## Internal Controls, Security & Risk Management - Network Security

<table>
<thead>
<tr>
<th>Job Family</th>
<th>Grade 12</th>
<th>Grade 13</th>
<th>Grade 14 - Individual Contributor</th>
<th>Grade 14 - Management Track</th>
<th>Grade 15 - Management Track</th>
</tr>
</thead>
</table>

### Purpose:
- **Grade 12 - Security Analyst**
  - Provides ongoing support of platform management and of the security infrastructure, including automation, processes, hardware and software.
  - Responsible for advanced security support and implementing highly complex projects with impact on the network and business system applications.
  - Leads/supervises day-to-day activities in support of the planning, scaling and integrating system capabilities (complex, multiphase) in alignment with functional plans, goals, and directions.
  - Oversees the planning, scaling and integrating system capabilities (complex, multiphase) in alignment with functional plans, goals, and directions.

- **Grade 13 - Sr. Security Analyst**
  - Works independently while leading and coordinating all levels of activities including project lifecycle and day to day operations.
  - Leads and/or oversees the development of protocols and standards for all network services and may have ultimate responsibility for their implementation and documentation. Leads and performs complex implementations and/or customizations of moderate/significant size and risk.
  - Designs hard/software configurations for moderate/complex solutions to address University needs. Reviews and approves designs. Involved in the design and development effort of large and complex soft/hardware that is deemed critical to the University’s operations. Performs complex implementations and/or customizations of moderate/significant size and risk.

- **Grade 14 - Lead Security Analyst**
  - Works closely with CUIT colleagues on all tasks in the network engineering and maintenance life cycle. May be responsible for directing and monitoring the work of team members and or project teams.
  - Work with all levels of organization on problem management and resolution. Provides assistance to less senior developers. Gives guidance to other team members. May oversee team members performing specific tasks.
  - Leads specific infrastructure, systems and administration initiatives. Provides expert level assistance to less senior system engineers; functions as a technical consultant.
  - Leads and/or oversees the development of protocols and standards for all network services and may have ultimate responsibility for their implementation and documentation. Leads and performs complex implementations and/or customizations of moderate/significant size and risk.
  - Designs hard/software configurations for moderate/complex solutions to address University needs. Reviews and approves designs. Involved in the design and development effort of large and complex soft/hardware that is deemed critical to the University’s operations. Performs complex implementations and/or customizations of moderate/significant size and risk.

- **Grade 15 - Director, Security**
  - The Director is charged with developing and executing a strategy within their respective area. He/She draws on experience and/or resources with in-depth knowledge of the business or function to provide system infrastructure solutions in support of IT objectives. He/She insures all projects are delivered within budget and on time. The Director will provide leadership and overall managerial oversight to their team.
  - Communicates with senior management on system-wide issues recommending solutions including resources needed, time required and benefits to be achieved. Designs hard/software configurations for complex and University-wide solutions to address University needs. Assesses the application of new and innovative technologies, methods and concepts. Provides installation design and direction to support new technologies. May involve hardware sizing and capacity planning. Establishes the methodology, standards and protocols for installation and implementation work.

### Relation to Supervision:
- **Grade 12 - Security Analyst**
  - Works under minimal direction and often without supervision.
- **Grade 13 - Sr. Security Analyst**
  - Works under minimal direction and often without supervision.
- **Grade 14 - Lead Security Analyst**
  - Led by senior leadership team member. Sets direction and goals for department and/or team.

### Function Details:
- **Architecture, Design, Development and Installation**
  - Does assigned research, design and development, such as the design/development of a single technology for a CUIT group or a small customer group. Installs low/moderately complex soft/hardware infrastructure.
  - Responsible for the development of new implementation guidelines or standards. Provides architecture for networks. Installs moderate/complex soft/hardware infrastructure. Performs complex implementations and/or customizations.
  - Leads the development of protocols and standards for all network services and may have ultimate responsibility for their implementation and documentation. Leads and performs complex implementations and/or customizations of moderate/significant size and risk.
  - Designs hard/software configurations for moderate/complex solutions to address University needs. Reviews and approves designs. Involved in the design and development effort of large and complex soft/hardware that is deemed critical to the University’s operations. Performs complex implementations and/or customizations of moderate/significant size and risk.

### Relationship Management:
- **Bachelors degree and/or its equivalent required. Minimum 3-5 years related experience.**
  - Solid network/systems knowledge and understanding of industry standards and practices.

- **Bachelors degree and/or its equivalent required. Minimum 4-6 years related experience.**
  - Strong networking knowledge and experience with multiple technical specialties.

- **Bachelors degree and/or its equivalent required. Minimum 5-7 years related experience.**
  - Expert level networking knowledge and experience with a specific technical specialty.

- **Bachelors degree and/or its equivalent required. Minimum 5-7 years related experience.**
  - Expert level experience with a broad range of technical specialties. Prior supervisory experience strongly preferred.
<table>
<thead>
<tr>
<th><strong>Soft skills:</strong></th>
<th>Demonstrates a variety of competencies including teamwork/collaboration, analytical thinking, and communication.</th>
<th>Demonstrates proficiency in a variety of competencies including teamwork/collaboration, analytical thinking, communication and influencing skills.</th>
<th>Demonstrates excellence in a variety of competencies including ability to manage a team, teamwork/collaboration with technical and functional clients/peers, analytical thinking, communication and influencing skills. Proven ability to act as a change agent.</th>
<th>Demonstrates excellence in a variety of competencies including ability to lead a team, teamwork/collaboration with technical and functional clients/peers, analytical thinking, communication and influencing skills. High degree of emotional intelligence. Proven ability to act as a change agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Skills:</strong></td>
<td>Proficiency in some/all of the following technologies: Knowledge of Scripting, Perl, Relational Databases, Windows, Unix/Linux, Network Protocols, Network Tools, Firewalls, Forensics &amp; Analytical Procedures.</td>
<td>Strong proficiency in some/all of the following technologies: Knowledge of Scripting, Perl, Relational Databases, Windows, Unix/Linux, Network Protocols, Network Tools, Firewalls, Routers/Switches, Forensics &amp; Analytical Procedures, Data Loss Prevention.</td>
<td>Expert level skills in some/all of the following technologies: Knowledge of Scripting, Perl, Relational Databases, Windows, Unix/Linux, Network Protocols, Network Tools, Firewalls, Routers/Switches, Forensic &amp; Analytical Procedures, Data Loss Prevention. Preferred: Accreditation in CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), or CISSP (Certified Information Systems Security Professional).</td>
<td>Strong Proficiency in some/all of the following technologies: Strong proficiency in some/all of the following technologies: Knowledge of Scripting, Perl, Relational Databases, Windows, Unix/Linux, Network Protocols, Network Tools, Firewalls, Routers/Switches, Forensic &amp; Analytical Procedures, Data Loss Prevention. Accreditation in CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), or CISSP (Certified Information Systems Security Professional).</td>
</tr>
</tbody>
</table>