

International Association of Risk and Compliance Professionals (IARCP)  
1200 G Street NW Suite 800 Washington, DC 20005-6705 USA  
Tel: 202-449-9750 Web: [www.risk-compliance-association.com](http://www.risk-compliance-association.com)

## Discover 12 amazing CRCMP Jobs (and what it takes to get hired)

### Senior Information Security Risk Analyst

Public Company Accounting Oversight Board - ★★★★★ 10 reviews -  
Washington, DC

Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



### Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★★ 3,153 reviews -  
New Brunswick, NJ

[Apply On Company Site](#)

Requirements:

- Stay abreast of regulatory environment regarding VRM.

#### Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

[www.simplyhired.com/search?q=crcmp&job=BY\\_s7GxAbt4KwSJ\\_aJA\\_4KaruYRQSQ](http://www.simplyhired.com/search?q=crcmp&job=BY_s7GxAbt4KwSJ_aJA_4KaruYRQSQ)



### Crcmp jobs

Sort by Date Added More Filters

Relevance ▾

Anytime ▾

None Selected ▾

### Risk Science Business Process Lead, Senior Associate

Capital One - McLean, VA

Est. \$110,000 - \$150,000 a year ⓘ

Lean, Six Sigma, BPM, PMP, PRM, or CRCMP. McLean 1 (19050), United States of America, McLean, Virginia....

### Application Security Advisor-Penetration Tester

USAA - San Antonio, TX

Est. \$100,000 - \$140,000 a year ⓘ

Professional designation in CISSP, CISA, CRISC, CISM, CEH, GWAPT, GWEB, or CRCMP. Purpose of Job IMPORTANT:....

## *Job Description 1*

**Title:** Senior Manager, Vendor Risk Management.

**Organization:** *Johnson & Johnson Family of Companies.*

**Location:** New Brunswick, NJ.

Johnson & Johnson is recruiting for a Senior Manager Vendor Risk Management to be based in New Brunswick, NJ, Tampa, FL, or within proximity of a J&J site in Europe, Middle East, or Africa.

Caring for the world, one person at a time, inspires and unites the people of Johnson & Johnson. We embrace research and science – bringing innovative ideas, products and services to advance the health and well-being of people. Employees of the Johnson & Johnson Family of Companies work with partners in health care to touch the lives of over a billion people every day, throughout the world.

We have more than 275 operating companies in more than 60 countries, with more than 128,700 employees. Our worldwide headquarters is located in New Brunswick, New Jersey, USA.

Johnson & Johnson Global Services, the global shared services organization supporting the businesses of Johnson & Johnson, performs select functional work in a consistent manner across regions and sectors using simplified, standardized end-to-end processes and state-of-the-art technology. The vision of Johnson & Johnson Global Services is “to be trusted business partners who deliver increasing value by creating and sustaining globally standard world-class services that enable the power of Johnson & Johnson.”

There are more than 2,000 employees in Human Resources, Finance and Procurement who work for Johnson & Johnson Global Services in key service centers located in Manila, Suzhou, Prague, Bogota and Tampa, as well as in local country-based hubs.

The Senior Manager, Vendor Risk Management (VRM) is responsible for supporting the activities related to vendor risk management of Payroll Providers globally. The goal being to ensure business owners consider, understand, and monitor their respective vendor’s organizational strategic fit, risk management controls, current financial conditions and potential changes, as well as, ensure adherence to contractual requirements, delivery of agreed upon performance levels, compliance with regulatory requirements. The Vendor Risk Manager must also identify and communicate to business the associated risks of vendor provided processes, controls and services in support of critical operations.

### **Job Responsibilities:**

- Support the VRM Compliance Framework to effectively manage vendor risk in accordance with internal policy and regulatory requirements, ensure strong oversight of all risks for Payroll Vendor’s hosted externally and provide visibility of existing and emerging risks.

- Identify, categorize and evaluate “Core Processes” and “Non-core Processes”, using a “Risk-Based Standard”, for potential or current service providers; delivering to the Payroll Leadership a risk-based ranking of business-critical processes and/or services which are provided and/or delivered by an independent third party.
- Based upon Risk Classification, complete analysis of risk factors for Payroll Vendors (including any subcontractors with access to customer information) and ensure the respective business owners are monitoring, reviewing, and mitigating risk associated with service providers using the following risk factors: Regulatory Compliance, Legal, Transactional, Financial Stability, Market Reputation, Operational, Business Continuity/Disaster Recovery, and Information Security.
- Lead and complete risk analysis for onsite assessments, with the assistance of the business, ensuring consistent execution.
- Working with the appropriate business users, ensure that for any identified risk that require mitigating action, including vendor disengagement, a plan is developed and executed that indicates the process and/or service involved, the outgoing vendor, the replacement vendor, the anticipated timeline, measurable milestones, expected completion date and the plan for contingencies should an orderly transition not occur.
- Monitor compliance with VRM Policy and General Procedures in dealings with vendors for the supply of services to Johnson & Johnson.
- Maintain established relationships with the Business and applicable stakeholders to ensure proper execution and compliance with VRM policies and procedures.
- Act as a subject matter expert to assist the business in identifying and mitigating risks on their vendor relationships.
- Assist in the reporting of vendor risk management activities.
- Ensure all vendor relationships are documented in the VRM system and all contracts related to vendors that provide outsourced services are uploaded in the system.
- Promote and deliver continuous training and awareness to Business partners on vendor risk.
- Liaison with internal and external auditors, as well as, J&J IT compliance to oversee audit activities, inquires, segregation of duty tasks and 3rd Party Vendor compliance requirements.

## Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification ([CRCMP](#)) designation is preferred.

- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.
- Global experience and the ability to excel in a team environment using conflict resolution; problem solving, strong leadership, modeling and facilitation skills is required.
- Experience within a large multinational company is preferred.
- Proven ability to collaborate with other departments, building relationships and gaining commitment and resources for payroll-led initiatives required.
- Strong ability to think critically and make effective decisions in high-pressure environment required.
- Ability to interact with employees at all levels and possess excellent business writing and verbal communication skills required.
- A sense of urgency in solving audit inquiries and requests to ensure timely resolution and an ability to work effectively under pressure required.
- Comfortable handling ambiguity and fluid situations, demonstrating a pragmatic approach required.
- Strong interpersonal skills and the ability to interact skillfully and confidently with internal stakeholders and colleagues to develop ideas, identify opportunities, and influence outcomes required.
- Attention to detail required.
- Strong ability to lead, manage, mentor, and delegate as appropriate by disseminating knowledge and techniques required.
- Experience with various Payroll applications globally is preferred.
- This position will require up to 25% domestic and/or international travel.
- This position can be located in [New Brunswick, NJ](#), [Tampa, FL](#), or [within proximity of a J&J site in Europe, Middle East, or Africa](#).

## *Job Description 2*

**Title:** Head of Governance, Risk & Compliance Office.

**Organization:** SAP.

SAP is the global market leader for business software and thus contributes a considerable part of the world's economic power grid.

At SAP you get your chance to put your ideas into action with maximum impact.

Provide high quality services to the business which enable that risks are properly managed, security measures are established and SOX compliance is secured.

Increase the added business value of governance, risk, and compliance processes at SAP through high-quality business services, without compromising on transparency and compliance.

Implement global risk and security management and SOX strategies, and develop regional procedures to ensure business integration.

Continuously work on improving the risk and security management practice and SOX compliance at SAP as part of the Global GRC management team.

Maintain information and communication flows to regional executive management on GRC related topics.

Build and maintain strong partnerships with key internal decision makers, and with external risk and security management and SOX practitioners.

Liaison with other regions and information sharing.

Be a trusted advisor to regional management and employees on GRC matters.

Manage a regional GRC function by integrating corporate risk and security management, and SOX requirements.

Develop and coach risk and security and SOX personnel, and manage performance in line with SAP's leadership competencies.

Continue improving proactive Risk Management with significant contribution towards generating consistent business value.

Establish a strong executive engagement model with the APJ senior management team.

Minimum 10 years of relevant experience including project management, business operations, and/or risk management.

Long term SAP implementation project or comparable consulting or GCO experience.

Prior assignment(s) in various lines of business at SAP is a plus.

Prior experience in risk-management related activities.

MBA or Master's degree in Business Administration, Accounting, Finance, IT, Computer Science.

Preferred to have any of: [CRCMP](#), FRM, CA/CPA, CIA, CISA, CRISC, or PMP certifications

Drive and focus on results in a complex environment (cross business units, cross countries)  
Sustained high performer with proven business acumen.

Solid experience in risk, security management and SOX compliance, and a deep understanding of the associated processes, methods, and tools.

A good understanding of [how risk management, security and SOX compliance](#) is applied in the various business areas and processes.

Fluent written and spoken English is a requirement, Asian working experience an advantage.

### *Job Description 3*

**Title:** Senior Audit Manager-Consumer Compliance.

**Organization:** *American Express.*

**Location:** New York.

Execute audits related to the compliance and regulatory functions within American Express, including key regulatory requirements (AML/BSA, USA PATRIOT ACT, FCRA, Truth in Lending, Truth in Savings, Fair Lending ECOA, UDAAP, FDCPA, SCRA, and the Credit act of 2009, etc).

Audits are integrated and consider financial, operational, compliance, and technology risks.

#### **The candidate will:**

- Support business monitoring and validation activities. Participate in and lead audit meetings with regulators, and with key leaders in AXP Compliance, Technology, and Operational Risk.
- Assess the impact of control deficiencies and inherent risks, including the evaluation of compliance requirements.
- Assist in the development of an audit plan and ensure effective and efficient execution of audits in conformance with professional and department standards, budgets, and timelines.
- Assist with validation of Key Milestones surrounding compliance and regulatory gaps. This includes assessment of documentation quality and sufficiency, evaluation of management's internal validation procedures, consideration of inter-dependencies, and responsiveness to findings issued by Internal Audit or regulatory comments/ MRAs.
- Effectively handle larger and more challenging workloads on successive assignments.
- Maintain internal audit competency through ongoing professional development.
- Act as a coach to assisting resources.

Seven or more years experience in Banking, Internal Audit and/or Risk Management with an emphasis on Consumer Compliance.

BA, BS, or equivalent degree in Accounting, Finance, Technology, Compliance.

Relevant Professional Certification (CBA, CCEP, [CRCMP](#), CAMS, CISA, CIA, CPA, MBA, or equivalent).

