U.S. SEC Cybersecurity Regulation
-
Cyber Risk Reporting Simplified

Item 106: cyber risk management and governance

The new US SEC Cybersecurity Regulations took effect in December 2023. It is a game changer for the world of cyber. The need to disclose material cyber incidents within 4 days will provide unprecedented visibility into attacks and damages caused to public companies. We have started to see such disclosures.
Much less discussed is item 106 of the regulation which requires:

"Annual disclosure of cybersecurity risk management, strategy, and governance."

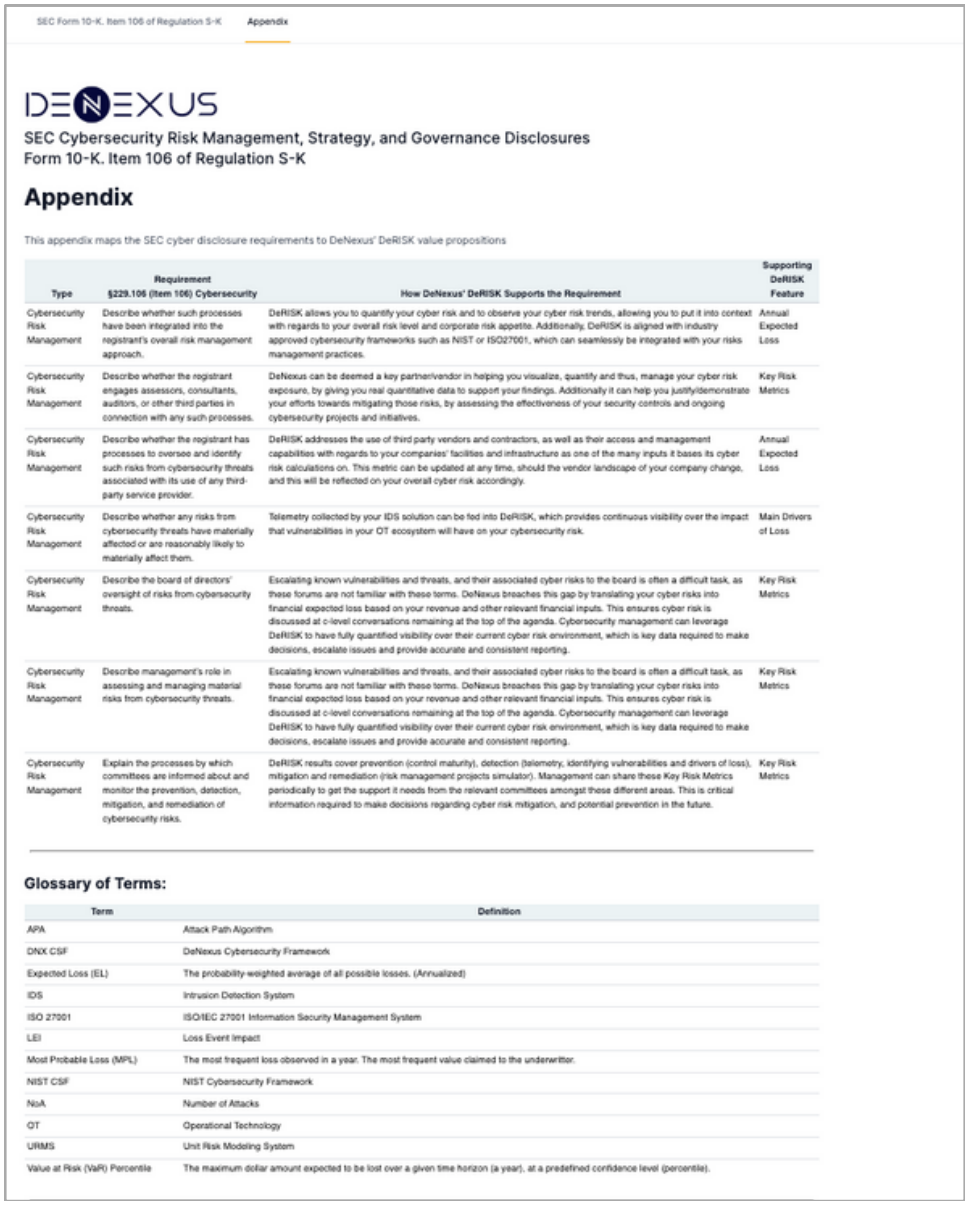
"Registrants to describe the board of directors' oversight of risks from cybersecurity threats (including identifying any board committee or subcommittee responsible for such oversight) and management's role in assessing and managing material risks from cybersecurity threats."

