Massachusetts Institute of Technology

IT Risk & Security Specialist Position Description

February 9, 2015

Information Systems & Technology

Table of Contents

General Characteristics **1**
Career Path **2**
Explanation of Proficiency Level Definitions **14**
Summary Proficiency Matrix **15**
Proficiency Matrix **16**

General Characteristics

Individuals within the IT Risk & Security Specialist role plan, execute, and manage multi-faceted projects related to risk management, mitigation and response, compliance, control assurance, and user awareness. They are focused on developing and driving security strategies, policies/standards, ensuring the effectiveness of solutions, and providing security-focused consultative services to the organization. These individuals provide expertise and assistance to ensure the Institute's infrastructure and information assets are protected. Individuals also select and implement appropriate tools for necessary surveillance and monitoring of the Institute's computing environment.

Individuals develop security policies and procedures such as user log-on and authentication rules, security breach escalation procedures, security assessment procedures and use of firewalls and encryption routines. They perform security assessments and security attestations. To enforce security policies and procedures, they monitor data security profiles on all platforms by reviewing security violation reports and investigating security exceptions. They update, maintain and document security controls and provide direct support to the Institute and internal IT groups. These professionals work directly with the customers, third parties and other internal departments and organizations to facilitate information security risk analysis and risk management processes and to identify acceptable levels of residual risk. They also communicate and educate IT and the Institute about security policies and industry standards, and provide solutions for enterprise/business security issues.

These professionals require strong analytical, communication and consulting skills with knowledge of Information Security and related technologies. Individuals keep abreast of current security threats and stay current with security technology evolution.

Career Path

The following section is intended to serve as a general guideline for each relative dimension of project complexity, responsibility and education/experience within this role. This table is not intended for use as a checklist to facilitate promotions or to define specific responsibilities as outlined in a job description. Actual responsibilities and experiences may vary.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Dimension			
Work Complexity	• **Works on** IT risk and security initiatives/issues for **one or more** IT functional area (e.g., applications, systems, network and/or Web) across the enterprise. • Develops security solutions for **low** to medium complex assignments. • Works on multiple projects as a **team member** and leads systems-related security components.	• **Develops and manages** IT risk and security for multiple IT functional areas (e.g., applications, systems, network and/or Web) across the enterprise. • Develops **and manages enterprise security services such as password auditing, network based and Web application based vulnerability scanning, virus management and intrusion detection.** • Develops security solutions for medium to **complex** assignments. • Works on multiple projects as a team member or **technical lead.**	• **Oversees the planning, execution, and management of multi-faceted projects related to compliance, control assurance, risk management, security, and infrastructure/information asset protection.** • Develops and manages security for multiple IT functional areas (e.g., applications, systems, network and/or Web) across the enterprise. • **Serves as a subject matter expert (SME) for performing vendor risk assessments to improve overall vendor risk posture.** • Develops security solutions for **critical and/or highly** complex assignments. • **Leads** multiple projects or **programs**.
Typical Responsibilities			
Strategy		• Provides strategic and tactical direction and consultation on information security and compliance.	• Provides strategic and tactical direction and consultation on information security and compliance.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Project/Work Planning	• **May participate** in security planning and analyst activities.	• **Participates** in security planning and analyst activities. • **Works in combination with IT teams to ensure security is engaged in projects.**	• Participates in security planning and analyst activities. • Works in combination with IT teams to ensure security is engaged in projects.
Policies, Procedures, & Standards	• Maintains an up-to-date understanding of industry best practices. • Develops, refines, and implements enterprise-wide security policies, procedures, and standards to meet compliance responsibilities. • Supports service-level agreements (SLAs) to ensure that security controls are managed and maintained. • Monitors compliance with security policies, standards, guidelines and procedures. • Ensures security compliance with legal and regulatory standards.	• Maintains an up-to-date understanding of industry best practices. • Develops, refines and implements of enterprise-wide security policies, procedures and standards to meet compliance responsibilities. • **Monitors the legal and regulatory environment for recent developments.** • **Recommends required changes to IT risk & security policies and procedures.** • Supports service-level agreements (SLAs) to ensure that security controls are managed and maintained. • Monitors compliance with security policies, standards, guidelines and procedures. • Ensures security compliance with legal and regulatory standards.	• **Acts as primary support contact for the development of secure applications and processes.** • **Provides objective evaluations of security controls, mechanisms and goals in comparison to best practices.** • Develops, refines and implements enterprise-wide security policies, procedures, and standards **across multiple platform and application environments** to meet compliance responsibilities. • **Ensures policies, procedures, standards, and system configurations are documented and tracked**. • Monitors the legal and regulatory environment for recent developments. • Recommends, manages, and implements required changes to IT risk & security policies and procedures. • Monitors compliance with security policies, standards, guidelines and procedures.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Governance	• Assists in the development of processes and procedures for the information security governance program, including control document reviews, participant assessment preparation, meeting coordination, assessment finding mediation, assisting control owner with remediation plan development, tracking findings through remediation, progress monitoring, reporting, and escalation.	• **Develops** processes and procedures for the information security governance program, including control document reviews, participant assessment preparation, meeting coordination, assessment finding mediation, assisting control owner with remediation plan development, tracking findings through remediation, progress monitoring, reporting, and escalation.	• Develops processes and procedures for the information security governance program, including control document reviews, participant assessment preparation, meeting coordination, assessment finding mediation, assisting control owner with remediation plan development, tracking findings through remediation, progress monitoring, reporting, and escalation.
Client Requirements	• Participates with team(s) to gather a full understanding of project scope and business requirements. • Works with clients to identify security requirements using methods that may include risk and impact assessments. • Analyzes client processes and requirements to determine conformance to security policies and procedures. • Provides security-related guidance on business processes. • Participates in designing secure infrastructure solutions and applications. • May work with Institute Risk Office and Audit to ensure proper risk management and audit compliance.	• **May engage directly with clients** to gather a full understanding of project scope and business requirements. • Works with clients to identify security requirements using methods that may include risk and impact assessments. • **Consults with other Institute and technical staff on potential operational impacts of proposed changes to the security environment.** • May work with Institute Risk Office and Audit to ensure proper risk management and audit compliance. • Provides security-related guidance on client processes. • **Works closely with IT and development teams** to design secure infrastructure solutions and applications, facilitating the	• May engage directly with clients to gather a full understanding of project scope and business requirements. • **Assesses client needs against security concerns and articulates issues and potential risks to management.** • **Works** with Institute Risk Office and Audit to ensure proper risk management and audit compliance. • Consults with other Institute and technical staff on potential operational impacts of proposed changes to the security environment. • Provides security-related guidance on client process. • Works closely with IT and development teams to design secure infrastructure solutions and applications, facilitating the

