A SPECIAL REPORT:
RISK MANAGEMENT AS A TEAM SPORT
In Partnership with OPUS
Our Mission Statement

The Ethisphere® Institute 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. Ethisphere believes integrity and transparency impact the public trust and the bottom line of any organization. Ethisphere honors superior achievements in these areas with its annual recognition of The World’s Most Ethical Companies®, and facilitates the Business Ethics Leadership Alliance (BELA), an international community of industry professionals committed to influencing business leaders and advancing business ethics as an essential element of company performance. Ethisphere publishes Ethisphere Magazine and hosts ethics summits worldwide.
1. The Chief Compliance Officer’s Perspective on Risk
   Interview with Jeffrey Eglash, Vice President, Ethics and Compliance, Nokia

2. Prioritizing Risks Across an Organization
   Interview with John Masserini, Chief Information Security Officer, Millicom

3. The CFO’s Perspective on Risk
   Interview with Laurel Krzeminski, Chief Financial Officer, Granite Construction

4. Managing Third Party Risks Across an Organization
   Written by G. Sonny Cave, Michael Zuraw, Shashwat (Shash) Dave, Mark N. Rogers, ON Semiconductor

5. Today’s High-Tech House of Cards
   Written by Aarti Maharaj, Ethisphere

6. Getting a Handle on GDPR
   Interview with Carolyn Herzog, EVP & General Counsel, and Tim Fitzgerald, Chief Information Security Officer, Arm
Today it’s clear that the companies with the most effective governance, risk and compliance programs get there through an integrated approach to risk across the organization. They treat those leaders who are responsible for managing key enterprise risks, including the general counsel, chief compliance officer, chief information security officer, CFO, and so forth, as partners to the business. These leaders see themselves enabling efficiencies, not creating obstacles – they respond with a “here’s how” and not a “no.”

When we work with, or speak to, the leaders of global companies throughout the year, there are a few consistent themes that arise from those that have best in class programs around compliance, ethics, risk management and similar areas. The most prevalent of those themes comes down to the idea that risk management is a team sport. Each of these leaders must not only communicate the importance around the work that they and their teams do to the rest of the company, but they must also work to understand the priorities and reasons behind the work their counterparts do.

This may be an overly simplistic idea in concept, but in practice it becomes far more difficult. Competing priorities, heavy workloads and responsibilities and other issues can all get in the way of effectively communicating and collaborating with colleagues across the company.

In order to help learn from companies that are doing it well, including some recognized as 2018 World’s Most Ethical Companies Honorees, Ethisphere and Opus have partnered to create this Special Report which highlights, in their own words, what company leaders are doing to build best in class ethics, compliance, governance and risk management programs.

Over the following pages you will hear from various leaders from Nokia, ON Semiconductor, Millicom, ARM and Granite Construction who share what they’re focused on when it comes to risk management, and how they work with others across the company to create strong and effective programs.

We hope this publication is helpful to you as you develop your own programs, and we look forward to hearing from you throughout the year to learn from your own experiences in this important area.

Sincerely,

Manny Conti  
Chief Executive Officer  
Opus

Erca Salmon Byrne  
EVP, Governance and Compliance and  
Executive Director, BELA  
Ethisphere
The Chief Compliance Officer’s Perspective on Risk

An Interview with Jeffrey Eglash, Vice President for Ethics and Compliance, at Nokia

Interview by
Aarti Maharaj

The Chief Compliance Officer is one of the key roles combating some of the most ever present, enterprise-level risks that a global company faces. Below, Jeffrey Eglash, who leads compliance for Nokia, talks through some of the challenges he faces, and how compliance leaders can help mitigate key risks via collaboration and communication with others across the company.

AM: What are some of the top two or three risk areas or challenges that you’re currently focused on from a compliance perspective at Nokia?

JE: I think the answer to that would probably change by the day, and maybe by the hour, depending on the issues that are in front of me at the moment. There are a few things that come to mind now.

First is around scope: Ensuring that our compliance program gets to all the corners of our organization. And by that I mean we have a number of joint ventures with different ownership stakes and so making sure we have the right compliance program, culture and infrastructure in place with the joint ventures is important. It also relates to what we call “ServCos,” or service companies. In our industry, these are companies that handle a lot of the day-to-day servicing needs of our customers, but where we still maintain some element of ownership or control of those organizations and so we have to ensure that those ServCos have the right compliance structure. Also, we’re frequently buying new businesses. We’re active in M&A and so we need to make sure that we perform due diligence and proper integration on newly acquired companies.

And then finally we’ve got a lot of really small and remote sites in different corners of the globe and so we need to make sure we reach all of those sites as well and have the right controls in place. So all of that and more makes up what I call the “scope” issue.

Other risks are narrower issues that come up with some frequency. One interesting example of that is around customer entertainment and hospitality. We get a lot of requests in from our business and commercial teams to bring customers to different sites or to offer entertainment or hospitality to our customers. Many of our customers are private, however many are state owned enterprises. Some are government enterprises. And so we need to make sure we strike the right balance and have the right rules around hospitality that balances in who the customer is and what the risk profile is.

Third, I would say people challenges. When we have compliance openings in some areas like China, India, Middle East, etc, finding the right compliance professionals to carry out sensitive investigations and to lead compliance programs has really proven to be a challenge. We’re used to finding great talent in mature markets in North America and Europe and so forth, but when we have openings in certain markets, finding top talent has proven to be challenging.

I know you said two or three but of course I can’t limit myself and so the final risks I will mention are investigations and hotline complaints, such as concerns that get raised that are really more of an HR nature than pure compliance or anti-corruption issues. We get a lot of complaints that come in through the compliance system that when you look right at them or parse them they’re really HR investigations.
On the one hand we want to make sure that they get addressed. If our employees are utilizing our complaint reporting channels then there is an obligation on our part to address them in a prompt, thorough and objective manner. We carry out proper investigations and if we find that there is an issue then we need to address it. We can’t let those cases fall through the cracks.

At the same time, as the Chief Compliance Officer, my focus has to be on those cases and those investigations that pose the greatest systemic risk to the company. And so how we manage this very large volume of internal HR complaints properly without losing focus on the cases that really matter the most for the company, those which raise the most serious issues, has been a big issue for us.

AM: So with all these risks being ever present to an organization, what advice or lessons in managing some of these challenges can you offer to other organizations dealing with the same things?

JE: I mentioned a number of different challenges, and I could try and give advice on each, but I would respond by offering a couple highlights.

