Risk Management

We engage cross-functionally and across brands to manage potential enterprise risks – closely monitoring emerging risks related to global security, climate change and information protection.

Company-wide enterprise risk assessments are updated every quarter.

Our Global Security team uses real-time information to monitor global risks daily.

ENTERPRISE RISK MANAGEMENT

Through our formal enterprise risk management program, RCL's Audit and Advisory department performs an annual company-wide enterprise risk assessment that is updated each quarter. The scope of this assessment includes, but is not limited to, economic, social and environmental risks. It identifies those risks inherent in our business plans and strategies with the greatest potential to impact the achievement of our business objectives.

Risks are evaluated through input from the corporate leadership team. The Audit and Advisory department then reviews and discusses the risk assessments and reports on key risks to the Audit Committee each quarter. Our full Board of Directors provides oversight of our enterprise risk management and our corporate progress against key performance indicators related to human capital development, customer relationship management and other key strategic functions of our company.

OUR INTELLIGENCE PROGRAM

Over the past two decades, global security risks – such as those related to terrorism, civil unrest, crime, emerging diseases, and piracy – have been more dynamic and continue to evolve. To proactively protect our guests and crew, our Company has an Intelligence Program that is administered through the Global Security Department and aims to provide timely and tailored risk-related intelligence and analysis to broaden our understanding of the global risk environment and assist in making short- and long-term decisions with regards to operations.

MANAGING CLIMATE RISK

At RCL, we classify risks related to climate and extreme weather as a business interruption risk that is overseen by our Safety, Security, Environment and Medical/Public Health departments. To proactively manage these risks, policies and procedures have been developed and incorporated in three defined plans: our Situation Management Plan (which provides a framework to follow should a business interruption occur), our Corporate Hurricane Plan (which addresses the most probable threat as our corporate headquarters is located in South Florida) and our Information Technology Disaster Recovery Plan (which focuses on critical information technology systems and is tested on an annual basis).

Additionally, we fund and conduct research onboard our ships to better understand how climate change may impact oceans.

ADDRESSING CYBERSECURITY THREATS

Our global cybersecurity program is transforming in alignment with our "digital footprint" initiatives to enhance guest experience. RCL's Information Security organization is tasked with managing technical and behavioral cyber risks; assuring compliance to regulatory and contractual requirements; and protecting guest, employee and global supply chain partner information.

OUR FOCUS AREAS	HOW WE EXECUTE
Risk Management Processes	We aim to develop repeatable, auditable and demonstrable processes to address cybersecurity risks in collaboration with business partners and suppliers.
Internal Controls and Expertise	We invest in our internal expertise to target emerging cyber risks. We also have begun a multi-year initiative to deploy technical and behavioral controls that support our security culture.
Partnerships	We actively partner with industry peers, trade associations and government agencies. We have also contributed to the development of industry guidelines in collaboration with global maritime organization.

We acknowledge that organizational costs of global cyber risk management are difficult to quantify and predict. International regulatory and contractual requirements change based on cyber attack impact. Sources, locations, technologies, methodologies and techniques used to conduct cyber attacks change frequently. Because of our global brand presence, we may be affected by unintentional or malicious actions of employees or contractors, cyber attacks by criminal groups, nation-state or social-activist (hacktivist) organizations, geopolitical events, natural disasters or other significant events. Our proactive focus on cyber risk management may not eliminate all actual or potential cyber risk, but enables the company to effectively and thoughtfully respond to and remediate cyber risk incidents.