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
		implementation of protective and mitigating controls.	implementation of protective and mitigating controls.
Risk Assessments	• Works directly with the clients, third parties and other internal departments and organizations to facilitate information security risk analysis and risk management processes and to identify acceptable levels of residual risk. • Conducts impact analysis to ensure resources are adequately protected with proper security measures. • Analyzes security analysis reports for security vulnerabilities and recommends feasible and appropriate options. • Creates, disseminates and updates documentation of identified information security risks and controls. • Reports on significant trends and vulnerabilities. • Develops plans to achieve security requirements and address identified risks. • Follows up on deficiencies identified in monitoring reviews, self-assessments, automated assessments, and internal and external audits to ensure that appropriate remediation measures have been taken. • Participates in the development and maintenance of a global risk framework (a single view of the	• Works directly with the clients, third parties and other internal departments and organizations to facilitate information security risk analysis and risk management processes and to identify acceptable levels of residual risk. • Conducts impact analysis to ensure resources are adequately protected with proper security measures. • **Assesses potential items of risk and opportunities of vulnerability in the network and on information technology infrastructure and applications.** • **Participates in the development of a** global risk framework (a single view of the company's risk profiles and tolerance.) • **Reviews risk assessments, analyzes the effectiveness of information security control activities, and reports on them with actionable recommendations.** • **Monitors risk mitigation and coordinates policy and controls to ensure that other managers are taking effective remediation steps.** • **Manages the oversight of technical risks assessments, such as vulnerability scanning**	• Works directly with the clients, third parties and other internal departments and organizations to facilitate information security risk analysis and risk management processes and to identify acceptable levels of residual risk. • Conducts impact analysis to ensure resources are adequately protected with proper security measures. • Assesses potential items of risk and opportunities of vulnerability in the network and on information technology infrastructure and applications. • Participates in the development and maintenance of a global risk framework (a single view of the company's risk profiles and tolerance.) • Reviews risk assessments, analyzes the effectiveness of information security control activities, and reports on them with actionable recommendations. • **Evaluates security risks and identifies and defines compliance strategies in accordance with policies and standards.** • **Provides information security management with risk assessments and security**