Relevant Banking industry experience, including the management of operational or

compliance functions.

Programming knowledge. Ability to create data queries and audit retrievals.

Understanding of business technologies and its impact to control practices.

Ability to effectively integrate business, operational, technological, financial, compliance and regulatory components in audit work.

Ability to identify problems and recommend solutions to complex control, financial, technical, compliance or regulatory issues.

Strong written and verbal communication skills to deliver high quality, actionable feedback on a variety of complex issues to executive and line management on control issues and potential solutions to close control gaps.

Ability to work independently within a team construct, while supporting teamwork and achievement of team objectives.

Minimal travel may be required.



#### *Job Description 4*

**Title:** Security Administrator, New Graduate.

**Organization:** IBM.

**Location:** Canada.

The candidate will maneuver a Security Compliance landscape where daily deliverables are completed successfully, and ongoing project initiatives are kept in motion requiring interaction across several teams/departments while keeping management informed of status and potential unmitigated risk.

#### Successful candidates will perform the following:

- Ensure audit readiness by being familiar with Company and Customer(s) standard guidelines and security self-assessment workbooks with addition of monthly reporting in key areas.
- Maintain security policies, processes and tools and act as the primary focal for IBM Internal Security Compliance teams, local and global delivery teams, and management chain with respect to security issues.
- Track process handling and implementation via standardized tools/databases to ensure security compliance.
- Work with skill technicians and end-users to develop application system requirements and to determine and resolve problems throughout the related testing process by identifying potential impact and by translating business requirements into computer requirements.
- Conduct internal investigations of security breaches by leading security related audits and risk based self assessments.
- Provide recommendations to management and customers regarding security related operations.
- Mentor personnel on security requirements and associated process/policy.
- Deliver ad hoc training on new compliancy tools and act as transitional project manager during any new security tool roll out.
- Act in audit focal point role during all IT audits and liaise between internal or external auditors and Sys admin personnel ensuring communications are kept succinct and that audit etiquette is maintained and proper audit artefacts are presented for evaluation.
- Lead mitigation efforts for any possible audit defect/conditions/findings.

Preferred Qualifications/Certifications but not a requirement:

Basic knowledge in Security Information and Event Management Certified in CISSP, CISA, CISM, [CRCMP \(IARCP\)](#), [CISRCP \(IARCP\)](#).

Familiarity with Unix and Windows based operating system security.

English: Fluent

IBM is committed to creating a diverse environment and is proud to be an equal opportunity employer.

All qualified applicants will receive consideration for employment without regard to race, color, religion, gender, gender identity or expression, sexual orientation, national origin, genetics, disability, age, or veteran status.

## *Job Description 5*

**Title:** Lead Information Security Advisor.

**Organization:** USAA.

**Location:** San Antonio, TX.

**Position Type:** Full Time Job.

We are currently seeking talented Lead Information Security Advisor for our San Antonio, TX facility.

### **Purpose of the Job**

- Develops strategies and Information Security plans.
- Provides thought leadership while managing multiple large-scale initiatives.
- Collaborates with all levels of USAA management and internal partners to assess Information Security and align to support the organization goals with Enterprise goals.
- Leads Information Security risk by identifying, evaluating, assessing, designing, monitoring, administering, reporting and implementing systems, policies and processes.
- Advises various levels of senior management on Information Security risk management issues and serves as the primary resource for cross functional team members on escalated issues of a unique nature.
- Works under minimal supervision on complex and unique work assignments and recommends appropriate solutions and problem resolution.

### **Job Duties**

- Leads technical thought leadership to guide the strategic direction to executive management focusing on Information Security risk of USAA development projects, departmental initiatives and other special projects.
- Identifies and leads requirements and recommends system security configurations; oversees security briefings and responding to inquiries.
- Provides advanced advice and acts as an Information Security subject matter expert liaison between the company and staff agencies through formal and adhoc inquiries.
- Provides governance and leads identifying, analyzing and initiating changes in the Information Security policies, guidelines and standards including advising company and staff agencies in support of developing and managing the Information Security

awareness program.

- Gives counsel to ensure that internally developed and commercially available business applications include adequate Information Security controls.
- Consults process owners on the identification, development and testing of Information Security controls for risk mitigation effectiveness.
- Performs physical site assessments of business partners and provides peer review of work product and deliverables.
- Counsels and performs release of information analysis to third party business partners and identifies alternative methods for securing and releasing information when applicable.
- Leads the planning, design, development and execution of the Information Security risk and control identification, evaluation, documentation, analysis and reporting processes including analytic tools.
- Provides expert analysis and recommendations on Information Security risk assessment and mitigation to internal and external clients or other analysts.
- Influences Information Security risk management strategies and approaches and educates risk owners on best practices.
- Regularly advises senior management on key Information Security risk management efforts.
- Establishes strategic partnerships to anticipate, advise, and effectively communicate (written and verbal) Federal and State regulatory and business partner Information Security risk requirements.
- Coaches and mentors peers and cross functional team members to achieve business result, development, and delivery.

### Minimum Requirements

- Bachelor's degree in MIS, Computer Engineering, Cyber Security, IT or related disciplines, or 4 years of additional work experience in IT, Information Security, Cyber Security or equivalent in lieu of a degree.
- 6 years leading within a matrixed corporate environment.
- Advanced knowledge risk, control, budgets, process and loss costing.
- Advanced knowledge relevant industry data sources, standards, data analysis tools and techniques.

