

**GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST**

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through GSA Advantage!, a menu-driven database system. The Internet address for GSA Advantage! is: <http://www.gsaadvantage.gov>

**WORLDWIDE FEDERAL SUPPLY SCHEDULE CONTRACT
SCHEDULE TITLE: GENERAL PURPOSE COMMERCIAL INFORMATION
TECHNOLOGY EQUIPMENT, SOFTWARE, AND SERVICES**

FSC GROUP: 70

**CONTRACT NUMBER:
GS-35F-0417X**

**PERIOD COVERED BY CONTRACT:
June 9, 2011 - June 8, 2021**

**Enterprise Risk Management, Inc.
800 S. Douglas Road, #940N
Coral Gables, FL 33134
(P) (305) 447-6750
(F) (305) 447-6752
<http://www.emrisk.com/>**

CONTRACTOR'S ADMINISTRATION SOURCE:
Silka M Gonzalez
President
Phone: 305-447-6750
Email: info@emrisk.com

General Services Administration
Management Services Center Acquisition Division
Modification #**PO-0004**, dated **June 9, 2016**

Business Size: SBA certified 8(a) / WOSB / EDWOSB / SBA Certified Disadvantage Business

DUNS: 610144201

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at <http://www.fss.gsa.gov>.

TABLE OF CONTENTS

GSA AWARDED TERMS AND CONDITIONS ENTERPRISE RISK MANAGEMENT, INC.....	3
TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF TRAINING COURSES FOR GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE (SPECIAL ITEM NUMBER 132-50).....	6
DESCRIPTION OF TRAINING COURSES (SIN 132-50).....	8
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51).....	19
LABOR CATEGORY DESCRIPTIONS (SIN 132-51).....	23

**GSA AWARDED TERMS AND CONDITIONS
ENTERPRISE RISK MANAGEMENT, INC.**

1a. **TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)**

**SPECIAL ITEM NUMBER 132-50 - TRAINING COURSES (FPDS Code U012)
SPECIAL ITEM NUMBER 132-51 - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES**

FPDS Code D301 IT Facility Operation and Maintenance
FPDS Code D302 IT Systems Development Services
FPDS Code D306 IT Systems Analysis Services
FPDS Code D307 Automated Information Systems Design and Integration Services
FPDS Code D308 Programming Services
FPDS Code D310 IT Backup and Security Services
FPDS Code D311 IT Data Conversion Services
FPDS Code D313 Computer Aided Design/Computer Aided Manufacturing (CAD/CAM) Services
FPDS Code D316 IT Network Management Services
FPDS Code D317 Creation/Retrieval of IT Related Automated News Services, Data Services, or Other Information Services (All other information services belong under Schedule 76)
FPDS Code D399 Other Information Technology Services, Not Elsewhere Classified

Note 1: All non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately.

Note 2: Offerors and Agencies are advised that the Group 70 – Information Technology Schedule is not to be used as a means to procure services which properly fall under the Brooks Act. These services include, but are not limited to, architectural, engineering, mapping, cartographic production, remote sensing, geographic information systems, and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

Note 3: This solicitation is not intended to solicit for the reselling of IT Professional Services, except for the provision of implementation, maintenance, integration, or training services in direct support of a product. Under such circumstances the services must be performance by the publisher or manufacturer or one of their authorized agents.

1b. **LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN:** See attached GSA awarded Pricelist

1c. **HOURLY RATES (Services Only):** See attached GSA Awarded Pricelist

2. **MAXIMUM ORDER*:**
SIN: 132-50: \$25,000
SIN: 132-51: \$500,000

*If the “best value” selection places your order over this Maximum Order identified in this catalog/pricelist, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contractor for a better price. The contractor may (1) offer a new price for this requirement; (2) offer the lowest price available under this contract; or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the Schedule contract in accordance with FAR 8.404