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
	company's risk profiles and tolerance.) • Captures, maintains, and monitors information security risk in one repository.	**and penetration testing.** • Participates in the development and maintenance of a global risk framework (a single view of the company's risk profiles and tolerance.) • Captures, maintains, and monitors information security risk in one repository.	**briefings to advise them of critical issues that may affect customer, or information security objectives.** • **Communicates with multiple departments and levels of management in order to resolve technical and procedural information security risks.** • **Develops remediation strategies to mitigate risks associated with the protection of infrastructure and information assets.** • **Captures, maintains, and monitors information security risk in one repository.** • **Serves as a subject matter expert (SME) for performing vendor risk assessments to improve overall vendor risk program.**
Information/Data Security	• Checks existing accounts and data access permission requests against documented authorizations. • Assists in the data classification process. • Develops and generates reports.	• **Consults with clients on the data classification of their resources.** • **Assesses threats and vulnerabilities regarding information assets and recommends the appropriate information security controls and measures.** • **Defines, recommends and manages security controls for information systems.** • **Manages project documentation (compliance documentation, security plans, risk assessment,**	• Assesses threats and vulnerabilities regarding information assets and recommends the appropriate security controls and measures. • Defines, recommends and manages security controls for information systems. • **Provides reports to leaders regarding the effectiveness of information security and makes recommendations for the adoption of new policies and procedures.** • **Develops and implements**

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
		corrective action plans, etc.) • **Analyzes reports and makes recommendations as needed for management decisions.**	**strategies to align information security with business objectives and goals, protecting the integrity, confidentiality and availability of data.** • **Reviews and delivers reports,** making recommendations as needed.
Institution Continuity and Disaster Recovery	• May assist with developing and documenting tactical Institution continuity and disaster recovery plans. • Assists in the development and implementation of disaster recovery test plans. • Participates in recovery drills.	• **Provides guidance on business continuity and disaster recovery design and implementation for enterprise-wide disaster recovery management programs, including maturity models, methodologies, sourcing strategies, plans, metrics and scorecards for all components of the programs.** • **Develops risk management procedures, Institution continuity scenarios, and contingencies and advises on Institution continuity and disaster recovery plans.** • **Identifies and makes recommendations regarding critical points of failure.** • **Recommends changes required to expand recovery plans.** • **Coordinates, assesses and communicates requirements associated with impact, continuity, and recovery.** • **Participates in new activities with appropriate technology groups, resulting in**	• **Contributes** to designing and implementing the enterprise-wide Institution continuity and disaster recovery management programs, including maturity models, methodologies, sourcing strategies, plans, metrics and scorecards for all components of the program(s). • Develops risk management procedures, Institution continuity scenarios, and contingencies and advises on Institution continuity and disaster recovery plans. • Identifies and makes recommendations regarding critical points of failure. • Recommends changes required to expand recovery plans. • **Reviews select changes to ensure they are appropriately assessed, tested, and incorporated into the larger enterprise plan.** • **Ensures Institution continuity and disaster recovery plans are documented and maintained.** • **Contributes to senior**

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
		recommendations to enable timely, effective decisions regarding impact, continuity, and recovery. • **Coordinates the development of disaster recovery test plans, testing, and documentation for each application.** • **Engages application and systems management in disaster recovery testing, objectives and auditing.** • **Participates in and plans recovery drills.**	**management reports on the impact, cost, and expectations of the enterprise disaster recovery plan.** • **Coordinates, assesses and communicates requirements associated with impact, continuity, and recovery.** • **Participates in new activities with appropriate technology groups, resulting in recommendations to enable timely, effective decisions regarding impact, continuity, and recovery.**
Security Assessments	• Assists/performs in security assessments and performs security attestations. • Participates in security investigations and compliance reviews as requested. • Monitors multiple logs across diverse platforms to uncover specific activities as they occur from platform to platform. • Consults with clients on security violations. • Coordinates all IT internal and external assessment components.	• Assists/performs in security assessments and performs security attestations. • Participates in security investigations and compliance reviews as requested. • **Conducts and reports on internal investigations of possible security violations.** • Consults with clients on security violations. • Coordinates all IT internal and external assessment components.	• Coordinates the **administration and logistical procedures** for disaster recovery testing, **and integration of all enterprise "critical" systems.** • **Identifies and coordinates resolution of recovery issues.** • **Ensures recovery drills are performed.** • **Analyzes recovery drills performance and recommends changes to plan, as needed.** • Participates in security investigations and compliance reviews as requested. • Consults with clients on security violations. • **Acts as liaison between internal audit and IT to ensure commitments are met and**