- 8 years facilitating risk assessment sessions with all levels of management and executive management.

#### Preferred.

- An advanced degree in MIS, Computer Engineering or Cyber Security. Professional designation in CISSP, CISA, CRISC, or [CRCMP](#).
- 10 years leading within a matrixed corporate environment.
- 10 years facilitating risk assessment sessions with all levels of management and executive management.
- Experience performing on site security evaluations.
- Experience with third party Information Security Oversight.

The above description reflects the details considered necessary to describe the principal functions of the job and should not be construed as a detailed description of all the work requirements that may be performed in the job.

Share our pride. Join our mission.

As a Fortune 200 financial services organization, USAA is on a mission to facilitate the financial security of our members, the men and women of the U.S. military and their families worldwide by providing a full range of financial services and products.

Headquartered on a showcase campus in San Antonio, TX, USAA attributes its longstanding success to its most valuable resource, our 26,000 employees.

They are the heart and soul of our member service culture.

Recently Ranked the #2 Place to Work in IT by Computerworld Magazine, we are recognized for the superior service we provide to our members, and the exemplary work environment we provide for our employees.

Everything that happens at USAA is based on our core values: Service, Loyalty, Honesty, and Integrity.

These are the foundations of how we do business with our members, as well as how we treat each other.

At USAA our employees enjoy one of the best benefits packages in the business, including business casual dress environment, comprehensive medical, dental and vision plans, along with wellness and wealth building programs.

Additionally, our career path planning and continuing education will assist you with your professional goals.

USAA also offers a variety of onsite services and conveniences to help you manage your work and personal life, including seven cafeterias, two company stores and three fitness centers.

Relocation assistance is available for this position.

Qualified applicants must successfully complete a preemployment background and drug screen.

USAA is an EEO/AA Employer all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, disability, protected veteran status or other status protected by law.

## *Job Description 6*

**Title:** Finance and Performance Management Systems, Risk Management, Manager.

**Organization:** *Accenture*.

**Location:** Negotiable.

Technology Growth Platform (TGP) offers a full range of global delivery services- including enterprise solutions, system integration, technical architectures, business intelligence, infrastructure consulting, and technology research/development.

Finance and Performance Management Risk professionals can expect to support clients to develop and deliver innovative solutions that can successfully and holistically transform a company's Finance and Risk capabilities.

You will support clients businesses in fulfilling compliance requirements cost- efficiently, providing insights for management to confirm that the company is on target in achieving its expected return while controlling exposure to risk.

By refining and optimizing our clients' abilities to identify risks, evaluate scenarios, determine response and monitor progress, we create substantial shareholder and economic value.

### **Basic Qualifications:**

6+ years experience in Financial Services - Finance or Risk.

3+years software configuration, design or implementation experience with one or more of the following: SAP, Oracle, PeopleSoft, Hyperion, Cognos, NetSuite, Algorithmics, SAS, Golden Source.

3+ years working in a technical or consulting environment.

Minimum of a Bachelor's Degree.

### **Preferred Qualifications:**

Demonstrated experience driving financial process improvements throughout an end to end process (e.g. Purchase to Pay, Record to Report).

Exposure to finance and risk processes (e.g., AML, RAPM, market risk, credit risk, operational risk).

Direct experience in creating business change through enabling technologies.

Professional Certifications Preferred: **CRCMP**, CRMP, CBCO CPA, CFA, CA, MBA.

Candidates who are currently employed by a client of Accenture or an affiliated Accenture business may not be eligible for consideration.

Applicants for employment in the U.S. must possess work authorization which does not require now or in the future sponsorship by the employer for a visa.



## *Job Description 7*

**Title:** Compliance Officer.

**Organization:** *Robert Half Finance.*

**Location:** New York.

A swanky and exclusive financial services company is looking for an Audit Manager for their Consumer Compliance group at their NYC office.

The person in this position will be responsible for executing audits related to the compliance and regulatory functions within the company.

This includes regulatory requirements like AML/BSA, USA Patriot Act, FCRA, Truth in Lending, Truth in Savings, Fair Lending ECAO, UDAAP, FDCPA, SCRA, and the credit act of 2009.

They will support business monitoring and validation activities in addition to assessing the impact of and development of an audit plan and its effectiveness.

### **Job Requirements**

The perfect candidate for this position will have 5+ years of previous experience in Banking, Internal Audit and/or Risk management with an emphasis in Consumer Compliance.

They will have a BA/BS in Accounting, Finance, Technology or compliance and will have a relevant professional certification (CBA, CCEP, **CRCMP**, CAMS, CISA, CIA, CPA, MBA, or equivalent).

They will have strong written and verbal communication skills and will deliver high quality feedback on a variety of issues.

### **Robert Half Finance**

Robert Half Finance & Accounting pioneered specialized financial recruitment and today is the worldwide leader. We specialize in placing professionals on a full-time basis in a variety of areas, including accounting, finance, bookkeeping, payroll, credit & collections, audit and taxation. For six decades we have been matching highly skilled accounting and finance professionals with our clients' positions. Our relationship with industry-leading companies in more than 350 locations around the globe gives you unparalleled access to exciting career opportunities.