First when I talk about the scope of compliance coverage, and I was mentioning merger & acquisition risk, one thing that I think is important is some healthy skepticism about the companies that you’re acquiring. When acquisition targets come along it’s sort of easy to be seduced by thinking, “Okay, this is the greatest company. They have the greatest products, everything about them is perfect. We must have them as part of our portfolio.”

But my experience has taught me that often you really want to have a healthy skepticism about those companies and really get under the covers. You need to look and see as much as you can about the companies, the people, the products, the programs and the culture and make sure it’s all a good fit. Make sure there aren’t any hidden skeletons or buried skeletons. And often when you do scratch beneath the surface you find that things aren’t quite what they appear.

It’s so important to get into those issues as early as possible and to think about how you’re going to get your arms around the problem. You need to think through whether there are financial or contractual processes you can put in place to limit your risks or whether there are remediation steps that need to be taken in order to minimize the risks to you as the acquiring company.

AM: Where do 3rd party related risks rank as they relate to those you mentioned? Do you see them increasing/decreasing in the coming years?

JE: I think third party risks are what you might call a hardy perennial. They’re always going to be there. I don’t have a crystal ball and I don’t know if challenges relating to third parties are going to increase or decrease but I would say with some degree of confidence it’s going to be a longstanding and perpetual concern.

I don’t have the statistics in front of me, but I’m sure that any analysis of previous enforcement actions around the FCPA and similar statutes would show that a very large, outsized proportion of enforcement actions for improper payments and similar actions relate to the activities of third parties.

So for any company including ours that has extensive reliance on third parties, whether you call them agents, consultants, resellers, distributors, etc, for any company that relies on such third parties you absolutely have to identify that area as one of the most, if not the most, critical risk area that needs to be addressed in terms of due diligence, monitoring, oversight and so forth.

AM: Do you have any predictions you might want to lend around key compliance risks you see coming around the corner for companies?

JE: Well I wish I did have that crystal ball. I would say that while in our program we focus intently, as we must, on anti-bribery, anti-corruption and improper payments, we are very mindful of the risks and the growing complexity in privacy, in data protection and security. Those are top of mind. I guess I would add to the list money laundering and trade controls as areas of increasing concern.

And then going back to that phrase I used before, hardy perennials, conflict of interest is one that can make serious fraud or controllership or embezzlement issues arise. So while it’s easy as a chief compliance officer to be intently focused on anti-bribery risks and the FCPA, there are so many other risks out there. And when I look at GDPR and data breaches and so forth they’re constant reminders that there are other huge risk areas to be aware of.

AM: Do you ever work or collaborate with other C-level leaders such as GC, HR, etc, in order to communicate these risks with them?

JE: I do. One of the things I try to do when I communicate with the leadership, whether it’s the executive leadership team or the board level, I try to bring to mind the enforcement environment that we’re currently operating in. Going back to my last point, while a lot of the focus is around FCPA, I understand and I know they are keenly aware of this broad range of risks as well.

In our company there are some risks that the compliance team owns and is directly responsible for, but there is an array of other risk areas where we don’t directly own them but we will coordinate with the other subject matter experts across the company to make sure that the right training, communications, policies and risk mitigation plans are in effect.

And so the degree to which I communicate on various risk areas with the leadership really depends on the degree to which I have direct responsibility over that particular risk.

AM: So how can leaders across roles work collaboratively to help identify and mitigate the greatest risks facing the company?

JE: Well for me again going back to my last answer, there are areas where Compliance has primary responsibility, but I also try to take a broad view and try to make sure in other areas there aren’t any gaps in terms of the training and in terms of the controls and so forth.

One key point is to ensure the various leaders avoid having this narrow and siloed view of the world. You have got to look more broadly and not assume that just because somebody else is
responsible for something you can’t do more on that issue as well. I also think companies like ours are increasingly looking at enterprise risk and trying to overcome this silo effect. They’re trying to understand and put together overarching risk registers that gather in one place all the risks that reside in different parts of the organization and make sure that there are owners and there are good controls in place to address each of them.

Because as you point out, the increasing complexity in so many of these areas is so great that I just don’t think you can have one individual, whether it’s the chief compliance officer or general counsel or chief risk officer, be knowledgeable about every aspect of risk that a multinational organization is facing these days.

AM: Do you have any advice as to how other companies can achieve this level of collaboration across function, which often can be difficult given the responsibilities and time commitments for these various executives?

JE: Well I think the answer is largely embedded in your question, which is collaboration and communication. I know in our organization we collaborate and communicate to an extraordinary degree, and the reason is that we are constantly talking with one another about who’s doing what to make sure everything is covered.

While it’s fine to have written rules and so forth, everyday something is going to come up that fits in between risk ownership, or doesn’t fit neatly into an organization chart, or comes up through a different part of an organization. So it’s just imperative, especially in our company where we’ve got hundreds of lawyers spread out all over the globe, in different time zones and different responsibilities and so forth, that we go to tremendous lengths to speak with one another as part of the legal team, and then that’s mirrored throughout the organization.

The compliance team talks constantly. In the executive leadership team there are numerous meetings, briefings, and reviews, both formal and informal, just to make sure that information gets shared. Hopefully to the point that nothing falls through the cracks and to ensure that we have early warning on emerging issues and so forth.

In an organization like ours, this kind of intensive collaboration and communication is probably the best solution and the best way to ensure proper oversight and management over the wide range of complex and diverse compliance risks we face.

AM: Thanks so much for sharing your thoughts with us!

About the Expert

Jeffrey Eglash is Vice President and Chief Compliance Officer at Nokia, where he has responsibility for the company’s global ethics and compliance program.

Compliance Across the Organization

Today’s leading compliance officers interact with their counterparts across roles, functions and regions. The following data comes from Ethisphere’s 2017 World’s Most Ethical Companies and highlights the ways that the best companies embed ethics and compliance across the organization:

Types of interactions the compliance and ethics function has with other functional groups in your company.

- Attend HR training events: 98%
- Add E&C questions to employee surveys: 98%
- Design audits and receive audit results: 97%
- Time in sales/marketing meetings to educate on E&C program as competitive advantage: 90%
- Sit on a steering committee: 82%
- Formal input on corporate business strategy: 80%

2017 WME Honorees
The CISO’s Perspective on Enterprise Risks

An Interview with
John Masserini, Chief Information Security Officer of Millicom

Interview by
Greta Baranowski

Global companies face a truly unlimited number of risks. The key for any successful risk management program is to identify the most critical risks your company faces, and apply resources against those accordingly. In the following interview, John Masserini, the Chief Information Security Officer at Millicom, shares his thoughts into how companies and leaders across the organization can best get a handle on the key risk areas they face.