3. **MIMINUM ORDER:** \$100
4. **GEOGRAPHIC COVERAGE:** Domestic and overseas delivery.
5. **POINT(S) OF PRODUCTION:** N/A
6. **DISCOUNT FROM LIST PRICES:** Refer to attached Awarded Pricelist
7. **QUANTITY DISCOUNT(S):** 2% for orders over \$100,000 for both SIN 132-50 and SIN 132-51
8. **PROMPT PAYMENT TERMS:** Net 5% 10 days for both SIN 132-50 and SIN 132-51
- 9a. Government purchase cards *are accepted* at or below the micro-purchase threshold
- 9b. Government purchase cards *are not accepted* above the micro-purchase threshold
10. **FOREIGN ITEMS:** N/A
- 11a. **TIME OF DELIVERY:** To be negotiated at the task order level
- 11b. **EXPEDITED DELIVERY:** To be negotiated at the task order level
- 11c. **OVERNIGHT AND 2-DAY DELIVERY:** To be negotiated at the task order level
- 11d. **URGENT REQUIREMENTS:** To be negotiated at the task order level
12. **FOB POINT:** Destination
- 13a. **ORDERING ADDRESS:**

Enterprise Risk Management, Inc.
800 S. Douglas Road, #940N,
Coral Gables, FL 33134.
P: +1.305.447.6750
F: +1.305.447.6752
- 13b. **ORDERING PROCEDURES:** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in FAR 8.405-3
14. **PAYMENT ADDRESS:**

Enterprise Risk Management, Inc.
800 S. Douglas Road, #940N,
Coral Gables, FL 33134.
P: +1.305.447.6750
F: +1.305.447.6752
15. **WARRANTY PROVISION:** N/A
16. **EXPORT PACKING CHARGES:** N/A
17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:**
Accepted at or below the micro-purchase threshold
18. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (if applicable).** N/A

19. **TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):** N/A
20. **TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE):** N/A
- 20a. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):** N/A
21. **LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE):** N/A
22. **LIST OF PARTICIPATING DEALERS (IF APPLICABLE):** N/A
23. **PREVENTIVE MAINTENANCE (IF APPLICABLE):** N/A
- 24a. **SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants):** N/A
- 24b. **Section 508 Compliance for EIT:** as applicable
25. **DUNS NUMBER:** 610144201
26. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE:** Active

**TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF
TRAINING COURSES FOR GENERAL PURPOSE COMMERCIAL
INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE
(SPECIAL ITEM NUMBER 132-50)**

1. SCOPE

- a. The Contractor shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of this solicitation.
- b. The Contractor shall provide training at the Contractor's facility and/or at the ordering activity's location, as agreed to by the Contractor and the ordering activity.

2. ORDER

Written orders, EDI orders (GSA Advantage! and FACNET), credit card orders, and orders placed under blanket purchase agreements (BPAs) shall be the basis for the purchase of training courses in accordance with the terms of this contract. Orders shall include the student's name, course title, course date and time, and contracted dollar amount of the course.

3. TIME OF DELIVERY

The Contractor shall conduct training on the date (time, day, month, and year) agreed to by the Contractor and the ordering activity.

4. CANCELLATION AND RESCHEDULING

- a. The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date, if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.
- b. In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the ordering activity will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.
- c. The ordering activity reserves the right to substitute one student for another up to the first day of class.
- d. In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

5. FOLLOW-UP SUPPORT

The Contractor agrees to provide each student with unlimited telephone support or online support for a period of one (1) year from the completion of the training course. During this period, the student may contact the Contractor's instructors for refresher assistance and answers to related course curriculum questions.

6. PRICE FOR TRAINING

The price that the ordering activity will be charged will be the ordering activity training price in effect at the time of order placement, or the ordering activity price in effect at the time the training course is conducted, whichever is less.

7. INVOICES AND PAYMENT

Invoices for training shall be submitted by the Contractor after ordering activity completion of the training course. Charges for training must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

8. FORMAT AND CONTENT OF TRAINING

- a. The Contractor shall provide written materials (i.e., manuals, handbooks, texts, etc.) normally provided with course offerings. Such documentation will become the property of the student upon completion of the training class.
- b. ****If applicable**** For hands-on training courses, there must be a one-to-one assignment of IT equipment to students.
- c. The Contractor shall provide each student with a Certificate of Training at the completion of each training course.
- d. The Contractor shall provide the following information for each training course offered:
 - (1) The course title and a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);
 - (2) The length of the course;
 - (3) Mandatory and desirable prerequisites for student enrollment;
 - (4) The minimum and maximum number of students per class;
 - (5) The locations where the course is offered;
 - (6) Class schedules; and
 - (7) Price (per student, per class (if applicable)).
- e. For those courses conducted at the ordering activity's location, instructor travel charges (if applicable), including mileage and daily living expenses (e.g., per diem charges) are governed by Pub. L. 99-234 and FAR Part 31.205-46, and are reimbursable by the ordering activity on orders placed under the Multiple Award Schedule, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts. The Industrial Funding Fee does NOT apply to travel and per diem charges.
- f. For Online Training Courses, a copy of all training material must be available for electronic download by the students.