## *Job Description 8*

**Title:** Operational Risk Officer.

**Organization:** *Hancock Bank.*

**Location:** Gulfport MS.

As member of the Enterprise Risk Management unit in Corporate Risk, Operational Risk Officer is responsible for the risk identification, assessment and mitigation processes of operational risks confronting Hancock Holding Company.

Operational Risk Officer will be responsible for the implementation of Risk and Control Self Assessment (RCSA) program for all lines of business (LOB) and corporate support units (CSU).

Essential Duties and Responsibilities include the following. Other duties may be assigned.

- Facilitates strategic RCSA process with LOB/CSU management and risk officers/liasons and conducts risk workshops and meetings to review LOB/CSU strategic playbooks and identify/assess/mitigate identified risks.
- Assists Corporate Risk Management in the development of policy / procedures, standards, templates / forms and MIS reports/systems to support RCSA process.
- Assures integrity of data, data collection and data analysis required to support operational risk dashboard metrics, operational risk reports & analysis, conducts summary evaluation of corporate operational risks, key risk indicators, risk assessment results, key performance indicators, gap assessment of strategic playbook(s), including collection of risk-related data from external resources, and recommends mitigation actions.
- Provides subject matter expertise in Basel Operational Risk and guide LOB/CSU risk personnel to effectively implement the bank's operational risk management model.
- Executes quarterly RCSA within assigned lines of business (LOB) and corporate support units (CSU) in collaboration with the respective LOB/CSU risk officers / liaisons / coordinators and collaborate with other corporate assessment areas like Compliance, IT Risk and Audit to streamline assessments.
- Provides subject matter expertise in Basel Operational Risk and guide the business segments to effectively implement the framework.
- Trains LOB/CSU risk officers/liasons/coordinators on RCSA process and operational risk matters.
- Ensures a comprehensive understanding of each coverage area's business objectives, environmental and control factors, and overall risk profile.

- Supports Director of Enterprise Risk Management (DERM) in operation and administration of Operational Risk Committee (OPCO) and respective sub-committees including OPCO reporting package, agenda and meeting minutes.
- Supports SRO and DERM in development and management of operational risk program to identify, evaluate and assess horizontal and vertical risks impacting all operational and line functions; set performance benchmarks, track enterprise losses, and recommend mitigation tactics to control losses from operational risk activities.
- Assists in development of action plans as needed, monitor progress of action plans identified in RCSA and escalate issues or delays as appropriate.
- Provides thought leadership to the organization on all matters pertaining to operational risk management.
- Attends ERM committee and sub-committee meetings.
- Supports SRO and DERM in reporting and responding to Federal Reserve, FDIC, and other pertinent regulatory bodies pertaining to enterprise risk management audits and related activities.
- Acts as a consultant to affiliates on matters pertaining to operational risk management.
- Represents the bank in civic, community and industry activities as required.
- Performs other related job duties and special projects as assigned.

## Qualifications

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required.

## Education and/or Experience Required:

- Bachelor's degree; at least four to six years related experience; or equivalent combination of education and experience.
- Risk analysis approaches - Basel II, COSO, ISO, COBIT.
- Preferred: Master's degree or equivalent and at least eight to ten years related experience.
- Mathematical Skills - Ability to work with mathematical concepts such as probability and statistical inference; Ability to apply concepts such as fractions, percentages, ratios and proportions to practical situations.

- Reasoning Ability - Ability to define problems, collect data, establish facts and draw valid conclusions; Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.

### Certificates, Licenses, Registrations

No specific requirements are needed to satisfactorily perform this job but are preferred: Professional Risk Managers International Association: PRM; [Certified Risk & Compliance Management Professional \(CRCMP\)](#); Associate in Risk Management (ARM or ARM-E Disaster Recovery Institute (DRI).

## *Job Description 9*

**Title:** Manager, Operational Risk Management

**Organization:** ADP.

**Location:** Roseland, NJ

### **Job Responsibilities:**

The Privacy & Operational Risk Team within ADP's Global Security Organization (GSO) is responsible for the design, implementation, and monitoring of ADP's global operational risk programs.

The successful candidate will be responsible for supporting the Senior Director of Global Operational Risk Management in helping lead these efforts for ADP.

The candidate must have strong skills in conducting operational, process, business, and technical analysis of problems, threats, incidents and other security related issues.

The candidate must also have the ability to communicate well, motivate and lead cross functional teams, coordinate risk, compliance, and regulatory management and operational risk remediation actions, and disseminate information as appropriate in support of ADP's critical business operations.

This position will provide overall project management and leadership support to the Senior Director of Global Operational Risk Management and will assist with the development, implementation and support of the firm's global operational risk framework, providing structured processes, tools, and assistance to business areas to capture, identify, evaluate, respond to, and report on risk issues.

Provide leadership to integrate Security Technology, Operations and Risk in creating Policy updates and training/awareness programs.

Communicate the importance of policy aspects to both executive and user communities in a technical and non-technical manner.

### **ESSENTIAL RESPONSIBILITIES:**

- Enterprise Risk Framework Design and Implementation.
- Plan, manage, and provide ongoing support for the firm's global governance, operational risk, and compliance (GRC) framework.
- Develop risk standards and best practices documentation required to support the security, risk, and compliance programs.
- Develop a corporate threat, risk, vulnerability and risk remediation assurance and

management program to identify, track, and remediate security and business operations vulnerabilities across the enterprise.

