Uptime Network Leadership Session

Enterprise Risk Management (ERM)

Uptime Network members discuss how data center teams interact with corporate risk departments, and how that dynamic has evolved.

The meeting was held February 27, 2025. All Network member insights are unattributed for confidentiality.

Readout prepared by Matt Stansberry, Executive Director
Data Center Practitioner Insight & Experience

uptime® INSTITUTE

Smarter Together

The Uptime Network is a community of data center owners and operators under mutual NDA. No member organizations or individuals are named.

This readout is based on a working session led by Matt Stansberry, Executive Director of Data Center Practitioner Insight and Experience and 30 members of the Uptime Network on Feb 27, 2025.

These readouts are designed to capture the iterative, collaborative knowledge-shared between Network members and Uptime technical SMEs. These documents do not necessarily represent the opinions of Uptime's technical leadership or members but instead provide members resources to track our community's ongoing discussions. These readouts are intended for Uptime Network internal use.

Email suggestions for future topics to Matt Stansberry: mstansberry@uptimeinstitute.com.

uptime® INSTITUTE

Surveying the Risk Landscape

ERM is a structured approach to identify, assess, and manage risks that could impact a company's strategic objectives, financial stability, regulatory compliance, or operations. It takes a holistic view of risks across the entire organization—rather than just within individual departments—so leadership can make informed decisions about balancing risk and opportunity.

This readout provides a snapshot of how different member companies structure ERM and captures the benefits and challenges of interdepartmental collaboration. We've scheduled an in-person follow-on workshop in New York, 26 March, 2025; details are on the last slide.

Matt Stansberry
Executive Director Data Center Practitioner Insight and Experience
Uptime Institute

uptime® INSTITUTE

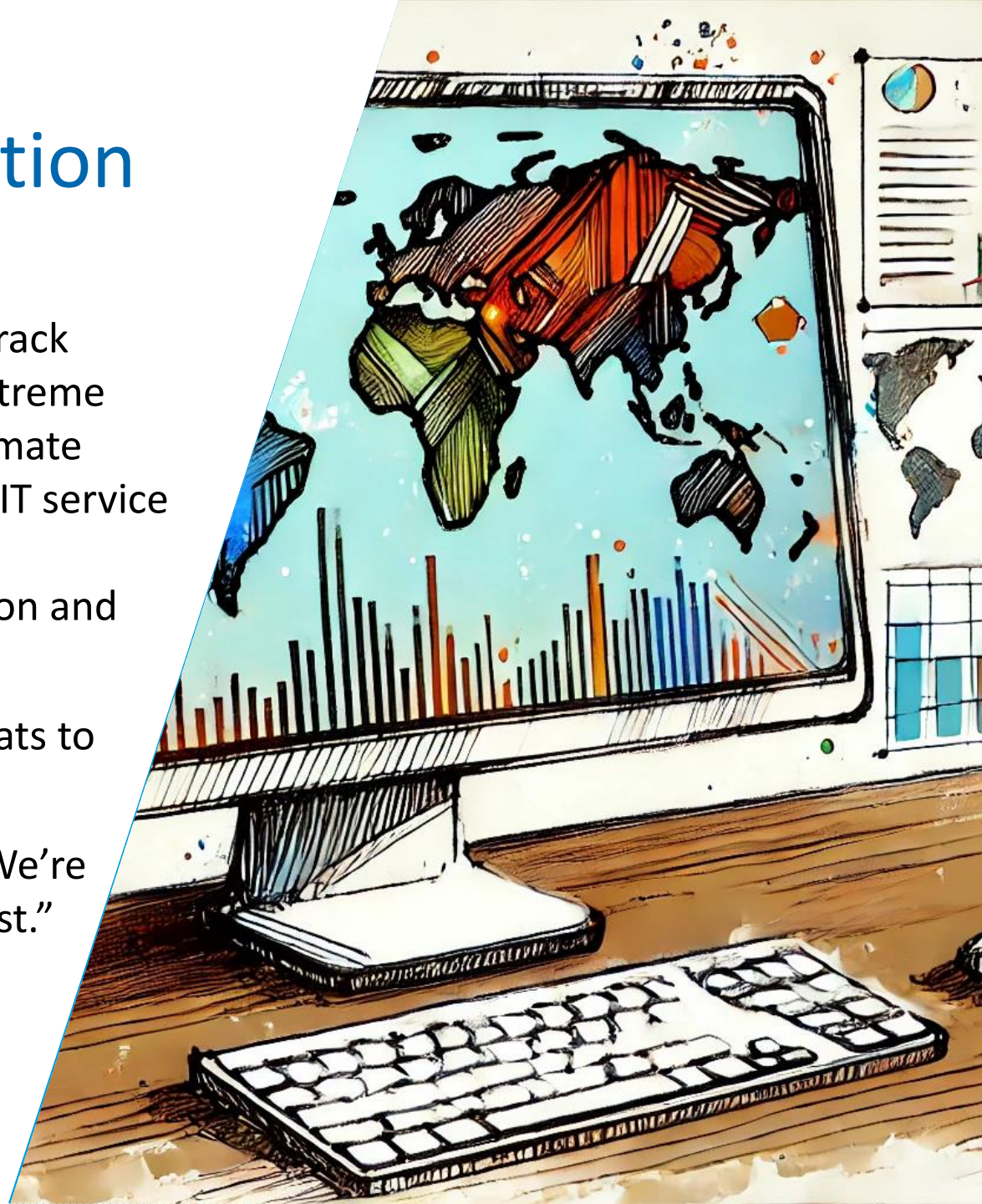
Network Members Share How Different Verticals Structure ERM