Few companies and their board of directors are ready. It might even be harder for companies in critical sectors such as energy, manufacturing, transportation, and data center operations as a great deal of the cyber risk is related to industrial or physical equipment which has often lagged IT in cybersecurity governance.

DeNexus delivers a turnkey Cyber Risk Executive Report tailored to SEC requirements for OT cyber risk management disclosure.

1 DeNexus simplifies the compliance work by mapping the SEC reporting requirements to specific risk KPIs

Our team has interpreted every requirement from Item 106 of Regulation S-K and aligned it with the specific cyber risk KPIs that our DeRISK platform compiles on an on-going basis to quantify cyber risks in OT environments.



SEC Form 10-K. Item 106 of Regulation S-K | Appendix

DENEXUS

SEC Cybersecurity Risk Management, Strategy, and Governance Disclosures
Form 10-K. Item 106 of Regulation S-K

Appendix

This appendix maps the SEC cyber disclosure requirements to DeNexus' DeRISK value propositions

Type	Requirement §229.106 (Item 106) Cybersecurity	How DeNexus' DeRISK Supports the Requirement	Supporting DeRISK Feature
Cybersecurity Risk Management	Describe whether such processes have been integrated into the registrant's overall risk management approach.	DeRISK allows you to quantify your cyber risk and to observe your cyber risk trends, allowing you to put it into context with regards to your overall risk level and corporate risk appetite. Additionally, DeRISK is aligned with industry approved cybersecurity frameworks such as NIST or ISO27001, which can seamlessly be integrated with your risks management practices.	Annual Expected Loss
Cybersecurity Risk Management	Describe whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes.	DeNexus can be deemed a key partner/vendor in helping you visualize, quantify and thus, manage your cyber risk exposure, by giving you real quantitative data to support your findings. Additionally it can help you justify/demonstrate your efforts towards mitigating those risks, by assessing the effectiveness of your security controls and ongoing cybersecurity projects and initiatives.	Key Risk Metrics
Cybersecurity Risk Management	Describe whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.	DeRISK addresses the use of third party vendors and contractors, as well as their access and management capabilities with regards to your companies' facilities and infrastructure as one of the many inputs it bases its cyber risk calculations on. This metric can be updated at any time, should the vendor landscape of your company change, and this will be reflected on your overall cyber risk accordingly.	Annual Expected Loss
Cybersecurity Risk Management	Describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect them.	Telemetry collected by your IDS solution can be fed into DeRISK, which provides continuous visibility over the impact that vulnerabilities in your OT ecosystem will have on your cybersecurity risk.	Main Drivers of Loss
Cybersecurity Risk Management	Describe the board of directors' oversight of risks from cybersecurity threats.	Escalating known vulnerabilities and threats, and their associated cyber risks to the board is often a difficult task, as these forums are not familiar with these terms. DeNexus breaches this gap by translating your cyber risks into financial expected loss based on your revenue and other relevant financial inputs. This ensures cyber risk is discussed at c-level conversations remaining at the top of the agenda. Cybersecurity management can leverage DeRISK to have fully quantified visibility over their current cyber risk environment, which is key data required to make decisions, escalate issues and provide accurate and consistent reporting.	Key Risk Metrics
Cybersecurity Risk Management	Describe management's role in assessing and managing material risks from cybersecurity threats.	Escalating known vulnerabilities and threats, and their associated cyber risks to the board is often a difficult task, as these forums are not familiar with these terms. DeNexus breaches this gap by translating your cyber risks into financial expected loss based on your revenue and other relevant financial inputs. This ensures cyber risk is discussed at c-level conversations remaining at the top of the agenda. Cybersecurity management can leverage DeRISK to have fully quantified visibility over their current cyber risk environment, which is key data required to make decisions, escalate issues and provide accurate and consistent reporting.	Key Risk Metrics
Cybersecurity Risk Management	Explain the processes by which committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity risks.	DeRISK results cover prevention (control maturity), detection (telemetry, identifying vulnerabilities and drivers of loss), mitigation and remediation (risk management projects simulator). Management can share these Key Risk Metrics periodically to get the support it needs from the relevant committees amongst these different areas. This is critical information required to make decisions regarding cyber risk mitigation, and potential prevention in the future.	Key Risk Metrics