- Work with the business to design and implement operational risk and compliance assurance solutions that mitigate security threats and risks, protect the corporate infrastructure, and enable business.
- Plan, manage and conduct operational risk assessments as needed.

#### Qualifications Required:

- Bachelors' Degree or industry equivalent work experience in international enterprise and business risk planning and management in a converged risk & security program.
- Certifications such as PMP, CISSP, CIPP, [CISRCP](#), CISM, [CRCMP](#), CISA with 8-12 years of applicable experience in the Risk, Compliance, Business Security or Audit field.

## *Job Description 10*

**Title:** Risk Management Professionals, Multiple Openings. A variety of openings available from consultant to Senior Manager (27 positions).

**Organization:** *Management Consulting (confidential).*

We are one of the leading providers of management consulting services worldwide with more than 15,000 consultants in 49 countries.

Join our Risk Management team and you will play a central role in helping organizations achieve their strategic and derived operational, reporting and compliance goals.

Our experienced professionals and cutting-edge solutions enable organizations to cost-effectively manage risks initiatives and controls.

As a Risk Management Business Consultant, you will support clients businesses in fulfilling compliance requirements cost-efficiently, providing insights for management to confirm that the company is on target in achieving its expected return while controlling exposure to risk.

By refining and optimizing our clients' abilities to identify risks, evaluate scenarios, determine response and monitor progress, we create substantial shareholder and economic value.

Our Risk Management group works with clients to protect and increases economic and shareholder value while fulfilling compliance requirements cost-efficiently and implementing effective risk governance and operating models.

We have the breadth of experience, global resources, superior assets and deep knowledge and insights to help the CRO create new forms of value and to help our clients become high-performance financial services businesses.

### **Minimum Experience Required:**

2 years + of demonstrated knowledge of the fundamentals of Enterprise Risk Management.

Minimum 2 years of experience creating business cases, evaluating financial performance, creating valuation models and performing market and competitive analysis.

Bachelor's Degree in business, finance, economics or similar field

Professional Certification Preferred: CRMP, [CRCMP](#), CPA, PMP, Six Sigma, etc. a plus.

*Job Description 11:*

**Title:** Risk Management Senior Manager.

**Organization:** *Accenture Management Consulting (AMC).*

**Location:** New York NY, Washington DC, Chicago IL, Reston VA, Jersey City and Florham Park NJ, Philadelphia PA, Boston MA, Atlanta GA.

**Level:** Sr. Manager.

Accenture is a global management consulting, technology services and outsourcing company, with approximately 211,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high- performance businesses and governments.

Join the Accenture Risk Management team and you will play a central role in helping organizations achieve their strategic and derived operational, reporting and compliance goals.

Our experienced professionals and cutting-edge solutions enable organizations to cost-effectively manage risks initiatives and controls.

As a Risk Management business consultant, you will support businesses in fulfilling compliance requirements cost-efficiently, providing insights for management to confirm that the company is on target in achieving its expected return while controlling exposure to risk.

By refining and optimizing our clients' abilities to identify risks, evaluate scenarios, determine response and monitor progress, we create substantial shareholder and economic value.

We have opportunities for you to join our Accenture Management Consulting practice in Financial Services Industry, Risk Management.

Accenture's Risk Management group works with clients to protect and increase economic and shareholder value while fulfilling compliance requirements cost- efficiently and implementing effective risk governance and operating models.

We have the breadth of experience, global resources, superior assets and deep knowledge and insights to help the C-Level suite, create new forms of value and to help our clients become high-performance financial services businesses.

Much of the work we do is at the cutting edge of innovation and thinking.

We involve our consultants in publishing and sharing this knowledge as thought leadership



to benefit clients, industry and fellow colleagues.

### Basic Qualifications:

Minimum 5 years experience performing Risk/Compliance Assessments and Diagnostics within the Financial Services Industry such as in Banking, and/or Capital Markets Industries.

Minimum 5 years of work experience in Financial Services - Regulatory/Operational Compliance Management, Credit/Market Risk, Fraud, or Financial Services Risk Management.

Minimum 3 years experience within a Management Consulting firm in Risk Consulting. Bachelor's Degree.

### Preferred Qualifications:

Minimum 3 years proven successful track record, offering impeccable service delivery and client - business development.

Minimum 5 years experience with Risk/Compliance Process Design and Reengineering.

Minimum 5 years FS Risk Operating model and/or Compliance Standards at FS client

Minimum 5 years Compliance related Regulatory Requirements, such as Basel II, CRA, SEC, etc. requirements.

Minimum 5 years experience with/of the following: SAS Fraud, Dedicat, Actimize, ACI, Norkom, Memento, Fair Isaac Falcon.

Minimum 5 years of experience in the following areas: Fraud, Banking, Payments, Cards, Electronic Banking with a Finance background - Understanding of Fraud related Regulatory Requirements.

MBA, or Bachelor's degree, emphasis on business, finance, or economics preferred.

Professional Certifications Preferred: [CRCMP](#), CRMP, CBCO, CBA, Six Sigma, etc.