- Hyperscale Organizations
- Financial Services
- Healthcare
- Colocation Providers

uptime® INSTITUTE

Example: Hyperscale Organization

- ERM rolls up to the Finance Department
- Risk managers embedded in the data center team track topics related to data center operational impact: extreme weather, manmade threats, supply chain delays, climate change impacts, legislative updates, cyber security, IT service outages, sustainability liabilities and other issues that could impact the performance, public perception and growth of the business.
- Embedded data center risk managers raise key threats to the ERM for board level awareness.
- The list of risks evolves, but as one member said, “We’re constantly adding risks, but very few come off the list.”



uptime® INSTITUTE

Example: Financial Services

- Highly regulated industry with mature, enterprise-wide ERM functions.
- In this case, the organization's risk management structure uses the three lines of defense methodology (see Inside Track for more on this framework.
  - The first line of defense is the business unit (in this case the mission critical department).
  - The second line of defense is Governance, tracking external regulators and compliance. Each business unit appoints a governance lead to coordinate activities and requirements.
  - ERM is the third line of Defense where key risks are rolled up to the senior leadership level.
- This organization's ERM methodology focuses on eight categories of risk: Credit, Market, Liquidity, Capital, Operational, Technology, Compliance, Reputational and Strategic.
- The majority of the ERM group's queries are related to risks categorized under cyber security, not necessarily infrastructure resiliency.

Example: Healthcare

- The healthcare example was the most complex, as several different teams in the company are tracking risk from different angles, including a group dedicated to tracking third-party risk.
- Fraud is a significant area of focus in healthcare, so an ethics team is dedicated to auditing internal, client and supplier fraud.
- There is a separate group focused entirely on healthcare delivery risk, and any IT service delivery impacts on that area are captured and assessed. Infrastructure teams are required to update this risk management group regularly for legal discovery purposes. Once a year, the IT Infrastructure group responds to a wide-ranging survey with open ended questions, addressing any self attested risks or risks reported by other departments related to IT service delivery.
- All these separate risk functions roll up under audit and report to the Legal department.

Example: Colocation Suppliers

Many colocation firms have an ERM function that is less established than the hyperscale's but matches their more infrastructure-focused approach to risk management.

For some for colos, ERM is situated in the finance department reporting into the CFO. Others risk teams function informally as a committee reporting to leadership.

The ERM function is present in privately held companies as well as publicly traded entities, with some opting to contract SMEs versus in-house risk teams, especially for topics like climate change adaptation, sustainable technology transition risk, and supply chain -- recent additions to the topic list that match the concerns of hyperscale tenants.

uptime® INSTITUTE

Is ERM Improving Data Center Risk and Resiliency?

uptime INSTITUTE

Uptime Network Member Experience: ERM Dynamics

"…We are experts in operational risk, and 90% of the risk assessment function is to meet governance requirements. This is a paperwork burden with limited payback.

As subject matter experts on managing risk, we carefully plan every activity in the data center. There is a very sophisticated change management process, every activity is carefully scripted. We commission all our systems, conduct regular drills. So why do I need this separate team to come in and tell me how to do the things I'm already doing very well?

That said, there is the 10% of the time when the ERM audits provide an epiphany.

