INSTITUTE OF FORENSIC SCIENCE
GUJARAT FORENSIC SCIENCES UNIVERSITY

IFS-GFSU CERTIFIED

INFORMATION SECURITY PROFESSIONAL

ISP

IFS-GFSU Certification #14001 Information Security Professional

An objective of the Indian National Cyber Security Policy – 2013:

To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

DATES FOR 2014 EXAMS

The exam for the IFS-GFSU Certification *#14001 Information Security Professional* will be conducted on the following dates in 2014:

Sunday 19th January, 2014
Sunday 20th April, 2014
Sunday 20th July, 2014
Sunday 19th October, 2014

Registration for the exam closes 30 days prior to the exam date.

SUMMARY OF EXAM INFORMATION

Exam Duration: **3 hours**
Passing Marks: **70%**

One-time registration fees: **Rs 1,000**

Exam Fees: **Rs 4,500** for students
Exam Fees: **Rs 10,000** for others

ABOUT IFS-GFSU

This certification is provided by Institute of Forensic Science, Gujarat Forensic Sciences University (IFS-GFSU). The Government of Gujarat, under the flagship of the Home Department of the Government of Gujarat, has established GFSU. GFSU is the only university across the world, dedicated to Forensic & Investigative Science.

ABOUT THIS DOCUMENT

This document is issued in pursuance of the IFS-GFSU Certification Policy.

This document is issued as a guide to candidates pursuing an IFS-GFSU certification. IFS-GFSU does not make any representations or warranties that the use of this document will assure candidates of passing any IFS-GFSU certification.

Gujarat Forensic Sciences University
DFS Head Quarters, Sector 18-A,
Near Police Bhavan,
Gandhinagar-382007,
Gujarat - India

Quick Guide to Earning & maintaining your IFS-GFSU certification

1	Obtain your one-time Permanent Registration Number.
2	Apply for the examination.
3	Prepare for the exam by studying the reference material comprising the IFS-GFSU Common Body of Knowledge for Information Security (CBOKIS).
4	Appear for the certification exam and obtain 70% in each section.
5	Earn your certification. Earn the right to use **ISP**. Get upgraded to **ISP+** after 6 years.
6	Earn 120 Continuing Education Units (CEUs) every 3 years and submit proof of the same.

Table of Contents

A. Benefits of IFS-GFSU Certifications

A1. Benefits to individuals

- ✓ Achieve a higher position, raise, and promotion faster[1]
- ✓ Become more employable[2]
- ✓ Affirm your professional expertise[3]
- ✓ Increase job security
- ✓ Demonstrate that you possess essential domain knowledge
- ✓ Boost relevance by staying current in the profession with continuing education requirements.
- ✓ Advance your career potential due to recognition as a certified professional
- ✓ Recognition of professional competence by professional peers and management
- ✓ Increase your value and income
- ✓ Keep up with ever-changing standards and technologies
- ✓ Validate your knowledge
- ✓ Differentiate yourself from your peers
- ✓ Boost your confidence
- ✓ Show that you know the most current principles and practices of your field
- ✓ Personal satisfaction of accomplishing a milestone in your career
- ✓ Stand out against other applicants in a tough job market.
- ✓ Get prepared for greater on-the-job responsibilities
- ✓ Potentially earn higher income for being formally recognized as a certified professional
- ✓ Demonstrate Your Commitment
- ✓ Build and enhance your credibility
- ✓ Build & Showcase Your Skills
- ✓ Become more marketable when you compete for top positions
- ✓ Raise your prestige among your staff and your peers
- ✓ Improve overall performance, remove uncertainty and widen market opportunities
- ✓ Ensure you are continually improving and refining your activities
- ✓ Become part of a professional network
- ✓ Enjoy better career flexibility
- ✓ Be recognized as being knowledgeable and skilled
- ✓ Open the doors of opportunity; enhance your career

[1] Salary surveys show that the majority of hiring managers consider certifications a factor in hiring decisions, and that obtaining relevant certifications often leads to a salary increase.