Choose a career at Accenture and enjoy an innovative environment where challenging and interesting work is part of daily life. With broad global resources and deep technical know-how, we collaborate with clients to cultivate ideas and deliver results.

Applicants for employment in the U.S. must possess work authorization which does not require now or in the future sponsorship by the employer for a visa. Accenture is an Equal Opportunity Employer.

*Job Description 12:*

**Title:** Corporate Risk Officer.

**Organization:** *Tompkins Financial Advisors*

**Location:** Ithaca, NY.

Responsible for directing the Corporate Risk Management (CRM) function including: Internal Audit, Compliance, BSA/AML, Information Security, and Risk Management for the company and its affiliates.

Responsible for the Enterprise Risk Management framework and Risk Management policies.

Collaborates with the Board and management to develop risk appetite for various business lines and monitor their performance relative to the established limits.

Shared responsibility for ensuring that effective operational and financial controls exist to support accurate financial reporting, and to identify and prevent fraud and other misconduct.

Through direct reports they ensure that the company's affiliates are in compliance with required regulations; that audit and compliance results are reported on a timely and systematic basis to the TFC Audit Committee, TFC BOD and affiliate boards.

Responsibilities also include managing and participating in key decision-making processes (eg strategic planning, new products and services, compensation design and operation).

Routine overnight travel is required to oversee risk-related operations throughout TFC geographic footprint – to manage staff, observe risk management infrastructure and communicate with affiliate management teams and boards.

**Primary Responsibilities:**

- Manage the implementation of all aspects of the risk function, including implementation of processes, tools and systems to identify, assess, measure, manage, monitor and report risks. Ensures that risk assessments and monitoring are prioritized and conducted in accordance with the organization's strategic direction, policies and regulations.
- Maintain current, working knowledge of evolving regulatory frameworks and fraud/threat environments, and develop strategies to proactively respond to an ever-changing regulatory & risk environment.
- Develop effective working relationships with business unit leaders to ensure that TFC strikes the appropriate balance between risk prevention and business strategy

execution, within the bounds of TFC's board-approved risk appetite.

- As a key member of TFC's \$10 Billion Asset Threshold working group, incumbent understands the various regulatory, governance, and operational impacts associated with crossing this asset threshold, and lead several sub-projects to ensure TFC's readiness.
- Establishes quantitative analyses and models to support recommended changes in risk policies and guidelines as well as new financial intuition initiatives.
- Directs the formulation and establishment of internal verification procedures consistent with sound audit theory and practice with all company affiliates.
- Serve as a resource and advisor to Management and the Board on risk related matters including those related to supervised departments, potential litigation, customer complaints, contract/ agreement drafting and review matters, incentive compensation risk assessment, products/ services, regulatory matters, fraud/ embezzlement, IT Security/ online account take-over, etc.
- Serves as a liaison to external auditors and regulatory agencies participating in audits and exams as required. Coordinates all key risk related reports for Management and the Board of Directors and Committees. Discusses significant or disputed findings and recommendations with Risk Management personnel and appropriate Management to facilitate resolution. Reports relevant information to the Board of Directors.
- Leads investigation activities relating to company assets as necessary; documents all such investigations.
- Leads risk-related due diligence and integration projects when potential acquisition candidates are being evaluated or integrated into TFC.
- Through direct reports:
  - o Directs the testing of SOX financial and fraud controls by staff and third parties throughout the company.
  - o Directs the formulation and establishment of internal verification procedures consistent with sound audit theory and practice with all company affiliates.
  - o Directs the reporting of information about the status of the company's customer accounts to customers, independent auditors, regulatory authorities, etc.
  - o Administers the established audit and compliance programs
  - o Directs the compilation of TFC Audit/Examining Committee reports.
  - o Directs the company's Pandemic Planning.

### Additional Responsibilities:

- Assist in the development of and manage processes to identify and evaluate business areas' risks and risk and control self-assessments. Recommends to Senior Management and Board Members policies and practices to reduce or improve risk exposure and loss prevention programs.
- Provide oversight and leadership to the Internal Audit, Compliance, BSA/AML, Information Security, and Risk Management Departments. Directs necessary investigations, reviews and other appropriate projects.
- Directs and makes presentations to the TFC Audit/Examining Committee for all company affiliates to inform them of audit, compliance, BSA/AML, and security results.
- Maintains and continues the development of own technical skills as well as those of direct reports through internal and external resources in order to remain current with changes in internal controls, applicable law and regulations, accounting standards, principals, techniques and new technology.
- All other duties as assigned.

### Required Qualifications:

- Bachelors or Master's Degree in: Business, Finance, Accounting, Criminal Justice or related field or professional degree or licensure in risk-related field (e.g., J.D.)
- Minimum of ten (10) years related senior management experience (including personnel management) that includes the integration of risk concepts into strategic planning, risk identification and mitigation activities in the banking, financial services or related industry.
- Strong analytical skills and ability to quickly & proactively address evolving regulatory frameworks and fraud/threat environments.
- Incumbent must have demonstrated ability to quickly absorb technical matters outside their own area of expertise, and respond to an ever-changing regulatory & risk environment.
- Ability to understand TFC's board-approved risk appetite and ensure the appropriate balance between risk prevention and business strategy execution.
- Adept at engaging appropriate stakeholders and peers throughout organization in risk/fraud mitigation strategies and regulatory compliance updates and implementation.
- Strong leadership, strategic thinking, excellent communication and presentation skills, attention to detail, independent judgment, risk assessment & problem solving

skills, strong business & financial judgment and problem solving skills.

