our *Ethisphere Maturity Assessment* services help companies embed a cycle of measurement, monitoring and improvement to build and strengthen effective compliance and risk management programs. These services include:

- Cybersecurity
- Intellectual Property Protection
- Trade Secret Protection
- Anti-Corruption

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.

4. 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 *Ethisphere Cybersecurity Maturity Assessment* is a service that 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.

5. What languages are available for the *Ethisphere Cybersecurity Maturity Assessment*?

The *Ethisphere Cybersecurity Maturity Assessment* is available in English and Japanese.

6. How long does it take to go through the *Ethisphere Cybersecurity Maturity Assessment*?

The *Ethisphere Cybersecurity Maturity Assessment* is a multi-step service. The first step, the online Self-Assessment, takes some initial preparation and document compilation, and then approximately 90 minutes to complete. The second step – the Independent Evaluation – takes about 90 minutes. In the weeks that follow the Independent Evaluation, Ethisphere will send the organization a summary report with an action plan for improvement. The process from completion of the Self-Assessment to receipt of the Summary Report can take as short as a few weeks and generally should take less than three months.

7. Will my organization be asked to produce documents? Where do I upload my organization’s documents?

Yes. Ethisphere experts will ask you to produce documents before the Independent Evaluation, such as your information security policy or procedures, a sample training, etc., to help understand your cybersecurity program. You will be able to upload those documents to the secure Ethisphere platform. A full list of suggested documents is available in the Ethisphere platform. Instructions on how to upload documents are contained in the *Respondent Instruction Guide* located in the Ethisphere platform’s Resources tab. These documents will be seen only by the Ethisphere experts and your Referring Company. All information and documentation you provide to Ethisphere will be treated as confidential and will only be shared with your Referring Company. Please note that if you do not provide documents to support your Self-Assessment responses, your Independent Evaluation scores will be negatively impacted. You may also upload redacted copies of the requested documents on the “My Documents” tab and/or share the unredacted documentation during a secure webcast during the independent evaluation meeting.

Not every question requires a supporting document. You may mark the document that is related to a particular answer at the question level if you have uploaded documents previously to the My Documents tab via the Dashboard. Please see platform Instructions for further details.

8. Who in my organization should be involved in the *Ethisphere Cybersecurity Maturity Assessment*?

Typically, one person will manage your organization's involvement in the *Ethisphere Cybersecurity Maturity Assessment* 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, procedures 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 a cross-functional team within the organization to answer specific questions.

The person who manages the completion of the Self-Assessment should also manage the Independent Evaluation, which involves a discussion with an Ethisphere expert evaluator.

For both completing the Self-Assessment and participating in the Independent Evaluation, 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/In-house counsel
- Finance
- Human resources/training
- Marketing/sales/business development
- Sourcing/procurement/supply chain

When completing the Self-Assessment in the platform, you will find a field labeled "contributor" at the question level. This is an optional tab provided to note if there is someone who has helped you to complete the question. You do not need to complete this field; however, it may be a useful record if completing the assessment across multiple years and/or during the independent evaluation review.

How Your Organization is Evaluated

9. 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 protect private and sensitive data. All 98 questions in the assessment are aligned to the subcategories in the NIST Cybersecurity Framework. A maturity score from 1 to 5 is automatically generated based on the organization's responses for each function, category and subcategory as outlined in the NIST Cybersecurity Framework.

When you start the assessment there are questions concerning the scope or coverage of your assessment. It is useful to think about this before starting. Are you answering the questions on behalf of your location in the law firm, for all locations in the United States (U.S.), or all locations globally (if you have locations outside the U.S.). There are also questions about which department you are in, and if you are doing the assessment considering all departments in the firm or just thinking about one department. Typically, you will be thinking about all departments in your firm in a specific geography as you answer the questions. Unless you have been instructed otherwise, you should assume the scope for the assessment is the U.S.

10. How does the Independent Evaluation work?

In most instances, the Independent Evaluation will be conducted by telephone and will include a review of provided documents. As noted above, failure to provide documents will negatively affect your organization's scores. The Independent Evaluation covers the same subcategories/controls in the NIST Cybersecurity Framework answered in the Self-Assessment. The Independent Evaluation is conducted as a shared learning discussion and is designed to help organizations better understand the level of maturity of the practices they have in place to manage and address cyber risk.

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

After completing the *Ethisphere Cybersecurity Maturity Assessment* service Self-Assessment and Independent Evaluation, your organization will receive the following:

- Maturity scores in each of the functions and categories that comprise the Self-Assessment and Independent Evaluation;
- An overall score; and,
- A Summary Report that benchmarks your scores against blinded, aggregated scores from other participating organizations. It also includes a summary of our recommendations and an action plan for improvement.

Your Referring Company will also receive this information.

Security for the *Ethisphere Cybersecurity Maturity Assessment* Participants

12. How will Ethisphere keep organization information secure?

The Self-Assessment and Independent Evaluation responses, any information you provide as part of the Independent Evaluation, and information Ethisphere provides to you are kept on a secure, password protected server. Each client organization has a separate eco-system that requires unique multi-factor authentication to access. Only you, the Ethisphere evaluator(s), Ethisphere administrative personnel and your Referring Company will have access to it on a "need-to-know" basis. You will have access to the assessment results, any uploaded documents and reports through a unique user ID and password.

Ethisphere's online services are 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.

13. Who do I contact if I need help?

Contact support@ethisphere.com.