COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023 Recommendations to Prepare for and Reduce the Cost of Cyber Insurance

Before an organization considers obtaining cyber insurance, it should conduct a thorough cyber and data security risk assessment and ensure it has, and is consistently enforcing, basic "cyber hygiene" practices. Below are some recommended tasks to complete prior to seeking cyber insurance coverage to ensure your organization is prepared for and can obtain the best rate for such coverage.

Category	Task	Notes
Risk assessment	Review National Institute of Standards and Technology (NIST) standards.[1]	
	Frame the risks (determine scope and types of risk events).	
	Assess and quantify your organization's risks (determine likelihood, impact, velocity).	
	Examine risk mitigation options and internal controls (e.g., governance measures, policies, processes, and procedures). Are they effective? How much will they reduce your risk?	
	Determine how you will monitor changes in risk over time.	
Inventory of critical information assets	What types of sensitive information does the organization need to protect?	
	Where are the organization's data assets housed—in which systems and locations?	
	What are the organization's most critical information assets, and how are they currently protected?	

Category	Task	Notes
	Map the organization's critical data flows. Where does critical data enter the organization from? Does the organization send or transfer critical data outside of its systems?	
Threats	Who has access to critical or sensitive data? How is access limited or controlled?	
	Do outside third parties have access to critical or sensitive data? How is their access controlled and monitored?	
	Is critical and sensitive data encrypted while being stored?	
	Is critical and sensitive data encrypted while being transferred?	
	What level of encryption does your organization use?	
	What encryption key security practices does your organization use?	
	What steps is the organization taking to secure its hardware, network, computer systems, devices, email, and messaging data?	
Cyber hygiene	Has the organization implemented data security and privacy policies, procedures, and controls to help minimize potential damages and reduce the chances of a data security breach? If so, are these policies, procedures, and controls consistently enforced?	
	Does the organization have a formal data security program designed to protect against, monitor, and detect both internal and external threats?	
	How does the organization restrict and monitor its users?	
	Does the organization have a program to educate its employees on the role of social engineering in cyberattacks, breaches, and incidents?	

Category	Task	Notes
	Does the organization conduct due diligence on its vendors and business partners and their cybersecurity programs and ensure they have cyber insurance in place?	
	Does the organization have strong password protection controls? Is it using multifactor authentication?	
	Does the organization use whitelisting for applications and websites to protect against malicious content?	
	Is the organization patching and updating software and operating systems on a consistent basis? Does it have a continuous monitoring and auditing program in place?	
Likely cyber incidents	What types of cyberattacks, data breaches, and incidents have others in your organization's industry experienced?	
	What types of cyberattacks, data breaches, and incidents have organizations in different industries but in companies with similar sizes and global footprints experienced?	
	What costs should the organization be prepared to incur as a result of a cyberattack, breach, or incident?	
Response plan	Does your organization have an incident response plan to respond and recover from cyberattacks, breaches, and incidents?	
	Who in your organization needs to be involved in responding to a cyberattack, breach, or incident? Have you developed a RACI chart or written response plan? (A RACI chart is a project management tool describing levels of involvement in a project as Responsible, Accountable, Consulted, and Informed.)	
	Run tabletop exercises with identified response team to walk through actual tasks that will need to be completed in the event of an incident, including system security communications, government regulatory reporting and disclosure, etc.	
	Are there backup, business continuation, redundancy, and resiliency measures in place to ensure the organization can continue to operate during a cyberattack, breach, or incident?	

Category	Task	Notes
Insurance coverage	Is there insurance coverage available to help mitigate the impact or help bear the costs associated with a cyberattack, breach, or incident?	