9. "NO CHARGE" TRAINING

The Contractor shall describe any training provided with equipment and/or software provided under this contract, free of charge, in the space provided below.

Not Applicable

DESCRIPTION OF TRAINING COURSES (SIN 132-50)

Information Security – Basics and Awareness

Brief Description: The training course covers the basic aspects of information security and awareness. The course is meant for students with minimal knowledge in the concepts of information security. This could include administrative staff, non-technical staff, management, and anyone else that may be interested in gaining a basic overview of how he/she can help the organization in protecting its information assets and improving its information security defenses by exercising and promoting an —attitude of securityl.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Data Privacy

Brief Description: The training course covers key concepts in data privacy and how it applies in the regulatory landscape. The course will include non-technical aspects of data privacy that focus more on the implications for the organization as a whole. Senior management and top-level management would benefit most from this course as it delves into key regulatory compliance aspects as well as short-term and long-term organizational strategy.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Regulatory Compliance and Information Security

Brief Description: The training course aims to educate students on information security centric regulatory compliance requirements, applicability, and issues. Depending on the organization in question, the training course shall focus on applicable information security related regulations and standards. These include, but not limited to, the Bank Secrecy Act (BSA), Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Family Education Rights and Privacy Act (FERPA), and the Payment Card Industry Data Security Standard (PCI DSS). This course will be most helpful to implementers of regulatory compliance measures in organizations and also to senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Network Security and Ethical Hacking

Brief Description: The training course provides students with an in-depth insight into how hackers operate, the tools and techniques they use, and an overall picture of the modus operandi of hackers. This course will help in obtaining

a detailed understanding of hackers and also teach students on how ethical hacking can be used to secure organizations. Such an understanding is helpful to design the defensive strategy of the organization and to know the enemy better. The course will cover fundamental concepts in ethical hacking and explain different methodologies and practices used to conduct ethical hacking tests. The course shall be technical in nature but non-technical audiences are encouraged to attend. This is not a hands-on course which teaches students how to hack. Rather, it is a course that will provide students with an understanding of how hackers function. The course will be most beneficial to technical staff and information security staff. Senior and top management will also find this course beneficial as will any other non-technical staff member that may be interested.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Ethical Hacking Live Demonstration

Brief Description: The training course is a great supplement to the Network Security and Ethical Hacking course. This course provides a more practical and demonstrative perspective on ethical hacking and the tools and techniques used by hackers. The course shall be highly technical in nature. Non-technical audiences may attend if interested, but might require more effort to follow and benefit from the course. The course will be most beneficial to technical staff and information security staff. Senior and top management may attend to gain an idea of how hackers attack organizations. While they may not follow the technical aspects of the course, it will be helpful in putting things into perspective.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Social Engineering

Brief Description: The training course aims to strengthen the weakest link in information security – people. Non-technical methods of hacking into organizations and compromising information have proven to be very effective over the years. This course delves into social engineering techniques that aim to exploit the inherent helpfulness, gullibility, and psyche of human nature. Social engineers manipulate employees into unwittingly divulging confidential information that can provide the criminals with access into the target organization's computer systems, devices, databases, and other critical technical infrastructure elements. Being aware of social engineering is very important for organizations to fortify their —human firewall. Students will learn about the latest techniques in use that are successfully penetrating organizations. Students will also understand the different methodologies that can be used to raise the level of security awareness in an organization and its employees. The awareness that this course will generate will be invaluable to all employees of organizations and can help incorporate an atmosphere of information security and responsible attitudes at the organization. Employees from all departments are encouraged to attend, as are senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Security Breaches and Investigation