[2] According to an IDC white paper, "63% of hiring managers believe certified individuals are more productive than their non-certified counterparts."

[3] Your employer, clients, employees and peers will recognize your GFSU credential as an indication of the skills and knowledge you've gained through certification.

A2. Benefits to organizations

- ✓ **Benchmark**
  With GFSU certifications, your organization will have a benchmark to compensate, measure and evaluate employees' skills for roles within the organization. GFSU certifications also provide a recognized benchmark of skills that can be aligned to organisational skills frameworks.

- ✓ **Consistency**
  With GFSU certifications, your teams are trained to consistent skill levels.

- ✓ **Staff motivation**
  The regular assessment process will improve staff responsibility, commitment and motivation and ensure competent employees.

- ✓ **Increased Productivity**
  GFSU certified professionals are typically more productive and work to consistent standards.

- ✓ **Assurance**
  GFSU certifications assure that the certified professional has the knowledge and skills needed to perform the allotted tasks.

- ✓ **Performance-related pay**
  Gaining GFSU certifications can be aligned to performance-related pay.

- ✓ **Customer satisfaction**
  GFSU certifications can ensure greater customer satisfaction (internal and external customers).

- ✓ **Employee satisfaction**
  GFSU certifications provide professional development, advancement and recognition opportunities for staff. This can also lead to lower staff turnover.

- ✓ **Higher quality**
  GFSU certifications lead to more reliable, higher quality results produced with increased efficiency and consistency by professionals who use industry standard techniques.

- ✓ **Culture of learning**
  GFSU certifications empower a culture of learning and improvement that increases return on investment.

- ✓ **Increased credibility**
  GFSU certifications demonstrate to customers, competitors, suppliers, staff and investors that you use industry-standard practices.

- ✓ **Stakeholder satisfaction**
  GFSU certifications demonstrate to your stakeholders that your business is run effectively.

B. About the Certification

B1. Importance of Information Security

An Information Security Professional is skilled in understanding and analyzing information security threats and implementing best practices for Information Security. The importance of Information Security can be understood from the following extract from the *Indian National Cyber Security Policy – 2013*:

> Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors.
>
> Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures.
>
> A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets.
>
> Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity.
>
> Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering , hactivism , cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc.
>
> The protection of information infrastructure and preservation of the confidentiality, integrity and availability of the information in cyberspace is the essence of a secure cyber space.

B2. Required competence

To earn this certification, candidates must take the certification exam and obtain a minimum of 70% marks.

B3. Abilities

Candidate's vision, hearing, mobility and other abilities must be such that would permit him to work efficiently in information security in an organizational environment.

B4. Prerequisites

The candidate must be a graduate in any stream from a recognized University.

B5. Code of Professional Ethics

All IFS-GFSU certified professionals should:

1. Encourage implementation of measures for control of corporate crime.
2. Perform duties to the best of their knowledge, skills and capabilities.
3. Maintain high standards of moral character.
4. Preserve the privacy and confidentiality of information obtained in the course of professional assignments, subject to regulatory requirements.
5. Ensure compliance with regulatory and legal framework.

Failure to comply with this Code of Professional Ethics may result in suspension and subsequent withdrawal of certification.

B6. Criteria for initial certification

1. Demonstrating mastery of IFS-GFSU Common Body of Knowledge for Information Security by successfully taking the certification exam with a score of at least 70%.

2. Being a graduate in any stream from a recognized University. Students pursuing graduation may appear for the certification exam and on successfully passing the exam will be issued a provisional certificate. Such applicants will be certified on submitting proof of graduation.

3. Accepting the IFS-GFSU Code of Professional Ethics.

B7. Criteria for renewal of certification

1. Earn 120 CEUs (Continuing Education Units) every 3 years.
2. Submit documentary evidence in respect of CEUs earned.
3. Submit administrative fee of Rs. 2,000 plus applicable taxes (every 3 years).
4. Compliance with IFS-GFSU Code of Professional Ethics.