Q: Could you tell us a bit about your current areas of focus, and top 2 or 3 priorities? Where does risk management fall vis a vis those?

JM: We are focused on centralizing critical security services and providing a global center of excellence which can be leveraged by all of our international operations. Not only does this offer a far better overall view of enterprise-wide risk, it also significantly reduces the overall financial impact by leveraging purchasing discounts and a standard service catalog across all internal organizations. Risk management is critical to the growth of the company and by providing enhanced visibility, we are able to focus on efforts and projects that provide the biggest risk mitigation for the efforts spent.

Q: What are the current challenges you, and CISOs broadly, are facing when it comes to risk management? What are some of the lessons you’ve learned, or advice you can offer, in terms of managing or combatting those risks?

JM: From a broad perspective, understanding how specific risks and issues directly impact the organization is the biggest challenge I often see. A specific technology risk in one part of the infrastructure may have a drastically different risk impact than the same risk in a different part of the company. Understanding that challenge is one of the key components to a functional risk management strategy.

“Risk management is critical to the growth of the company and by providing enhanced visibility, we are able to focus on efforts and projects that provide the biggest risk mitigation for the efforts spent.”

If an organization dropped everything each time a ‘critical’ vulnerability was announced, they would get little of their strategic plan accomplished. The more mature organizations know now to balance mitigating risks on those systems which are critical to the revenue generation of the company, and accepting the risk of those that are not. This shouldn’t imply that the less important hosts or applications shouldn’t be patched, it only means they will be prioritized until the scheduled outage window, update release, or other manageable timeframe.

I’ve found one of the best tools to help any risk professional understand criticality of infrastructure to a revenue stream is a regularly updated Business Impact Analysis (BIA). Admittedly, BIA’s are typically only thought of when dealing with Business Continuity & Recovery planning, but I leverage them heavily to drive risk mitigation or project management decision making. A CISO can truly build strategic processes into their risk management efforts by using the results of
“Not only is it important to get the other teams onboard with your message, but it’s just as important that you are onboard with theirs.”

the BIA’s to drive everything from vulnerability mitigation to justification for substantial efforts such as Identity and Access Governance.

Q: How do you interact with other department leads/c-suite members in order to both understand and support their risk mitigation efforts? And on the flip side, are there ways they can help support your risk mitigation efforts?

JM: Partnering with all technical and business teams is critical to a security program’s success. Not only is it important to get the other teams onboard with your message, but it’s just as important that you are onboard with theirs. Understanding business goals and technology efforts is crucial to maturing the operational aspect of the security program.

Take for example an effort like GDPR. While in most cases, the GDPR program is managed through the Privacy Office/Legal Team, there is no way possible to satisfy the requirement without understanding the risk mitigation and security controls which are in place. Additionally, the training requirements resulting from the GDPR effort could easily fit into any mature Security Awareness effort, thereby providing a productivity benefit by incorporating privacy and security training together.

Another benefit the security team can bring to other teams is the ability to see the ‘big picture’. This doesn’t mean other teams don’t have a holistic approach, but unlike the majority of technology teams, the security team often understands environments end-to-end. In many instances, the networking teams don’t need to be concerned with the details of a server configuration, and the impact of that to the application that’s running on it. A mature security program would have insight into everything from the application, to the host it is running on, down to the network requirements it needs to perform its function. This end-to-end visibility provides a unique insight that allows the security teams to assist in more strategic architecture maturity discussions.

Q: What does success look like for you when it comes to risk management?

JM: Successful risk management is not the complete elimination of risk, but balancing mitigation efforts with business drivers and regulatory requirements. Every company makes decisions daily on what risks to accept and what to avoid. Technical risk should be no different. To me, a successful risk management program means we understand where our risk is, we all agree as to the level of risk we have, and are comfortable with the plans to mitigate or accept it.

Q: Finally, are there any key pieces of advice you can offer to other companies when it comes to creating an effective risk management structure?

JM: There is an old industry adage – Security For the Sake of Security is Failed Security – that still holds true to this day. A mature security program must consider the drivers and expectations of the business and needs to account for times when the acceptance of risk is an adequate response.

Another element that has benefited me over the years is the ability to associate a risk mitigation strategy with a hard revenue generation goal of the business. Does your organization have a consumer application or web site that generates revenue? Can you develop a financial model that associates an outage, a denial of service or a site defacement to a loss of revenue or customers? If so, then associate the risk mitigation strategies of protecting against that loss to the potential lost revenue of such an event. If you find yourself proposing a solution that costs more than the revenue lost, then perhaps an alternative approach is in order.

Q: Thanks so much for sharing your insight with us.

about the Expert

John Masserini is Chief Information Security Officer at Millicom, an international telecommunications and media company.

GDPR by the Numbers

Today’s The General Data Protection Regulation, or GDPR, is one of the most talked about regulations of 2017. And that doesn’t look like it will change in 2018. Here are some key numbers around this new, all encompassing regulation:

- 4% — The percent of annual revenue a company can be fined for violating the rule
- April 27, 2016 — The date the regulation was adopted
- 1995 — The year that the previous data protection rule was put in place, which is now being replaced by GDPR
The CFO’s Perspective on Risk

Laurel Krzeminski, Chief Financial Officer of Granite Construction, Shares Her Thoughts on Mitigating Risk through Collaboration

Interview by Tyler Lawrence
We recently had the opportunity to catch up with Laurel Krzeminski, the CFO of Granite Construction, a 95-year-old company and one of the largest infrastructure projects and construction material producers in the United States. In the following article, Mrs. Krzeminski shares her thoughts as to how senior roles across the company can collaborate with one another to ensure a strong culture of ethics and compliance.

**TL:** Earlier in this publication we heard about key risks from the perspective of the Chief Compliance Officer. As the CFO, can you share a bit about your approach to some of the key risks you have to face on a regular basis?

**LK:** As CFO, I am charged with growing and protecting the financial health of Granite for its stakeholders. One of my many duties is being a member of Granite’s Corporate Compliance Committee. Here at Granite, the Committee plays an active role in sharing information and addressing compliance risks present throughout the organization. A healthy company is generally built on a foundation of ethics, compliance, safety and sustainability. Our Compliance Committee brings together senior leaders responsible for mitigation of risks across the company from safety, quality, environmental, finance, information technology, as well as human resources.