Brief Description: The training course helps students understand the implications and aftereffects of an information security breach. The course delves into details of how an information security breach should be handled at an organization, the regulatory implications, the technical and strategic implications, the process of investigating a breach, and how remediation should be approached. When protected data is lost, you must move quickly to protect customers, comply with disclosure laws, and avoid damaging front-page headlines. This course will help students learn the critical steps to take immediately after a data breach to comply with new laws and prevent legal, financial, and reputational damage. Students will learn how to secure their organization against a data breach. Lastly, the course will review case studies to illustrate some of the hidden and surprising data security dangers that may lurk in organizations. Some knowledge of digital forensics will be helpful, although not required, for this course. This course may include a live demonstration. This course will benefit technical staff, information security staff, and implementers of regulatory compliance measures in particular. Senior and top management will also gain important insights from this course.

Approximate Training Time: 4 – 5 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Business Continuity Planning

Brief Description: The training course provides students with an understanding of business continuity planning that they can take back to their organizations. The course covers important regulatory and implementation aspects of business continuity planning. Students will learn what goes into strategizing, designing, creating, implementing, and testing a robust and successful business continuity plan. Students will also learn the distinction between a business continuity plan and a disaster recovery plan. This course is specifically directed at technical staff, information security staff, implementers of regulatory compliance, business continuity planning teams, senior management and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Vulnerability Assessment

Brief Description: The training course guides students on the advantages and strengths of vulnerability assessment and how it can be effectively used to fortify and organization's information security defenses. The course will touch upon various tools and techniques for vulnerability assessment, strategic planning, effectively performing vulnerability assessments, and how to use results for improving the information security defenses of an organization. While large portions of the course will be technical in nature, non-technical students may attend if interested. This course will benefit technical staff, information security staff, and implementers of regulatory compliance. Senior and top management will benefit too in gaining an understanding of what goes behind a successful vulnerability assessment and how it can be a useful tool for organizations.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Digital Forensics

Brief Description: The training course helps students gain the necessary understanding and training on digital forensic methods. Digital forensics is an important tool for security incident response and security breach investigation. This course will teach students the investigation methodology, evidence acquisition method, evidence preservation, evidence analysis, evidence examination, as well as data recovery and reporting. This course will conclude with a live demonstration and case study of a digital forensic investigation. The live demonstration of this course will be very technical in nature. The theoretical sections of the course, while technical, will be explained in non-technical terms as well to encourage more inclusion of non-technical audiences who can benefit from the course. This course will benefit technical staff, information security staff, and implementers of regulatory compliance. Senior and top management are highly encouraged to attend, as are non-technical employees who have an interest in digital forensics and wish to learn.

Approximate Training Time: 3 – 4 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Web Application Security and Ethical Hacking

Brief Description: The training course will teach the concepts of web application security. The course will delve into methods, techniques, and tips for securing web-based applications and the typical flaws that come about with them. Ethical hacking concepts will then be discussed in order to use it as an effective tool to integrate security into web-based applications. The course will be technical in nature and will mainly benefit technical staff, information security staff, and implementers of regulatory compliance. Non-technical employees with an interest are encouraged to attend. Senior and top management can gain useful insights by attending and are also encouraged to attend.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Web Application Hacking Live Demonstration

Brief Description: The training course is a great supplement to the Web Application Security and Ethical Hacking course. This course provides a more practical and demonstrative perspective on web application hacking and the tools and techniques used by hackers. The course will provide students with a more practical understanding of how to minimize critical web application security problems. The live demonstration will show students how application hacking techniques can be used to secure organizational web applications and also demonstrate how hackers exploit common vulnerabilities affecting systems such as e-commerce websites, online banking systems, shopping carts, etc. The course shall be highly technical in nature. Non-technical audiences may attend if interested, but might require more effort to follow and benefit from the course. The course will be most beneficial to technical staff and information security staff. Senior and top management may attend to gain an idea of how hackers attack organizations. While they may not follow the technical aspects of the course, it will be helpful in putting things into perspective.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Mobile Device Security