Glossary of Terms:

Term	Definition
APA	Attack Path Algorithm
DNX CSF	DeNexus Cybersecurity Framework
Expected Loss (EL)	The probability-weighted average of all possible losses. (Annualized)
IDS	Intrusion Detection System
ISO 27001	ISO/IEC 27001 Information Security Management System
LEI	Loss Event Impact
Most Probable Loss (MPL)	The most frequent loss observed in a year. The most frequent value claimed to the underwriter.
NIST CSF	NIST Cybersecurity Framework
NoA	Number of Attacks
OT	Operational Technology
URMS	Unit Risk Modeling System
Value at Risk (VaR) Percentile	The maximum dollar amount expected to be lost over a given time horizon (a year), at a predefined confidence level (percentile).

2 DeNexus compiles the data for you

When you deploy DeRISK, DeNexus SaaS platform, we integrate with your cybersecurity environment to automatically pull security data from every site, allowing us to quantify your cyber risks and model key risk metrics to support compliance reporting:

Value at Risk (95th percentile)

Value at Risk (99th percentile)

Most Probable Loss

Annual Expected Loss

Main Drivers of Loss

Main Types of Potential Loss

Main Drivers of Potential Loss

Loss Exceedance Curve

3 DeNexus delivers a ready-to-use Executive Report

Cybersecurity insights are typically expressed in technical terms such as CVEs in systems, lack of compliance to specific controls in a regulation, or even, when simplified, as a score A to F or Red, Yellow, Green. These might be hard to interpret for the team responsible for SEC reporting and for the board of directors.

DeNexus goes one step further: we translate cybersecurity data into business metrics and quantify cyber risk in monetary terms presented in a SEC-ready Cyber Risk Executive Report. Your CFO and the board can use DeNexus Executive Report to understand and accurately interpret how cyber risk are being managed in the organization and how to prioritize cybersecurity investments.

4 Going beyond the SEC cybersecurity regulation

DeNexus delivers the key information needed to show proactive management and governance of cyber risk in your industrial environments (OT networks).

Because we collect security insights at each site and every system, our platform, DeRisk, also delivers evidence-based recommendations on where to start with risk mitigation projects across your site portfolio and how to best allocate your cybersecurity budget to reduce cyber risk.

Main Types of Potential Loss

Loss Event	Annual Expected Loss ($)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Loss Of Productivity	$2,479,248	3.3	62.6%	0.9%
Downtime	$907,630	1.2	22.9%	0.3%
Extortion				
Equipment Damage				
Forensic Investigation				

Main Drivers of Potential Loss

Initial Access Vector (IAV)	Annual Expected Loss ($)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Exploitation Of Remote Services	$1,059,624	1.4	26.7%	0.4%
Remote Services	$907,051	1.2	22.9%	0.3%
Drive-By Compromise	$532,713	0.7	13.4%	0.2%
Phishing	$426,650	0.6	10.8%	0.2%
Spear Phishing	$390,384	0.5	9.9%	0.1%

DeNexus empowers you to optimize your cybersecurity budget.

U.S. SEC Cybersecurity Regulation
-
Cyber Risk Reporting Simplified

About DeNexus

DeNexus is the leading provider of cyber risk modeling for industrial networks, global (re)insurers and insurance linked securities (ILS) investors.

Our mission is to build the global standard for industrial cyber risk quantification for agencies, shareholders, investors, boards, and the risk transfer market.

Our flagship platform, DeRISK, is the world's first evidence-based, data-driven, self-adaptive, cloud-based technology powered by AI, ML and Probabilistic Inference that helps asset owners gain visibility into their true cyber risk exposure, probability of loss and financial impact of a cyber event that guides risk stakeholders towards the best risk mitigation paths for their organization.

Global 2000 companies in power production, energy transmission and distribution, transportation, manufacturing and hyperscale data center operations trust DeNexus today to help them prioritize cybersecurity investments.

Visit us at https://www.denexus.io