We employ professional staff in the appropriate areas to deliver and ensure the proper execution of financial reporting requirements and oversight of compliance and regulatory requirements. These employees, senior business advisors in their respective operations, are key advocates for the compliance program, working closely with the Company’s compliance team.

We believe that our measured, systematic approach to risk and compliance positions us with the appropriate controls in place. Ultimately, it comes down to people and culture and delivering on our Core Values and operating by our Code of Conduct every single day. At Granite, ethics and compliance is not just a responsibility, it is a way of life, and part of our commitment to our stakeholders.

**TL:** How do you work with other senior leaders across the organization, also responsible for managing key risks, to ensure conversation and efficiencies across the organization, and to make sure risks don’t fall into silos?

**LK:** All senior leaders play a key role in managing risk and are part of the compliance team I mentioned. Across diverse geographies and diverse businesses we consistently employ a well-defined framework to address risk, compliance, and the control environment. This together with our flat management structure, enables more consistent execution. Our effort to manage risks ranges from implementing our Board-driven compliance program, including major construction project reviews to managing risks locally through consistent processes.

This is the framework that we use across the enterprise to create unique, but consistent KPIs. This, in turn, provides us with top-down and bottom-up visibility to efficiently manage enterprise risk.

**TL:** What keeps you up at night as it pertains to your role at Granite? What does success look like?

**LK:** The things that keep me up at night are typically things that one never expects will happen. We work very hard to plan proactively for what we reasonably control. Our strong culture of ethics and our compliance program guides us on how to handle those expected risks and those that are uncommon. But everything in our business begins and ends with our people, and doing our best to position them to safely, successfully build critical local, state, and national infrastructure.

 Probably the one thing that keeps me up at night more than others is ensuring that all of our employees safely return home each night after a day of work for Granite. These employees are proud of the foundation of values and ethics that guide us. Success in our business is reflected in developing our people, building a sustainable business, and delivering appropriate returns for all of Granite’s stakeholders.

**TL:** Any advice for other companies as to how they can encourage teamwork and cooperation across senior roles?

**LK:** Bringing in the right people to join your organization is key. As builders, our work demands team players at every level within the Company. Successful leaders must not only be smart, entrepreneurial and passionate about our mission, but they must also be willing to roll up their sleeves and work across functions and all levels within the organization to be effective.

Treating people right, and executing work in accordance with the core values laid out in our Code of Conduct ensures that we will maintain a sustainable and profitable company, as we have for the past 95-years.

---

**About the Expert**

Laurel Krzeminski is Chief Financial Officer at Granite Construction, one of the largest infrastructure contractors and construction materials producers in the U.S.
Using Enterprise Risk Management to Manage Global Supply Chain Risks

ON Semiconductor’s General Counsel Describes a Maturing Culture of Risk-Aware Decision-Making

Written by G. Sonny Cave, Michael Zuraw, Shashwat (Shash) Dave, Mark N. Rogers

ON Semiconductor is a multi-year recipient of Ethisphere’s World’s Most Ethical Companies recognition. This has been accomplished in large part due to the strong work of the general counsel’s office and legal team laying out comprehensive policies and processes for creating a strong ethics and compliance program. In the following article, ON Semiconductor’s EVP and Chief Compliance & Ethics Officer, Chief Risk Officer and Board Secretary, Sonny Cave, identifies some of the key policies and practices of the company around addressing and mitigating one of the key risk areas all companies face, those stemming from third parties, and how this work is driven and reinforced by core values and a strong global culture.

OUR CORE VALUES DRIVE OUR CULTURE – IN EVERYTHING WE DO

At ON Semiconductor, our core values are Respect, Integrity and Initiative. They define and drive actions of our employees and third parties representing ON Semiconductor, and our corporate ethos requires of our employees and representatives to place every action in the context of our core values. These core values also form the basis for corporate social responsibility at ON Semiconductor. This allows us to promote collaborative and mutually rewarding partnerships with our vendors, suppliers and other third parties, including our customers.

SUPPLY CHAIN MANAGEMENT AT ON SEMICONDUCTOR

Our Global Supply Chain Organization (GSCO) engages a sizeable number of third-party partners, spread across 5 continents. Maintaining a flexible, reliable and responsive supply chain while shipping more than 1 billion units per week with greater than 94 percent average on-time delivery requires significant collaboration and coordination with our customers, distribution partners and vendors. With our core values forming a basis for everything we do, we attempt to partner with third-party suppliers and vendors who embrace our values and culture or have a similar corporate and compatible ethos. Third-party suppliers and vendors are managed through a centralized sourcing organization supported by on-site procurement teams with centralized reporting to the Chief Procurement Officer.

PROCESSES AND POLICIES

Our membership in the Responsible Business Alliance (RBA), formerly known as Electronic Industry Citizenship Coalition (EICC), is a central component of corporate social responsibility at ON Semiconductor. All suppliers are required to agree and comply with ON Semiconductor’s Code of Business Conduct and the RBA Code
of Conduct. As a full member of the RBA, we abide by the RBA Code of Conduct and are committed to upholding RBA standards regarding labor, ethics, environment, health and safety, and management systems. In addition to complying with all the laws and regulations, we are also committed to ensuring that our suppliers and vendors maintain a supply chain that embodies our values.

We continuously work with our suppliers to certify that our products are free from any restricted materials and to ensure that all metals utilized in our products are sourced from conflict-free mines. We conduct due diligence within our supply chain to assure minerals are not being sourced from entities supporting armed conflict in certain areas. We expect our suppliers to engage in similar due diligence to analyze their sources and to complete the current CFSI Conflict Minerals Reporting Template (CMRT).

We also ensure that our workers are not required to surrender government issued identification or work permit originals to our company or any of our labor agents. Our human resources staff as well as our labor agents undergo anti-human trafficking training. On-site verifications are conducted to ensure compliance. We also investigate incidents of slavery and human trafficking in our supply chain through the use of risk assessments and site visits.

Our global minimum employment age policy is designed to ensure that sufficient measures and controls are in place to verify the minimum age of individuals working at our company. We apply the same minimum age requirement for employment at our supplier companies and labor agencies. We strive to ensure that our suppliers have the necessary policies, procedures, measures and controls in place through risk assessments and on-site verification to avoid incidents of child labor within our supply chain.