Brief Description: The training course provides students with an understanding of the very real emerging threat of mobile device security. Organizations are increasingly dependent on mobile devices either directly or indirectly, and it has become difficult to ignore the security issues that have accompanied these devices. The capabilities and flexibilities provided by mobile devices such as cellular phones, laptop computers, Personal Digital Assistants (PDAs), portable storage devices, and several other such gizmos have also brought along new entry routes for hackers to penetrate organizations. This course helps students learn how to protect organizational mobile devices by understanding the common threats that affect them and the countermeasures available to minimize the risk of physical loss/theft as well as logical information compromise. Students will also gain tips and advice on how to use mobile devices in public areas, on the move, or about town in a secure manner. Overall, students will learn the smart approach to manage risks associated with mobile resources assigned to employees. Employees from all departments are encouraged to attend, as are senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Viruses and Malware

Brief Description: The training course aims to teach students the basics of viruses and malware. The course will describe the ever-changing landscape of viruses, malware, and malicious code and how this affects organizations and productivity. The course will also delve into techniques and tips on how employees across the spectrum can improve their organization's resistance to viruses and malware. Students will develop a more cautious and responsible attitude towards viruses and malware as a result of this course. This is a basic course aimed at generating awareness. Employees from all departments are encouraged to attend, as are senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Pandemic Flu Awareness and Prevention

Brief Description: The training course aims to generate awareness of the very real threat posed by pandemic flu and outbreaks. Some regulations now require that employees be trained and made aware of pandemic flu and how to prevent its proliferation. The course explains the necessary steps to ensure that the effects of a pandemic outbreak on normal organizational operations are minimized. The course also teaches the important elements that go behind creating a successful pandemic prevention program and how an organization should prepare, respond, and recover in the event of a pandemic. Regulatory compliance implementers will gain the most from this course. Employees from all departments are also highly encouraged to attend, as are senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Identity Theft and Risk Assessments

Brief Description: The training course delves into the real and emerging threat of identity theft and how it affects organizations today. Students will be able to identify and conquer their concerns about identity theft by gaining the insight and information needed to address the looming problem. Students will learn about the most vulnerable aspects of most organizations, and how risk assessments can be used as an effective tool to not only plug the security holes but also help avoid financial disaster for organizations and their customers. The course also discusses identity theft regulations that have come to the fore under the Fair and Accurate Credit Transactions Act (FACTA). Students will gain an overview of the FACTA and learn about the components of a compliant Identity Theft Prevention Program. Students will also learn about the critical components to combat identity theft, including employee training, policies and procedures, service provider oversight, and enforcement. Regulatory compliance implementers will gain the most from this course. Employees from all departments are also highly encouraged to attend, as are senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

PCI DSS Compliance

Brief Description: The training course is focused on the Payment Card Industry Data Security Standard (PCI DSS). Students will gain an overview of the PCI DSS and what it entails. Students will be able to identify what it takes to be compliant with the requirements set forth by the PCI DSS. The PCI DSS imposes rigorous and often complicated data security standards on anyone who accepts, stores, and/or processes credit cards and payments. Organizations must comply with these complicated data security standards or risk revocation of their card-processing privileges at best, or heavy fines from credit card companies at worst. This course will serve as a great guide to students on the PCI DSS and will enable students to help their organization comply with the standard. Regulatory compliance implementers will gain the most from this course. Employees from all departments are also highly encouraged to attend, as are senior and top management.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

E-Discovery

Brief Description: The training course helps students understand Electronic Discovery (EDiscovery) and what it entails. The course will discuss the amendments to the U.S. Federal rules of civil procedures regarding E-Discovery and examine the requirements for retrieval, production, and preservation of electronic evidence. The course will also explore guidelines for submitting subpoenas to third parties, the business challenges of e-discovery, and the consequences of noncompliance. It is important to note that Enterprise Risk Management, Inc. is not a legal expert and that all information provided as a part of this course is focused on technical and business strategy aspects related to e-discovery. Regulatory compliance implementers will gain the most from this course. Senior and top management are highly encouraged to attend.

Approximate Training Time: 2 – 3 hours depending on student involvement and interaction.

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

Webinars

Brief Description: All training courses mentioned and described above are provided by Enterprise Risk Management, Inc. as webinars as well in order to offer flexibility in terms of time and location.

Approximate Training Time: Same as the individual training course time.