Also, when you have the external regulators come through your data center, they put you through the ringer – a lot of reporting and time go into that. The effort doesn't necessarily contribute to the day-to-day operations, but it does sharpen our compliance skills."

Uptime Network Member Experience: Resiliency Awareness

“We try to anticipate areas of risk. When a project is proposed to reduce costs that we believe will reduce resiliency, I fill out a paragraph on the risk questionnaire to identify downstream implications.

The business team will say *But it's a great thing! It’s going to save us lots of money! It’s going be great for our patients!*

But it's a huge risk, and to mitigate that we’re going to have to build redundancy into systems to isolate failures, and when they hear they need to spend money to do that, they say … *Oh.*

What happens if the network is cut; how long can a hospital function under those conditions?

The risk surveys have an impact. There is follow up and it brings attention to leadership. It's just one of the tools ERM uses, in addition to all the other regulatory audits. But I do think they have a positive impact.”

uptime® INSTITUTE

Does ERM support funding to address vulnerabilities?

Network Members Respond

“It's a little indirect, but if the internal audit finds a risk mitigation exposure, that informs the business justification for increased funding. If you find an older CMMS system is vulnerable to data integrity issues, you can make the case to secure the funding for an upgrade if it’s not already in the budget plan.”

“Yes. In terms of budget prioritization, data center resiliency is identified with direct health care delivery in terms of our mission, so yes, we do get priority on those items. I think that participating in these discussions brings it front-of-mind. We're so busy doing our regular day-to-day roles; this brings attention to this area and helps us address issues more proactively.”

Maintaining The Human Element

One member raised the issue that quantifying data center risks in terms that inform ERM's data driven decision making can be difficult. "The KPIs we manage for data center operational risk don't always translate to the enterprise-wide view of priorities."

Another mentioned "We are pushing down the path toward more quantitative modeling. But I don't want to underestimate the value of the gut feeling of direct managers. I've I found that they are typically right, so I don't want to take them out of the loop."

uptime INSTITUTE

Future Cross Departmental Collaboration

Finding those rare epiphany moments in the audits, keeping risk front of mind in day-to-day operations, and getting funding prioritization for identified vulnerabilities are all positive outcomes of ERM collaboration. But where do we go from here?

Members suggested ERM teams could coordinate in-house data center SMEs to assist in managing ERM's relationship with colocation and cloud providers, as data center teams are already aligned on ERM's assessment processes and priorities.

Another member raised the issue that data center teams struggle to communicate the full business ramification of technical risks to ERM colleagues. In order to address this challenge, members recommended dedicating staff to be ERM liaisons, cross-training on risk definitions and working together to modeling downstream impacts.

Separating Risk from Known Vulnerabilities

One member suggested the data center industry needs to more narrowly define risk.

“ERM often includes known vulnerabilities in the definition of risk that I don't think should be included. There are issues and incidents, and there are things that have happened. My team addresses risk from a hypothetical ‘could’ situation.

If we are talking about known software vulnerabilities, those are vulnerabilities, not risks. And they require a different discipline and management process.

I think we need industry alignment around what should be included in the discipline of risk management, because it seems really overloaded.”

The Path Forward

Data center leaders should develop the ability to communicate operational risk in financial terms that are clearly understood by senior leadership.

This will require an ongoing effort, to test some of the recommendations of the members in this document, to increase cross-departmental collaboration and engagement in corporate risk initiatives.

Next slide: Opportunities to continue this ERM discussion with your peers.

uptime INSTITUTE

Take the Next Steps

- ATLANTA MARCH 18-19: Discuss in-depth data center risk topics with your peers at the Uptime Network Americas Spring Conference. Registration is open; data center tour capacity is limited.
- NEW YORK MARCH 26: Continue this discussion with data center leaders and ERM teams, Weds Mach 26 (10am-2pm) with guest presenter Sim Segal, head of Columbia University's ERM MBA program. RSVP required – mstansberry@uptimeinstitute.com
- AMSTERDAM APRIL 15-16: Uptime Network EMEA Spring conference.
- Further Reading:
  - Addressing supply chain risk in data center cybersecurity
  - Uptime Institute's Standardized Comprehensive Infrastructure Risk Assessments for Financial Sector Institutions
  - Jamie Thompson, AWS Presentation on Enterprise Risk Management
  - Sim Segal's ERM Glossary

uptime INSTITUTE

uptime® INSTITUTE

Visit www.uptimeinstitute.com/ui-network for more information.

Uptime Institute
405 Lexington Avenue
New York, NY 10174