We expect our suppliers and vendors to share our values of corporate social responsibility including environmental protection, labor practices, human rights, fair business practices, supply chain responsibility and contribution to community and society. We clearly communicate our expectations to our suppliers, assess risks within our supply chain and validate compliance of suppliers to the RBA Code of Conduct and local laws and regulations through site visits.

**BEYOND POLICIES / BEYOND COMPLIANCE - Progress to Best-in-class supply-chain management**

While conformance and compliance with policies, processes and codes of conduct is important, our goal is to develop, promote and fortify a highly ethical culture resulting in a best-in-class supply chain management program where our interests are aligned with those of our suppliers, vendors, communities and environment in which we operate. At ON Semiconductor, we utilize compliance as a yardstick, or a measuring tool, to quantify compliance rather than utilizing compliance as a fail-safe. Through our actions, example and guidance in areas ranging from Corporate Social Responsibility and Enterprise Risk Management to Environment, Health and Safety, we intend to replicate our culture of high ethical standards and risk-aware decision making across all areas of our supply chain to identify, prioritize, manage and mitigate risks inherent in our supply chain.

**Risk Appetite**

Below is an example of Risk Appetite statements ON Semi develops and shares in order to guide the company’s approach to identifying and addressing key risks:

**Risk Appetite for Ethical Behavior and Third-Party Association Risks**

**Risk Type:** Ethical Behavior Risk
**Risk Statement:** The risk that employees at any level violate ethical standards as outlined in the company’s Code of Conduct - including, but not limited to Insider Trading, Fraud, and Bribery & Corruption

**Risk Appetite:** RISK AVERSE – CRITICAL (Averse to taking any risk / No tolerance)

**Risk Type:** Third-party Association Risk
**Risk Statement:** The risk that questionable actions on the part of the company’s suppliers, partners, customers, or others tied directly to the company violate our stated company values and ethical standards, driving negative publicity by association which may negatively impact brand value and reputation

**Risk Appetite:** RISK AVERSE – CRITICAL (Averse to taking any risk / No tolerance)

**Enterprise Risk Management**

Below is how the company defines its approach to Enterprise Risk Management across the board:

**ERM at ON Semiconductor:** Incorporated in 2014 with the full support of executive leadership and Board of Executives, the goal of our Enterprise Risk Management (ERM) program is to systemically, consistently and effectively identify, evaluate, prioritize and manage key risks affecting the company across all functional areas. Our ERM program strives to develop and promote a risk-aware culture across the organization and drive efforts to not only mitigate our top priority risks but to also capitalize on certain risks that are well within our defined risk appetite.

Critical to the execution of the ERM program, we have appointed a Chief Risk Officer and a Corporate Risk Committee, in addition to creating a comprehensive network of ERM Risk Champions to support the program.
The Enterprise Risk Management (ERM) process at ON Semiconductor requires every functional area to identify, evaluate, prioritize and communicate top risks to our executive staff and the Board of Directors. Presentations to the Board include a risk heat map depicting top risks, risk rating score, target risk level and a summary of relevant mitigation actions, including status and completion timeframe. Risk reports and heat maps are shared across functional organizations.

As every functional area in the organization utilizes a common language for risk identification, risk scoring and prioritization, cross-functional teams can identify and aggregate similar risks. More importantly, any functional group can identify and report risks regardless of the reporting structure. For instance, recently, our Manufacturing, Facilities and Information Technology teams identified risks that could adversely impact our global supply chain. As a result of this enterprise-wide risk reporting and aggregation, we are able to prioritize resource allocation to effectuate risk mitigation plans.

Risk mitigation plans often require cross-functional coordination across various teams. Often, the risk identifier or the owner is not solely responsible for the risk mitigation plans. In the example above, the risk mitigation plan included a task force composed of individuals from Manufacturing, Procurement, Supply Chain, Information Technology, Facilities and Environmental, Health and Safety team members.

Like any other organization, we have to take some risks in order to meet our objectives. At ON Semiconductor, our Risk Appetite statements (see sidebar) clearly define the amount and type of risks we are willing to take in order to meet our strategic goals and objectives. Our commitment to high ethical standards is unambiguously evident in our corporate risk appetite statements. Our corporate risk appetite provides no tolerance for risks arising out of ethical behavior of our employees or an associated third party. As a result, if any functional area identifies a high likelihood of risks that fall within these categories, these risks are automatically assigned a higher priority for mitigation and risk response strategies. In addition to the traditional compliance efforts, we also utilize our ERM tools and processes for early identification of risks across all functional groups.

While we utilize our ERM program and processes to address specific risks, a more important component of the ERM program is to develop a risk-aware culture across every function of the organization, including our third party vendors.

### About the Authors

G. Sonny Cave is EVP, General Counsel, Chief Ethics & Compliance Officer, Chief Risk Officer and Corporate Secretary, Law Department. Michael Zuraw is Senior Director, Enterprise Risk Management; Shashwat (Shash) Dave is Program Development Manager, Enterprise Risk Management; Mark N. Rogers is Senior Vice President, Assistant General Counsel, Assistant Secretary and Assistant Compliance and Ethics Officer; all at ON Semiconductor.
Free your business from third party risk.

Regulatory pressure is increasing, resources are decreasing and threats—like cyber risk, bribery and corruption—are rising fast.

And the biggest risks are from your third parties.

Don’t get caught off guard.

Free your business, with Opus.

Opus combines the most innovative SaaS platforms with unparalleled data solutions, helping you turn information into action so your business can thrive.

Learn more today, at www.opus.com
Today’s High-Tech House of Cards
Mitigating Risk in the Supply Chain

Written by Aarti Maharaj

As we speak with c-suite leaders across a variety of companies and ask about the risks they face and are most concerned about, risks relating to third parties inevitably come up first. Whether from suppliers, agents, distributors, partners, etc, working with third parties is both a critical part of a successful global companies and the source of much frustration and sleepless nights. In the following article we explore the ways companies can manage the myriad of enterprise level risks that arise from working with third party organizations.

Who can forget that sickening feeling you would get as a child when one card in your house fell, causing the entire structure to collapse? It could wash out hours of work, causing you to start all over again. This is the same feeling that can rush over you when addressing the ethics and compliance challenges that companies face when dealing with a globally diverse system of third parties, suppliers, M&A targets, distribution partners, agents. If one party in the chain of stakeholders falls, it can bring down all the others. To further exacerbate the issue, the level of sophistication and the variety of threats to company information security continues to grow as if someone is deliberately blowing your house down. Among the obstacles are outside intrusions that use third parties as a conduit to improperly and unlawfully exercise control and expose the company and its relationships to significant risks.