Location: Since the training course will be offered online as a webinar, this is available at practically any location where a student can connect a basic computer to an Internet connection. Due to the web-based nature of this training, no additional reimbursements for expenses are involved.

Class Size: Any number of students can access the webinar as it is online in nature.

CISSP Examination Preparation Class

Brief Description: The training course helps students preparing for the Certified Information Systems Security Professional (CISSP) certification examination. The CISSP is one of the most coveted and sought-after certifications in the information security industry. CISSP certified professionals are able to lift their professional careers to the next level and their organizations benefit heavily from the expertise and knowledge of their CISSP employees. Students of this training course will be guided through an interactive week of sessions that will cover every area of the CISSP examination and provide tips, case studies, and guidelines that will equip students to take the examination with confidence. The training course will cover the following key examination areas –

- Access Control Systems and Methodology
- Applications and Systems Development
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Law, Investigation, and Ethics
- Computer Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Network Security

All employees preparing to take the CISSP certification examination will greatly benefit from this course.

Approximate Training Time: 5 days of training sessions with 8 hours of training per day (plus a 1 hour break for lunch).

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

ISO 27000 Audit Training

Brief Description: The ISO 27001 Internal Auditor Course will help delegates comprehend and develop the skills necessary to perform internal audits as mandated by the requirements of the ISO Standard. Upon successful

completion the delegates will be prepared to carry out the internal audit necessary for the organization to comply with ISO 27001 requirements. During training, candidates will learn how to initiate, prepare, conduct and finalize an audit. The course will include guidance from the ISO 19011: 2002 Guidelines for quality and/or environmental management systems auditing. In addition, through the use of case studies, the course delegates will be taught overall principles of auditing and learn the details and rationale behind ISO 27001 requirements. Delegates will receive; Course Outline and Notes (consisting of copies of the instructors slides), Case Studies and accompanying exercises, and copies of the ISO 27001 and the ISO 19011 standards. The course instructor will provide the delegates with an evaluation based upon participation and comprehension determined through the case study exercises. The course will consist of instructor's presentations, classroom discussions, case study reviews and associated exercises. Approximately 50% of the course involves practical activities. The final exercise for delegates is drafting an actual audit report based upon a case study.

Approximate Training Time: 3 days of training sessions with 8 hours of training per day (plus a 1 hour break for lunch).

Location: This course is available at the customer location, within any city in the United States of America and any other city worldwide. Additional reimbursements will be charged for travel, expenses, and any other incidentals.

Class Size: Maximum of twelve (12) students per session. No minimum requirement.

ISO 27000 Implementation Training

Brief Description: The ISO 27001 implementation course gives corporate and institutional information security professionals the knowledge to implement and maintain an ISO 27001 compliant Information Security Management System. Delegates will receive practical knowledge for defining, implementing and maintaining an ISMS in accordance with ISO 27001 requirements and the ISO 27002 guidelines. During training, candidates will learn how to initiate, define, implement and maintain an ISO 27001 compliant ISMS. The course will include guidance from the ISO 27002 Code of Practice (best practice guide to the application of information security controls) In addition, through the use of case studies, the course delegates will be given practical instruction on:

- ISMS definition
- Defining Information Security policies

Courses

SIN(s) PROPOSED	Course #	Course Title	Course Length	Minimum Participants	Maximum Participants	PRICE OFFERED TO GSA	QUANTITY/VOLUME DISCOUNT
132-50	100	Information Security	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	110	Data Privacy	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	120	Regulatory Compliance and Information Security	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	130	Network Security and Ethical Hacking	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	140	Ethical Hacking Live Demonstration	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	150	Social Engineering	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	160	Security Breaches and Investigation	4 to 5 Hours	1	12	\$11,339	2% for orders over \$100,000
132-50	170	Business Continuity Planning	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	180	Vulnerability Assessment	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	190	Digital Forensics	3 to 4 Hours	1	12	\$10,205	2% for orders over \$100,000
132-50	200	Web Application Security and Ethical Hacking	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	210	Web Application Hacking Live Demonstration	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	220	Mobile Device Security	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	230	Viruses and Malware	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	240	Pandemic Flu Awareness and Prevention	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	250	Identity Theft and Risk Assessments	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000