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
			controls are properly implemented. • **Ensures coordination** of all IT internal and external assessment components.
Security Monitoring and Reporting	• Performs security monitoring and reporting, analyzes security alerts and escalates security alerts to local support teams.	• Performs security monitoring and reporting, analyzes security alerts and escalates security alerts to local support teams.	• **Oversees security incident and response management**
IT Operations	• Provides security support for application- and infrastructure-related projects to ensure that security issues are addressed throughout the project life cycle. • Interfaces with third-party vendors to evaluate new security products. • Performs assessment of third party vendors. • Assists in the development and implementation of information security disaster recovery test plans. • Engages application and systems management in information security disaster recovery testing, objectives and assessment. • Participates in recovery drills. • Provides responsive support for problems found during normal working hours as well as outside normal working hours.	• Provides security application- and infrastructure-related projects to ensure that security issues are addressed throughout the project life cycle. • **Defines security configuration and operations standards for security systems and applications, including policy assessment and compliance tools, network security appliances, and host-based security systems.** • **Defines and validates baseline security configurations for operating systems, applications, networking and telecommunications equipment.** • Interfaces with third-party vendors to evaluate new security products **or as part of a security assessment process**. • Performs assessment of third-party vendors. • **Coordinates the development of information security disaster**	• Defines security configuration and operations standards for security systems and applications, including policy assessment and compliance tools, network security appliances, and host-based security systems. • Defines and validates baseline security configurations for operating systems, applications, networking and telecommunications equipment. • Interfaces with third-party vendors to evaluate new security products or as part of a security assessment process. • **Coordinates with vendors to ensure managed services are implemented and maintained appropriately.** • **Analyzes** security assessments for third-party vendors. • **Makes recommendations to address issues.** • **Develops impact analysis.** • **Assists business partners with**

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
		recovery test plans, testing, and documentation for each application. • **Coordinates the administration and logistical procedures for information security disaster recovery testing, and integration of all enterprise "critical" systems.** • **Identifies and coordinates resolution of recovery issues.** • **Ensures recovery drills are performed and analyzes performance.** • **Provides responsive support for problems found during normal working hours as well as outside normal working hours.**	**the determination of critical business processes and systems.** • Identifies and coordinates resolution of information security recovery issues. • Provides responsive support for problems found during normal working hours as well as outside normal working hours.
Incident Mgmt.	• Performs control and vulnerability assessments. • Identifies and resolves root causes of security-related problems. • **Responds** to security incidents, conducts forensic investigations and targets reviews of suspect areas. • **Works with** teams to resolve issues that are uncovered by various internal and third party monitoring tools.	• **Leads** and responds to security incidents and investigations and targets reviews of suspect areas. • Identifies and resolves root causes of security-related problems. • **Consults on** teams to resolve issues that are uncovered by various internal and third party monitoring tools.	• **Assists security operations team in troubleshooting and resolving escalated security** • Identifies and resolves root causes of security-related problems **and related issues.** • Consults on teams to resolve issues that are uncovered by various internal and third party monitoring tools.
Information Security Performance Management	• Generates ad hoc and routine performance reports. • **Analyzes** reports and makes recommendations for improvements.	• **Monitors** and analyzes information security performance reports and escalates issues as needed. • Communicates reporting results	• **Develops measures to evaluate the information security programs and modifies strategies as appropriate.** • **Reviews and delivers**