According to a recent study sponsored in 2017 by Opus, a global risk and compliance SaaS and data solution provider, approximately 56 percent of companies experienced cyberattacks against third parties that resulted in the misuse of their company’s sensitive or confidential information—an 8 percent increase from 2016. Of the organizations polled, about three-quarters said they believed the total number of cybersecurity incidents involving third parties are “increasing.”

“Good risk management is an enabler to business. It can provide a powerful competitive advantage and drive growth,” said Emanuele ‘Manny’ Conti, Chief Executive Officer at Opus. “The number one risk factor for companies is third parties and without effective leadership and collaboration it is easy to lose sight of all your vendors.”

The report, titled “Data Risk in the Third Party Ecosystem,” finds that the risks related to third parties are exacerbated as the majority of companies lack visibility into their third-party relationships. Although the number of third parties with access to confidential or sensitive information has increased by 25 percent, compared with 2016, more than half of the companies studied do not keep a comprehensive inventory of all third parties with whom they share sensitive information. And, only 18 percent of respondents know how third parties access and process data.

Dov Goldman, VP, Innovation & Alliances of Opus, said that companies need to inform and arm themselves with information and data about their third parties. “The key here is working together with third parties as well as internal stakeholders to mitigate risks,” Goldman said. “We are working very hard to enable our customers to leverage data and knowledge so ultimately they will be able to free themselves of the complexity associated with risks and make better business decisions relating to their partners.”

Collaborating with the CISO and Privacy by Design

The expansion of regulatory requirements over the last several years has led compliance costs to skyrocket, and companies are looking for ways to rationalize their processes and use technology to create greater efficiencies and performance. This is where the role of the Chief Information Security Officer (CISO) comes into play. Over the years, the function has emerged as an important part of how companies operate.

According to Conti, “CISOs are a very important component for managing risk and we are seeing more collaboration with this function across companies as they continue to ensure that all digital assets are protected. By design, CISOs are in a great position to collaborate as they oversee the function and can act independently.”

For Goldman, the role of the CISO will only grow in significance as third parties gain access to a company’s data. “Privacy and security is the business of the entire business and on a high level when you are designing systems, data is the key competitive market weapon,” said Goldman. As companies look for new ways
to collaborate and work across the organization to understand where their third-party data risks lie, Goldman said that a new concept is emerging, similar to tone at the top: privacy by design. Essentially, it means that information security and privacy don’t come after the fact – they’re engineered into all parts of the business’s processes upfront and are constantly monitored.

“Boards are going to demand that their systems are based around the principle of privacy by design. It’s a good business concept for companies to constantly evaluate the value proposition to their customers regarding the data they are providing.”

Roadblocks and Closing the Gaps Between Collaboration

While the ever-changing risk landscape certainly creates the challenge of simply keeping up, one of the barriers that Opus has seen across the spectrum is companies failing to fully adopt the same internal language when it comes to risk and risk management. “Creating a consistent risk management framework can help bridge the collaboration gap that may exist in an organization,” said Lee Kirschbaum, Senior Vice President, Head of Product, Marketing, and Alliances at Opus. “Once the risks are understood and the common language of risk management is established, it becomes easier to work together and collectively own the problems that exist instead of casting the problem back to what has historically been an owner of risk or a single individual.”

As the number and diversity of third parties continues to increase, Kirschbaum added that some of the major challenges companies face include:

- Visibility;
- The sharing of information in a common and consistent framework;
- Clarity around what different business lines are doing and why it matters;
- The lack of streamlined and integrated processes; and
- The need to monitor information and react quickly should something change.

“Risk is no longer just the problem of the Chief Technology Officer or the CISO. If you think about today’s environment when other parts of the organization don’t consider risk, they may create shadow components and fail to realize that they have been exposed to risk, which is no longer under the company’s umbrella,” added Kirschbaum.

Treating Third Party Risk Management as a Team Sport

The experts at Opus say that compliance and risk mitigation is like a team sport, where a company is only as strong as its weakest link. They also agree that, like a finely tuned athlete, the focus must be on constantly getting better because the competition (cyber criminals) are always finding new ways to enrich themselves at the expense of honest companies.

Conti said that in his experience, there are some companies that are successful at handling third party risk management through implementing best practices and viewing risk as a team sport. Conti also found that the best companies measure, monitor and collectively make informed decisions about risks.

“Highly functioning risk management teams enable performance, not inhibit it,” he said. “Company leaders are also part of the team sport as employees look to them to live the values they espouse.”

Like that house of cards, security in today’s environment is fragile. Unlike a child’s game, however, the risks are great. It does not take much to bring a company down, so the best course of action is to remain vigilant. Know who your vendors are and who their vendors are as well. Prepare for the unexpected because today’s risk rarely announces itself prior to becoming a crisis. Finally, stay team focused because the “bad guys” are always looking for a dark corner where they can gain access to the information you work so hard to obtain and protect.
Getting a Handle on GDPR

A Conversation with Carolyn Herzog, EVP & General Counsel, and Tim Fitzgerald, Chief Information Security Officer, Arm

Interview by Stefan Linssen

GDPR is one of the most discussed new regulations for global companies today, and many are still working feverishly to get a handle on the impact it will have on their organization. To help share insight into how company leaders can collaborate to help get a handle on this issue, we recently spoke with Carolyn Herzog, EVP and General Counsel of ARM, and Tim Fitzgerald, Chief Information Security Officer at ARM, to talk through how they collaborate to become prepared to address the significant expectations that come from GDPR. The following is a transcript of our conversation.

Q: Can you each share one or two or three key risks or priority areas that you’re currently focused on within your respective roles?

CH: When we talk about the synergies between how data privacy regulations and security work together we’re really trying to find those key risks, understanding our data strategy and understanding how to protect our employee and customer information. So from a legal perspective we are like everybody else trying to prepare for GDPR in particular. As part of that, and as a global company we’re looking at the potential impact of GDPR, but also understanding where our data is going to be flowing on a global basis. On top of that, we’re focused on making sure that we are going to be compliant and as transparent as possible with our employees and our customers around that data.