- Deep understanding of risk management function, including Internal Audit, Compliance, Security and Risk Management theories, practices and policy development; proficient interpersonal relations skills; demonstrated management skills.
- Unequivocal integrity, ethics and commitment to corporate values.

#### Preferred Qualifications:

- Experience with regulatory examinations, including direct interaction with regulators/examiners, is strongly preferred
- Experience with physical/fraud security matters, investigations and response, including both internal fraud investigations & external fraud (payments/transfers fraud) is also plus.
- One or more of the following certifications are preferred: [Certified Risk and Compliance Management Professional \(CRCMP\)](#), [Certified Information Systems Risk and Compliance Professional \(CISRCP\)](#), Certified in Risk and Information Systems Control (CRISC), Certified Internal Auditor, CPA or J.D.

*One more career, from the public sector*

**Title:** Senior Information Security Risk Analyst.

**Organization:** *Public Company Accounting Oversight Board (PCAOB).*

**Location:** Washington, D.C.

The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, accurate and independent audit reports. The PCAOB also oversees the audits of broker-dealers, including compliance reports filed pursuant to federal securities laws, to promote investor protection.

### Job Description

The PCAOB has a full-time, regular position for a Senior Information Security Risk Analyst focusing on the areas of risk management and policy in the Office of Information Technology (OIT) at its Washington D.C. office.

You will manage and mitigate Information Security risk by identifying, evaluating, assessing, designing, monitoring, administering, reporting and implementing systems, policies and processes.

The Senior Information Security Risk Analyst provides Information Security risk insight and guides management on Information Security risk issues, and serves as advisor to peers, team members and the PCAOB staff. You will utilize your exceptional communication skills to provide leadership for your colleagues and the organization.

### Responsibilities

- Provides advice, guidance and assistance to executive management focusing on Information Security risk to guide the strategic direction of PCAOB development projects, departmental initiatives and other special projects.
- Determines requirements, recommends system security configurations, and risk mitigation effectiveness.
- Provides advice and influences Information Security risk management strategies and approaches and educates risk owners on best practices.
- Identifies, analyzes and initiates changes in the Information Security policies, guidelines and standards as well as provides governance advice to the PCAOB.
- Ensures that internally developed and commercially available business applications include adequate information and security controls.
- Designs and executes the Information Security risk and control identification,

evaluation, documentation, analysis and reporting processes including analytic tools.

- Conducts periodic audits of various applications and systems to ensure information security processes and procedures are effective.
- Assists with the investigation, documentation, and response to all suspected information security events.
- Ensures process owners identify, develop and test Information Security controls for risk mitigation effectiveness.
- Works closely with external IT auditors and internal teams on managing and supporting IT audits.
- Participates in designing, communicating, and maintaining IT security program policies and procedures.
- Serves as a mentor to peers and team members for assigned area of responsibility. Guides team members in the development and delivery of their work.
- Other duties as assigned.

### Qualifications

- Bachelor's degree in MIS, Computer Engineering, Cyber Security, IT or related disciplines OR 4 years of additional work experience in IT, Information Security, Cyber Security preferred.
- 6+ years Information Security experience within Information Technology.
- 6+ years hands-on experience conducting risk assessment sessions with all levels of management and executive management.
- In-depth knowledge and experience in relevant industry data sources, standards, data analysis tools and techniques.
- Demonstrable expertise and knowledge of risk, control, budgets, process and loss costing.
- Strong knowledge of risk monetization and costing.
- An understanding of multiple, industry-standard Information Security frameworks.
- Strong knowledge in relevant industry data sources, standards, data analysis tools and techniques.
- Experience collaborating with and influencing multiple stakeholders to solve a complex problem.

- Excellent written, oral, presentation, facilitation, negotiation and communication skills.
- Professional designation in CISSP, CISA, CRISC, or **CRCMP** preferred.

### Our Values

The PCAOB encourages a spirit of cooperation and teamwork, and fosters an environment of professional growth where employees can exercise their leadership ability, creativity, technical competence, and public interest focus in helping the PCAOB fulfill its mission.

### Equal Employment Opportunity

All PCAOB employees are entitled to equal opportunity and a professional work environment, free of discrimination and harassment. A workplace free of discrimination is fundamental to professional success and to the PCAOB's mission. The PCAOB will consider for employment all qualified applicants with criminal histories in a manner consistent with applicable law.



## Disclaimer



The CRCMP is a professional certificate recognized by the industry, provided by the International Association of Risk and Compliance Professionals (IARCP).

Neither the CRCMP nor any other professional certificate can guarantee a new or better job. There are many factors that matter, like the personality of the candidate, the supply and demand, etc.

This is what firms often require from experts:

1. To have one university degree.
2. To stay current, and to provide evidence for that, by obtaining professional certificates (the more, the better).

The IARCP is not involved in personnel recruiting.

International Association of Risk and Compliance Professionals (IARCP)  
1200 G Street NW Suite 800 Washington, DC 20005-6705 USA  
Tel: 202-449-9750 Web: [www.risk-compliance-association.com](http://www.risk-compliance-association.com)