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
	• Communicates reporting results to information security management.	**and analytical evaluation** to information security management.	**information security performance summary with analytical evaluation to leadership teams, as needed.** • **Identifies areas needing improvement and develops recommendations.** • **Anticipates and addresses potential issues.**
Research/ Evaluation	• Assists in application security risk assessments for new or updated internal or third party applications. • **Assists in the evaluation** and recommendation for tools and solutions that provide security functions.	• Leads and reviews application security risk assessments for new or updated internal or third party applications. • **Evaluates** and recommends tools and solutions that provide security functions. • **Maintains contact with vendors regarding security system updates and technical support of security products.**	• Leads and reviews application security risk assessments for new or updated internal or third party applications. • Evaluates and recommends tools and solutions that provide security functions. • Maintains contact with vendors regarding security system updates and technical support of security products. • **Assists in cost-benefit and risk analysis.**
Communications/ Consulting	• Collaborates on projects to ensure that security issues are addressed throughout the project life cycle. • Informs stakeholders about compliance and security-related issues and activities affecting the assigned area or project. • Interfaces regularly with staff from various departments communicating security issues and responding to requests for assistance and information. • Reports to management	• **Serves in an advisory role in application development and infrastructure projects to assess security requirements and controls and ensures that security controls are implemented as planned.** • Collaborates on projects to ensure that security issues are addressed throughout the project life cycle. • Informs stakeholders about compliance and security-related issues and activities affecting the	• Serves in an advisory role in application development and infrastructure projects to assess security requirements and controls and ensures that security controls are implemented as planned. • Collaborates on projects to ensure that security issues are addressed throughout the project life cycle. • Informs stakeholders about compliance and security-related issues and activities affecting the assigned area or project.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
	concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance.	assigned area or project. • Interfaces with **Institute and IT leaders** communicating security issues and responding to requests for assistance and information. • Reports to management concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance.	• Interfaces with Institute and IT leaders communicating security issues and responding to requests for assistance and information. • Reports to management concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance. • **Represents security and IT risks among other company risk departments and committees.**
Training	• Assists in the development and delivery of IT risk & security awareness and compliance training programs • May guide users on the usage and administration of security tools that control and monitor information security.	• **Develops and delivers** IT risk & security awareness and compliance training programs. • **Provides security briefings to advise on critical issues that may affect the client.** • **Conducts knowledge transfer training sessions to security operations team upon technology implementation.**	• **Drives IT changes to ensure effective risk based implementations, awareness and accountability.** • **Evaluates the effectiveness of awareness and training programs and makes recommendations for improvement.** • Provides security briefings to advise on critical issues that may affect the client. • Conducts knowledge transfer training sessions to security operations team upon technology implementation.
Organization Change Management			• Generates appropriate communication, process and educational plans for mitigating the disruption of change. • Identifies and removes obstacles to change.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Coaching / Mentoring	• Coaches less-experienced team members.	• **Provides ongoing knowledge transfer to team members and clients on security products and standards.** • Coaches less-experienced team members.	• Provides ongoing knowledge transfer to team members and clients on security products and standards. • Coaches less-experienced team members.
Typical Education / Experience	• Bachelor's Degree in Computer Science, Information Systems or other related field, or equivalent work experience. • Typically has 3-5 years of combined IT and security work experience with a broad range of exposure to systems analysis, application development, database design and administration. • Requires knowledge of security issues, techniques and implications across all existing computer platforms.	• Bachelor's Degree in Computer Science, Information Systems or other related field, or equivalent work experience. • Typically requires **5-7** years of combined IT and security work experience with a broad range of exposure to systems analysis, application development, systems administration **and 1-3 years of experience with IT security.** • **Working** knowledge of security issues, techniques and implications across computer platforms. • **Experience designing and implementing security solutions.** • **Requires Security Certification (i.e., Certified Information Systems Security Professional (CISSP).**	• Bachelor's Degree in Computer Science, Information Systems or other related field, or equivalent work experience. • Typically requires **7 or more** years of combined IT and security work experience with a broad range of exposure to systems analysis, application development, systems administration and **over 5 years' experience designing and deploying security solutions.** • Requires in-depth knowledge of security issues, techniques and implications across all existing computer platforms. • Requires Security Certification(s) (i.e., Certified Information Systems Security Professional (CISSP), **or Certified Information Security Manage (CISM).**

Explanation of Proficiency Level Definitions

Proficiency scale definitions are provided to help determine an individual's proficiency level in a specific competency. The rating scale below was created as a foundation for the development of proficiency level definitions used for assessments.

