OVERVIEW

The Governance, Risk, and Verification (GRV) Analyst provides technical and business support to the Global Cyber Security Team for risk management tools and processes at all LVSC properties. This role is tasked with implementing, and maintaining the risk management tools. The GRV analyst will create and maintain all of the processes and procedures for the use of the tools. This position is considered the subject matter expert (SME) for the risk management tools and all of the processes and procedures that support them.

The Governance Risk and Verification Analyst reports to and provides support to the Executive Director, Global Cyber Security Policy & Training.

All duties are to be performed in accordance with departmental and Las Vegas Sands Corp’s policies, practices, and procedures.

Essential Duties & Responsibilities

Key Responsibilities

This SME will work with the Cyber team members and IT to design, deploy, configure and maintain Governance, Risk, and Verification hardware, software, and processes, including:

TOOL IMPLEMENTATION

- Functional and technical requirements gathering and documentation.
- Workflow creation and documentation.
- Coordinate the design of technical and documentation feeds to the tool. Must have experience with data feeds/ APIs, Data Driven Events, and configuration for data feeds.
- Tool deployment testing – user, functional, and technical testing.
- Project management skills including regular status reporting in accordance with the direction given by the Executive Director Governance and Risk.
- Create and communicate the processes and procedures that are internal to the team and to external tool users.
- Create, test, and deploy tool training in coordination with the Cyber Training Sr. Manager.
- Create and report project progress metrics.
TOOL’S USE

- Experienced in Cyber end-to-end governance of risk, including assessments, methodologies, mitigations, risk register.
- Experienced in verification of cyber risk mitigation.
- Experienced in reporting and explaining risk to audiences that possess varied levels of understanding.
- Track and follow-up on all due dates for risk cycle activities.
- Responsible for on-going support of the tool, and maintenance of all documentation pertaining to the tool and its use.

Key Processes

- Use of state-of-the-art Governance, Risk, Compliance (GRC) tools such as, EMC/RSA Archer, or IBM OpenPages.
- Knowledge of industry, federal, state, and international cyber regulations and their compliance. Including:
  
  PCI DSS  
  GLBA  
  Sarbanes-Oxley  
  HIPAA/HiTech  
  EU and other global PII laws and directives.

- Business Analyst experience a plus.
- Interface with business and IT stakeholders and serve as support for the program.
- Ability to build trust with customers and stakeholders.
- Strong organizational and time management skills, customer service focus, attention to detail, and process orientation.
- Ability to communicate clearly and concisely, both orally and in writing.
- Ability to distill and present information to the business community in non-technical terminology.
- Flexibly to adapt to a changing environment.
- Ability to set priorities, meet deadlines and manage projects.
- Self-motivated with the ability to execute direction from the Executive Director of Governance and Risk.

Consistent and regular attendance is an essential function of this job

Performs other related duties as assigned
Minimum Qualifications

- 21+ years of age
- Proof of authorization/eligibility to work in the United States
- Bachelor’s degree or equivalent work experience
- This position will be part of the team that is responsible for establishing and maintaining an enterprise GRV vision, strategy, and program.
- 2+ years’ experience in risk management is required.
- 2+ years’ experience in designing, deploying, and using a GRV solution is required.
- CISSP or GISP certification. 5 years’ experience in a combination of Information Technology (IT) and Information Security (Cyber) operations experience or 5 years’ experience in Cyber Operations can be substituted for the certifications.
- Knowledge and experience in cyber systems, network domain structures, identity management, security architecture, incident response, privacy and data protection, network, website, application, database, and operating systems security, and wireless networking.
- Strong understanding of Configuration Management Database (CMDB) and IT asset management.
- Experience with Microsoft server 2012, Microsoft SQL server and databases, XML/XSLT.
- Knowledge and experience with the ISO 27000/NIST/SOX/PCI series Information Security family of documents.
- Strong negotiating skills with IT, Business and Audit personnel.
- Ability to work independently on special projects.
- Participate in incident response as needed.
- Ability to communicate effectively in a positive/upbeat fashion utilizing English, both in oral and written form.
- Have interpersonal skills with focused attention to guest needs to deal effectively with all business contacts.
- Maintain a professional, neat and well-groomed appearance adhering to Company appearance standards.
- Maintain consistent adherence to the Las Vegas Sands Corp Unmatched Guest Service Standards.
- Work varied shifts, including weekends and holidays.
- Provide off-hours support on an infrequent, but as needed basis. (Potential shifts may run 24/7 due to the need of the business.)

Work Environment

- Work in a fast-paced, results-oriented and ever-changing environment
- Able to maintain composure under pressure and consistently meet deadlines with internal and external customers and contacts
- Maintain physical stamina and proper mental attitude while dealing effectively with guests, management, team members, and outside contacts
Job Segment: Risk Management, Developer, Network, System Administrator, Database, Finance, Technology