132-50	260	PCI DSS Compliance	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	270	E-Discovery	2 to 3 Hours	1	12	\$9,071	2% for orders over \$100,000
132-50	300	CISSP Examination Preparation Class (8hrs per day - 5 days per week)	5 Days	2	12	\$36,286	2% for orders over \$100,000
132-50	300	CISSP Examination Preparation Class (8hrs per day - 5 days per week)	5 Days	1	1	\$3,024	2% for orders over \$100,000
132-50	400-1	ISO 27000 Audit Training	3 Days	1	12	\$36,145	2% for orders over \$100,000
132-50	400-2	ISO 27000 Implementation Training	3 Days	1	12	\$36,145	2% for orders over \$100,000

Webinars

SIN(s) PROPOSED	Course #	Course Title	Course Length	Minimum Participants	Maximum Participants	PRICE OFFERED TO GSA (including IFF)	QUANTITY/VOLUME DISCOUNT
132-50	100	Information Security	2 to 3 Hours	1	TBD	\$2,251	2% for orders over \$100,000
132-50	110	Data Privacy	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	120	Regulatory Compliance and Information Security	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	130	Network Security and Ethical Hacking	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	140	Ethical Hacking Live Demonstration	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	150	Social Engineering	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000

132-50	160	Security Breaches and Investigation	4 to 5 Hours	1	TBD	\$2,814	2% for orders over \$100,000
132-50	170	Business Continuity Planning	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	180	Vulnerability Assessment	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	190	Digital Forensics	3 to 4 Hours	1	TBD	\$2,532	2% for orders over \$100,000
132-50	200	Web Application Security and Ethical Hacking	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	210	Web Application Hacking Live Demonstration	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	220	Mobile Device Security	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	230	Viruses and Malware	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	240	Pandemic Flu Awareness and Prevention	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	250	Identity Theft and Risk Assessments	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	260	PCI DSS Compliance	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000
132-50	270	E-Discovery	2 to 3 Hours	1	TBD	\$2,701	2% for orders over \$100,000

All 100 & 200 level courses provide a minimum of 3 hours training designed to provide an overview of the subject matter referenced in the Course Title. In-depth training with a specific focus on a particular organization or subject matter can be designed to fit the client need. Development costs for specifically designed training will be quoted based on the hourly rates presented for SIN 132-51 shown above.

**TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT)
PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51)**

1. SCOPE

- a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.
- b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

- a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.
- b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
- c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

- a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
- b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. PERFORMANCE OF SERVICES

- a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
- b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
- c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
- d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

- (a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-
- (1) Cancel the stop-work order; or
 - (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
- (b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-
- (1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
 - (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.
- (c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
- (d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. INSPECTION OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS --COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I - OCT 2008) (DEVIATION I - FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

7. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data - General, may apply.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9. INDEPENDENT CONTRACTOR

All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

- b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

- (a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

- (1) The offeror;
- (2) Subcontractors; and/or
- (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

Please refer to the sections of this document that follow.

LABOR CATEGORY DESCRIPTIONS (SIN 132-51)

IT Security / Assurance Functional Senior Consultant

Knowledge and Experience

- A minimum of nine (9) years of direct professional experience and subject matter expertise in one or more service line: information security, risk management, digital forensics, information technology (IT) audits, regulatory compliance, and/or attestation services.
- Comprehensive knowledge and wealth of professional experience in information security, risk management, digital forensics, information technology (IT) audits, regulatory compliance, and/or attestation services.

Duties and Functional Responsibilities

- Work as project team members and oversee allocated aspects of projects.
- Prepares project plan and provide projects technical quality control
- Oversee, mentor, and work with subordinate team members on projects.