Being Developed: (BD)	Demonstrates **minimal** use of this competency; limited knowledge of subject matter area; needs frequent assistance and **close supervision** for direction. Currently developing competency.
Basic: (B)	Demonstrates **limited** use of this competency; basic familiarity of subject matter area; needs additional training to apply without assistance or with **frequent supervision**.
Intermediate: (I)	Demonstrates **working or functional proficiency** level sufficient to apply this competency effectively without assistance and with **minimal supervision**; working/functional knowledge of subject matter area.
Advanced: (A)	Demonstrates **in-depth proficiency** level sufficient to assist, consult to, or lead others in the application of this competency; in-depth knowledge in subject matter area.
Expert: (E)	Demonstrates broad, in-depth proficiency sufficient to be recognized as an **authority or master performer** in the applications of this competency, recognized authority/expert in subject matter area.

As you complete the competency assessment, read all of the proficiency level definitions for a competency (provided in the next section) and select the one that is most characteristic of the demonstrated performance. If more than one definition is descriptive, select the highest level that is typically exhibited.

Summary Proficiency Matrix

The chart provides a summary of proficiency ratings.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Competencies			
Accountability: Clearly defines mutual expectations of self and others. Takes appropriate actions to ensure obligations are met. Revises standards in response to change.	**I**	**A**	**A**
Change Advocate: Identifies and acts upon opportunities for continuous improvement. Encourages prudent risk-taking, exploration of alternative approaches, and organizational learning. Demonstrates personal commitment to change through actions and words. Mobilizes others to support change through times of stress and uncertainty.	**B**	**I**	**A**
Consulting: Uses professional knowledge, experience and technical expertise to respond to questions, facilitate problem-solving, and generally advise, influence and provide guidance to customers and business partners over whom there is no direct authority.	**B**	**I**	**A**
Decisiveness: Assesses the scope and potential impact of an issue or opportunity. Uses business criteria and values to evaluate alternative courses of action. Makes a timely choice based on the options and information available.	**B**	**I**	**A**
Information Seeking: Gathers and analyzes information or data on current and future trends of best practice. Seeks information on issues impacting the progress of organizational and process issues. Translates up to date information into continuous improvement activities that enhance performance.	**B**	**I**	**A**
Risk Management: Identifies risks and obstacles to plans. Defines scarcity and conflicts of resource needs, and potential constraints. Investigates risks within various project elements, assesses impact, and develops contingency plans to address major risks.	**B**	**I**	**A**
Thoroughness: Demonstrates attention to detail and accuracy. Defines and organizes tasks, responsibilities and priorities. Takes responsibility for timely completion.	**I**	**A**	**E**

Proficiency Matrix

The following charts illustrate proficiency levels for each competency.

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Competencies			
Accountability: Clearly defines mutual expectations of self and others. Takes appropriate actions to ensure obligations are met. Revises standards in response to change.			
Being Developed (BD): Asks questions and provides feedback in an effort to clarify mutual expectations. Seeks advice on tasks and responsibilities when needed.			
Basic (B): Checks assumptions about mutual expectations and clarifies standards of performance. Checks the scope of responsibilities of self and others. Monitors day-to-day performance, and takes corrective action when needed to ensure desired performance is achieved.	✓		
Intermediate (I): Sets objectives that meet organizational needs. Provides recommendations to individuals and teams on ways to improve performance and meet defined objectives. Monitors and provides feedback on individual and team performance against defined standards.		✓	
Advanced (A): Sets enhanced objectives for self and others. Monitors performance trends and identifies opportunities to improve standards. Provides regular feedback and suggests alternative approaches necessary to ensure that organizational objectives and superior standards are achieved. Delegates responsibility and reallocates resources as needed to ensure that priorities are met.			✓
Expert (E): Defines strategic areas of responsibility. Plans and decides upon the reassigning and restructuring of significant organizational resources. Influences and sponsors cross-organizational decisions on work prioritization, resource allocation and long-range standards of performance.			