TF: I think there are some very obvious intersections between privacy and security. At one part security is a core pillar of a good privacy program. No matter whether we live up to the other concepts, or in general privacy regulations or methodologies, if we don’t secure the data properly it will be undone. So I think there are a couple challenges that come along with accomplishing that. First of all, the very basic principle is you need to do what the industry norms expect you to do. The foundational type controls that every company should be doing in order to protect your customers’ data.

Where I think it gets interesting for ARM, and Carolyn and I are in the thick of it together here, is there is a lot of shifting sands for us in that we’re attempting to move into new businesses, different joint venture type models in Asia and so forth. Thinking about leveraging and harnessing data that comes from our products in ways that we have not conceived of before has provided us with a whole host of new potential issues that ARM as a company has not had to contend with in the past with respect to security and privacy.

Q: GDPR is obviously the big thing going on right now and it’s the thing that everyone’s talking about and focused on in compliance. How much would you say some of your colleagues outside of the compliance or CISO role are aware of the impact of GDPR or just how much it’s stressing out the legal profession? Is it really understood across the enterprise, or do you find you have to really put effort into educating your colleagues?

CH: I have found that ARM has a very unique culture. I’m just about a year in and Tim is five months in. What has been interesting to me is I think people here tend to ask for more information about compliance that in my prior experiences. I think part of that is driven from being in the hardware industry where quality control is something that really drives a compliance culture and a desire to make sure that things are done very carefully. Some of it is also just the nature of the company, which is very integrity driven. And also we are a British company, so there is a great deal of awareness around European regulation and the desire to be compliant.
There's a lot of different ways you might come at this problem. We want to do about it. That's still hard to come by because it's more a matter of deciding and taking action on what GDPR and privacy and security are important or that the risk is.

So I think it's not a matter of trying to convince people that customer types of relationships with the services group, which is now called the Internet of Things Services Group. So as Tim mentioned we're working with new product areas and new technologies, which creates a focus area for us that is very much top of mind.

So at the same time that we do get more questions around compliance for GDPR, we're also investing more resources into compliance with GDPR and around our security to be better prepared. And we're putting more efforts around thought leadership into some of the ethical considerations around how the data is used, and some of the new technologies in areas like machine learning and artificial intelligence.

**TF:** I guess I would just add that I don't think you would find a person in ARM who wouldn't say that security and privacy is important. There's a high degree of recognition here. But because of what ARM has historically done with a licensing model, as Carolyn has pointed out, and with our IP being widely dispersed, there's sort of a limited view point on handling these new focus areas. So between the two of us we're doing a fair amount of education with ARM right now around talking about what it means to be in these different businesses, what are the potential implications of collecting and using data, and so forth.

Sometimes lawyers and compliance professionals are really good at creating checkpoints. We don't always think through whether or not the things we're putting in place actually added a level of bureaucracy rather than removing a level of bureaucracy.

Just literally earlier today we were part of a data strategy discussion and I think it was a proud moment for me having come to work at ARM because the conversation of that meeting was not around how do we monetize and make money, the conversation was about how do we right by our customers, even the ones we don't have yet.

So I think it's not a matter of trying to convince people that GDPR and privacy and security are important or that the risk is real, it's more a matter of deciding and taking action on what we want to do about it. That's still hard to come by because there's a lot of different ways you might come at this problem.

Q: As you’ve prepared ARM to be ready to respond to GDPR, can you share any advice or lessons that you learned along the way that you feel may be helpful to other organizations?

**CH:** Well for one if you’re only just starting your GDPR preparedness program now then you’re never going to make it. Two, it’s the collaboration that makes the big difference. You can’t do any compliance program in a vacuum. Compliance really does take a village and you have to understand where the touch points are and how you are going to make compliance for GDPR work across the entire company. As Tim mentioned we’re spending a lot of time not only talking to our teams together and talking through how we can work together to make this work, but also leveraging other parts of the company to make sure there is awareness building and that people understand what their roles are.

One of the big parts of all this for me is thinking about the broader compliance program and how to make it work. There was a champion kick off last week to make sure that the different people in the different business units knew what their roles and responsibilities would be as just part of the privacy program. And then from a security perspective, Tim’s team is doing the same to understand where the data is, what’s most important, how we manage it, and together thinking about how we make sure we have truthfulness and transparency to our customers.

**TF:** I would only add one piece of advice, and it’s probably the most obvious advice in the world, but that is to focus your efforts. Most companies have an awful lot of PII (personally identifiable information), which means they have a really wide landscape associated with GDPR. And if you haven’t fully mapped that out by this point you’re in a tough spot. But there are some systems that are going to be clearly more important than others and I see our approach here as we check them off one at a time. You can’t do them all at the same time. I hesitate to even say this, and to be quoted as saying my advice is to simply focus your efforts, but the reality is that’s where we are now.

Q: The two of you manage different key risks within your respective roles. What’s the right way to build a working relationship between functions such as the GC and CISO, as well as other key roles across a company?

**TF:** Even though I just started at ARM 5 months ago, Carolyn and I have the benefit of working together for more than 8 years. We both came from Symantec recently in similar roles and have developed a really good relationship with respect to how we work together. Both cathartically, and over how hard the some of these things are, but I think there are a couple of practices that help with this.

One, and you can overdo this, but there are several mechanisms that can be used to share data with respect to privacy risk. At ARM, Carolyn chairs our privacy council and I chair our security council. And the whole purpose of those groups is to discuss risk in our respective areas. Bringing together senior business leaders to discuss the biggest risks that are present, getting coordinated action on what we’re going to prioritize and where we’re going to focus, etc. And if nothing else, we use these groups to make good determinations on behalf of the business in terms of where we’re going to execute outside of our respective roles.

**CH:** And the other thing I would add to that is with the years of
experience working together, Tim and I know that we come to the problems with the same mindset around the importance of data security and privacy, and how well these subject matter areas are dependent on one another. There’s equal meaning in our minds to the importance of the subject matter area and fortunately we have the right executive leadership here that also agree with us in terms of the importance. So we have good support systems here to help us execute on the strategy that we’re putting forth.

There are some things that are in their infancy here, and there are some things that are already well established, so we’re really working on the program from the premise of figuring out where are the biggest risks and where should are our priorities be. Because of that some things are just starting to kick off.