Education and Qualifications

- Master's Degree in Computer Science, Information Systems, Information Security, Engineering, or a related, highly specific technical field.
- Multiple reputed, industry-specific certifications including (but not limited to) the following –
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Information Systems Manager (CISM)
 - Certified Information Technology Professional (CITP)
 - Certified Public Accountant (CPA)
 - GIAC Security Essentials Certification (GSEC)
 - GIAC Systems and Network Auditor (GSNA)
 - Microsoft Certified Professional (MCP)
 - Certified Wireless Network Administrator (CWNA)
 - Payment Card Industry Qualified Security Assessor (PCI QSA)
 - Payment Application Qualified Security Assessor (PA QSA)
 - Payment Card Industry Approved Scanning Vendor (PCI ASV)
 - ISO 27001:2005 ISMS Lead Auditor
 - ISO 27001:2005 ISMS Lead Implementer
- Required to demonstrate continuous improvement and contribution in various knowledge domains via industry articles, presentations, seminars, training programs, and other active involvements both in industry and academia.

IT Security / Assurance Functional Consultant

Knowledge and Experience

- A minimum of six (6) years of direct professional experience and subject matter expertise in one or more service line: information security, risk management, digital forensics, information technology (IT) audits, regulatory compliance, and/or attestation services.
- Extensive knowledge and professional experience in information security, risk management, digital forensics, information technology (IT) audits, regulatory compliance, and/or attestation services.

Duties and Functional Responsibilities

- Work as project team members and oversee allocated aspects of projects.
- Prepares project plan and provide projects technical quality control
- Oversee, mentor, and work with subordinate team members on projects.

Education and Qualifications

- Master's Degree in Computer Science, Information Systems, Information Security, Engineering, or a related, highly specific technical field.
- Multiple reputed, industry-specific certifications including (but not limited to) the following –
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Information Systems Manager (CISM)
 - Certified Information Technology Professional (CITP)
 - Certified Public Accountant (CPA)
 - GIAC Security Essentials Certification (GSEC)
 - GIAC Systems and Network Auditor (GSNA)
 - Microsoft Certified Professional (MCP)
 - Certified Wireless Network Administrator (CWNA)
 - Payment Card Industry Qualified Security Assessor (PCI QSA)
 - Payment Application Qualified Security Assessor (PA QSA)
 - Payment Card Industry Approved Scanning Vendor (PCI ASV)
 - ISO 27001:2005 ISMS Lead Auditor
 - ISO 27001:2005 ISMS Lead Implementer
- Required to demonstrate continuous improvement and contribution in various knowledge domains via industry articles, presentations, seminars, training programs, and other active involvements both in industry and academia.

IT Security / Assurance Project Team Leader

Knowledge and Experience

- A minimum of four (4) years of direct professional experience and subject matter expertise in one or more service line: information security, risk management, digital forensics, information technology (IT) audits, regulatory compliance, and/or attestation services.
- Substantial knowledge and professional experience in information security, risk management, digital forensics, information technology (IT) audits, regulatory compliance, and/or attestation services.

Duties and Functional Responsibilities

- Work as project team members under the supervision of senior team members.
- Perform implementation-level tasks on projects under the direction and guidance of senior team members.

Education and Qualifications

- Master's Degree in Computer Science, Information Systems, Information Security, Engineering, or a related, highly specific technical field.
- At least one, industry-specific certification including (but not limited to) the following –
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Information Systems Manager (CISM)
 - Certified Information Technology Professional (CITP)
 - Certified Public Accountant (CPA)
 - GIAC Security Essentials Certification (GSEC)
 - GIAC Systems and Network Auditor (GSNA)
 - Microsoft Certified Professional (MCP)
 - Certified Wireless Network Administrator (CWNA)
 - Payment Card Industry Qualified Security Assessor (PCI QSA)
 - Payment Application Qualified Security Assessor (PA QSA)
 - Payment Card Industry Approved Scanning Vendor (PCI ASV)
 - ISO 27001:2005 ISMS Lead Auditor
 - ISO 27001:2005 ISMS Lead Implementer

- Required to demonstrate continuous improvement and contribution in various knowledge domains via industry articles, presentations, seminars, training programs, and other active involvements both in industry and academia.

GSA Approved Labor Categories

SIN	GSA SERVICE PROPOSED (e.g. Labor Category/Task)	UNIT OF ISSUE (e.g. Hour, Task, or Sq ft)	Proposed GSA Rate w/ IFF
132-51	IT Security/Assurance Functional Senior Consultant	Hour	\$181.36
132-51	IT Security/Assurance Functional Consultant	Hour	\$163.22
132-51	IT Security/Assurance Project Team Leader	Hour	\$145.09