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Change Advocate: Identifies and acts upon opportunities for continuous improvement. Encourages prudent risk-taking, exploration of alternative approaches, and organizational learning. Demonstrates personal commitment to change through actions and words. Mobilizes others to support change through times of stress and uncertainty.			
Being Developed (BD): Supports change initiatives by following new directions as directed and providing appropriate information. Asks for feedback and ideas on how to do a better job and tries new approaches.			
Basic (B): Participates in change initiatives by implementing new directions and providing appropriate information and feedback. Offers ideas for improving work and team processes. Experiments with new approaches and improves productivity through trial and error.	✓		
Intermediate (I): Participates in change programs by planning implementation activities with other change champions. Interprets the meaning of new strategic directions for the work group and sets objectives and standards. Implements monitoring and feedback systems. Evaluates progress and finds ways of making continuous improvements. Solicits and offers ideas for improving primary business processes. Improves effectiveness and efficiency through the involvement of peers and business partners by initiating new approaches.		✓	
Advanced (A): Leads the planning and implementation of change programs that impact critical functions/processes. Partners with other resource managers/change agents to identify opportunities for significant process enhancements. Recommends changes that impact strategic business direction. Sets expectations for monitoring and feedback systems and reviews performance trends. Evaluates progress and involves peers and team members in analyzing strengths and weaknesses in performance. Improves efficiency by spearheading pilots and planned functional change initiatives.			✓
Expert (E): Reviews, sponsors and approves recommendations for enterprise-wide change programs that impact cross functional key processes. Partners with other business leaders to identify opportunities for significant technology/process enhancements. Lobbies for changes that impact strategic business direction. Approves strategic monitoring criteria and reviews high impact enterprise performance trends. Evaluates progress against key performance drivers and assesses organizational opportunities and risks. Solicits the support of business leaders in planning and spearheading enterprise change initiatives.			

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Consulting: Uses professional knowledge, experience and technical expertise to respond to questions, facilitate problem solving, and generally advises, influences and provides guidance to customers and business partners over whom there are no direct authority.			
Being Developed (BD): Shares information in relation to procedures and routine activities. Provides guidance and advice. Suggests caution as appropriate. Asks questions that raise awareness and demonstrate insight.			
Basic (B): Shares information and reports on the immediate situation. Provides feedback and advice as appropriate in relation to procedures and routine activities. Asks questions that raise awareness and demonstrate insight.	✓		
Intermediate (I): Conducts investigations and interprets issues within operational and professional contexts. Provides guidance and counsel. Suggests caution to impacted areas as appropriate in relation to matters of policy interpretation and implementation of operational improvement. Conducts discussions that share information and trigger solutions and improvements.		✓	
Advanced (A): Leads research and summarizes requirements for the engagement. Interprets issues within the framework of core business processes. Provides substantiated, risk-assessed options and counsel in relation to process enhancement and professional expertise. Facilitates dialogues that produce new perspectives and trigger recommendations for substantial innovative enhancements, and analysis of consequences.			✓
Expert (E): Collaborates with clients to determine the scope of engagement. Advises senior leaders on environmental analysis, planning opportunities, and implementation considerations for strategic interventions. Researches long-range world-class business and technology trends. Uses formal techniques of facilitation and analysis to assist leadership in criterion-based decision-making and strategic planning.			

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Decisiveness: Assesses the scope and potential impact of an issue or opportunity. Uses business criteria and values to evaluate alternative courses of action. Makes a timely choice based on the options and information available.			
Being Developed (BD): Applies values, policies and procedures to make timely, routine decisions of limited, clear choice. Seeks instructions or escalates matters that require judgment.			
Basic (B): Applies values, policies, procedures and precedent to make timely, routine decisions of limited, clear choice. Seeks advice and guidance or escalates matters that require judgment.	✓		
Intermediate (I): Applies values, business strategy, policies, procedures and precedent to make timely decisions with limited consequences. Gathers data to support recommendations and seeks approval for taking action that will set precedent while minimizing potential risk.		✓	
Advanced (A): Applies values, business strategy, policies, precedent, and experience to make complex decisions with uncertain consequences. Makes benchmarked, researched recommendations with contingency plans in place for potential adverse consequences. Lobbies business partners and subject matter experts for consensus in taking action that sets direction in at least one critical business function. Promotes a tolerance for risk within boundaries that equate with the benefits.			✓
Expert (E): Applies values, business strategy and collective experience to make policy decisions with incomplete, conflicting information and uncertain long-term consequences. Sponsors and approves benchmarked, researched recommendations with contingency plans in place. Participates with senior business leaders and subject matter authorities in defining strategies and courses of action that will impact the enterprise. Makes timely decisions that set enterprise-wide direction. Promotes a tolerance for high long-term risk that equates with significant returns on the investment.			