**TF:** We haven’t experienced this in ARM yet but Carolyn and I have been through the trenches a couple times in other scenarios, and there’s nothing like a security event or privacy event where you have to dissect all the ways that it went wrong as a means of establishing shared priorities and shared purpose. That’s not the way you want to get to addressing some of these issues, but it’s pretty effective when it does happen. Thinking how do we not want to be in this position gives us a lot of focus.

**CH:** Yeah it does. One of the great legal strategies when giving presentations is to tell the war stories of how you don’t want to be on the front page of the Wall Street Journal. You’re in the luxury spot when you’re not in one of those positions. But sometimes you do have your own war stories of lessons learned which help to make sure you have the opportunity to self correct along the way.

**Q:** You were talking about communication earlier and working across the company to communicate. One of the things that we hear frequently is the need for company leaders to communicate the ‘why’ behind ethics and compliance activities, and to highlight that the work you are doing helps build a strong culture and doesn’t just check regulatory boxes. Can you share a bit around how you communicate the ‘why’ behind the work you’re doing with something like GDPR?

**CH:** One reason that I think ARM is sort of a unique environment is that I get more questions here from my colleagues than I think I’ve ever experienced in my career. So I find that I have to produce really good training because people really do listen to it and read it, and they ask me questions that I wasn’t always prepared to answer. People here really do take in the training and absorb it.

I think one of the things that we would like to do more of is what Tim and I started to do in our prior roles, and that would be to become more creative in our training. Because people absorb training quite well here, we haven’t had the high demands to make creative or entertaining training. Or adaptive learning type training that helps people learn along the way by adapting to their level of learning. I think we will want to start incorporating that because it’s just better for the organization and enhances the reputation of the work that we’re doing.

**TF:** We’re about to kick off the first security training I’ve been part of since joining Arm, and the feedback we’ve had to contend with are two fold: first, that we need to talk to our staff like adults and that the content needs to be more sophisticated and not pander to...
the lowest common denominator, and second, that our trainings should reflect the fact that we trust our staff. It’s a nice problem to have that our staff is asking us to make the trainings more sophisticated and serious.

I like to think about training as a marketing program. We put a different hat on and we say that we’re trying to truly influence behavior. Just like if you’re trying to get somebody to buy that stick of gum at the checkout line, how are we going to approach the problem from a marketing perspective to see what kind of social, cognitive levers we can pull that will actually start influencing their job day-to-day.

Historically a lot of the training programs that I’ve put together are trying to tap into what people’s motivations really are and see if we can produce something that’s meaningful against those motivations in order to change the norms.\n
“Historically a lot of the training programs that I’ve put together are trying to tap into what people’s motivations really are and see if we can produce something that’s meaningful against those motivations in order to change the norms.”

Q: On the flipside of what we’ve been discussing, how do the two of you receive information or data or so forth from other leaders who might be focused on their own key risks which don’t traditionally overlap with the role of the GC, CISO, etc?

TF: Core function for me is I’m here to support the business. I have to understand what their risk profile is otherwise I can’t do my job very well. I think Carolyn would probably say the same. It’s a little more interesting when we start talking about how they hear risk among each other. Because I think legal and security are both the types of functions where our sole purpose is to understand how to address risk.

ARM has pretty impressive risk management systems in place. It’s really well documented how all these things are supposed to work and stick together. The challenge is in making that work in real life. But people are pretty open here and they’re really willing to share what their risks are and what they’re dealing with. So it’s not for shortage of information, the real challenge is in trying to put one risk besides another and arbitrate which one deserves more priority or more attention. That’s everyone’s problem and still, I think, difficult to solve despite how strong a system might be.

CH: I agree. I also think one of the challenges for organizations in a changing industry is lack of collaboration, which is something that fortunately we don’t face here. There’s an extreme openness and an extreme desire to collaborate. Success is about speaking the same language and making sure that you’re all trying to get to the same outcome. Because sometimes you can use the same words but they actually might be interpreted in different ways. Particularly when you’re speaking across borders.

Another challenge can be when people are used to speaking in the language of their business. That’s something that I found to be an area where I have to pay particularly close attention and maybe ask more follow on questions to make sure I really understand what’s being said. It does take time and effort to make sure you’re investing in that and thinking towards the long term goals of the business. You want to be sure your efforts are applied towards achieving the long term goals of the business.

You also have to think about the automation aspect of things, and how you can work towards streamlining and removing bureaucracy rather than adding bureaucracy. Sometimes lawyers and compliance professionals are really good at creating checkpoints. We don’t always think through whether or not the things we’re putting in place actually added a level of bureaucracy rather than removing a level of bureaucracy, and I think to be a really good compliance professional, or to create a really good compliance program no matter what the subject, in addition to creating these assets in people that get them to really think about it and make it part of their everyday habits, you have to make sure that you have streamlined processes, and make sure that there’s a level of automation that ensures compliance just becomes habit. This has to be easy rather than making people jump through 16 hoops to get to the point of compliance that they need to reach.

TF: That’s a good point. These are enabling functions. Rather, they can be enabling functions or they can be a pain. It depends on how you come at the problem. Trying to think your way through risk management as a way to help the business move faster can sometimes make the problems harder but certainly makes the solution more valuable. And that’s how we’re attempting to come at the problem.

About the Experts

Carolyn Herzog is Executive Vice President and General Counsel at Arm. Prior to Arm, Carolyn served as Chief Compliance Officer, Vice President and Deputy General Counsel at Symantec.

Tim Fitzgerald is Chief Information Security Officer at Arm, a UK-based semiconductor and software design company.
ABOUT OPUS

Opus is a global risk and compliance SaaS and data solution provider founded on a simple premise: that faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace.

Today, the world’s most respected global corporations rely on Opus to free their business from the complexity and uncertainty of managing customer, supplier and third-party risks.

By combining the most innovative SaaS platforms with unparalleled data solutions, Opus turns information into action so businesses thrive.

For more information about Opus, please visit www.opus.com.

ABOUT ETHISPHERE

The Ethisphere® Institute is the global leader in defining and advancing the standards of ethical business practices that fuel corporate character, marketplace trust and business success. Ethisphere has deep expertise in measuring and defining core ethics standards using data-driven insights from our Ethics Quotient®, and works with the world’s largest companies to enhance culture capital with the insights from our culture assessment data set, which is grounded in our 8 Pillars of Ethical Culture. Ethisphere honors superior achievement through its World’s Most Ethical Companies recognition program and provides a community of industry experts with the Business Ethics Leadership Alliance (BELA). More information about Ethisphere can be found at http://www.ethisphere.com.