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Information Seeking: Gathers and analyzes information or data on current and future trends of best practice. Seeks information on issues impacting the progress of organizational and process issues. Translates up to date information into continuous improvement activities that enhance performance.			
Being Developed (BD): Asks questions and solicits procedural information that explains how day-to-day tasks are conducted. Collates facts and data. Checks and monitors progress of activities in area of responsibility. Seeks out the appropriate people for guidance when needed to get things done.			
Basic (B): Seeks information on both formal and informal processes. Uses appropriate tools, techniques and sources to gather, update and monitor information. Checks for accuracy of interpretation. Seeks out the appropriate people for guidance when needed depending on the type of issue.	✓		
Intermediate (I): Utilizes a variety of information and data sources pertaining to organizational and professional trends. Checks the source for omission and accuracy. Identifies the sources that are appropriate for specific types of information. Checks for bias and omission. Seeks out the appropriate people to approach for guidance either formally or informally depending on the type of issue. Links information in a lateral as well as linear manner. Finds hidden data. Relates and manipulates data from various sources to create a fuller picture. Investigates and uncovers root causes of a problem or issue.		✓	
Advanced (A): Researches organizational and professional trends. Networks internally and externally on areas of interest and concern. Evaluates sources, and collates and compares findings for bias, omission and accuracy. Conducts objective analysis. Prioritizes information by source. Monitors systematically. Deploys resources (time, people, and systems) to ensure timely management reporting. Reviews and determines need for corrective action and/or business opportunities.			✓
Expert (E): Studies environmental, business and technological trends and forecasts. Networks among thought leaders and strategic influencers. Differentiates data sources for validity, reliability and credibility. Tracks and synthesizes systemic benchmarking trends. Evaluates composite information in relation to its impact on decision-making and strategic implications. Sets expectations for and reviews management and key stakeholder reports. Assesses validity of business strategy recommendations against trend data. Steers senior leadership towards making informed, sound strategic decisions.			

Title	IT Risk & Security Specialist I	IT Risk & Security Specialist II	IT Risk & Security Specialist III
Thoroughness: Demonstrates attention to detail and accuracy. Defines and organizes tasks, responsibilities and priorities. Takes responsibility for timely completion.			
Being Developed (BD): Applies attention to detail to routine tasks defined in formal, written procedures and oral instructions. Seeks guidance on the quality and the degree of completion required for completing new tasks. Reprioritizes, as new deadlines are set. Responds constructively to customer feedback on task output.			
Basic (B): Performs tasks according to quality and output standards. Takes initiative to ensure that outcomes meet internal and external customer requirements. Solicits feedback on performance in new tasks. Measures accuracy using performance metrics. Sets improvement standards to reduce errors, omissions and oversights.	✓		
Intermediate (I): Demonstrates operational agility. Uses organizational systems that result in multiple critical activities to be identified and completed on time. Renegotiates priorities as necessary. Puts systems in place and uses them to monitor and detect errors and problems. Tests and inspects outputs, and applies quality checks prior to work submission.		✓	
Advanced (A): Identifies potential areas of conflicting priorities and vulnerability in achieving standards. Reviews department's progress against established goals, objectives, service level targets and project milestones. Supports others in achieving deliverables by efficiently allocating resources and providing common organizing systems, techniques and disciplines. Maintains a proactive work review and approval process prior to assignment completion. Solicits internal and external customer evaluation of performance and devises measures for improvement.			✓
Expert (E): Sets the vision, defines the value and acts as role model for creating a culture that sets superior standards and delivers on time and on budget. Agrees upon service level and project expectations with senior leaders. Reviews enterprise's progress against established goals, objectives, service level targets and project milestones. Devises strategies for delivering large-scale projects on time. Proactively conducts business review meetings for reprioritization of resources and taking corrective action to respond to strategic initiatives. Holds self and leadership team members accountable for achievements, publicly recognizing successes. Identifies areas of potential vulnerability in achieving strategic business drivers. Supports the enterprise in achieving deliverables by investing in world-class organizational processes.			

Any questions regarding this Report should be addressed to:

Diana Hughes
Director of HR and Administration
Information Systems and Technology
Massachusetts Institute of Technology
(617) 253-6205
dhughes@mit.edu