B8. Grounds for suspending and withdrawing certification

The Certification Management Committee, Institute of Forensic Science, Gujarat Forensic Sciences University (IFS-GFSU) may suspend and withdraw a certification for any of the following reasons:

1. Violation of the terms of any undertaking made to IFS-GFSU.
2. Failure to obtain the required CEUs (Continuing Education Units) every 3 years.
3. Failure to submit documentary evidence every 3 years of CEUs earned along with the applicable administrative fee.
4. Violating any provision of the IFS-GFSU Code of Professional Ethics.
5. Providing any false information to IFS-GFSU.

B9. Exam Overview

The Information Security Professional (ISP) certification from Institute of Forensic Science, Gujarat Forensic Sciences University (IFS-GFSU) proves specialist level expertise in information security. An *IFS-GFSU Certified Information Security Professional* is skilled in understanding and analyzing information security threats and implementing best practices for Information Security.

B10. Development of the exam

The Certification Management Committee of IFS-GFSU is responsible for operational policies and procedures, implementation of the policies and procedures, resources for certification activities (personnel, outsourcing, premises, including examination sites, equipment and resources for carrying out certification activities), assessment activities, decisions on certification, including the granting, maintaining, recertifying, expanding, reducing, suspending or withdrawing of the certification, contractual arrangements. The Certification Development Committee of IFS-GFSU is responsible for development and maintenance of the certification schemes. Subject Matter Experts come under the Certification Development Committee.

B11. Subject Matter Experts

Subject Matter Experts for certification programs conducted by Institute of Forensic Science, Gujarat Forensic Sciences University advise in the development and review of the certification scheme[4]. The Subject Matter Experts for *IFS-GFSU Certification #14001 Information Security Professional* are (in alphabetical order):

Jimmy Mate, Assistant Manager, EY

With over 7 years of experience in Forensic Technology, he currently holds the position of Assistant Manager with a Big4. His expertise covers Digital Forensic Data Analysis, Computer Forensics, Fraud Investigations along with evaluating design & operating efficiencies of internal controls at the entity & process level and identifying areas of improvement & cost savings. He has addressed various sectors like Cement Manufacturing, Apparels & Footwear, Pharmaceutical, Information Technology, Automotive, Micro Finance, Consumer Electronic manufacturing, Media & Entertainment, Hospitality, Business & Technology Services, Insurance and Steel Manufacturing. He has also worked on designing & execution of training modules in the area of Forensic Technology for Government Organizations & Corporates.

M Lingesh, Information Security Manager, ISO 27001 Lead Auditor, CISA, CPP, CFE

M Lingesh is a retired Naval Officer with 20 years of military experience. He has been working in the Information Security field for around 7 years.

Nishant Mohorikar, Head of Security Operations Center

He is a CISSP and GREM with 12+ years of experience in the domain of Information Security Consulting and establishing Security Operations Centre. He has played a key role in establishing and managing Security Operations Centre in Chennai, directing and executing Application Security Code Audits, Penetration Testing and Wireless Security assessments. He has managed and directed consulting assignments on compliance requirements like SOX-404.

[4] This includes criteria for initial certification and recertification; curriculum for certification examinations and tests; assessment methods for initial certification and recertification; surveillance methods and criteria (if applicable); criteria for suspending and withdrawing certification; criteria for changing the scope or level of certification (if applicable); submitting questions for inclusion in the certification examinations and tests (optional).

He can effectively manage codes of practice, which include CoBIT, SSE-CMM, PCI-DSS, ISO 27001, OWASP, ISSAF, NIST, ISF, OSSTM, CLASP. He has security expertise at both the strategic and hands on levels to provide the ability to strengthen enterprise risk exposure through best practice planning and pro-active solution implementation. He has expertise in designing Information Systems Security policy and procedures, secure coding practices and designing application architecture.

He has directly managed and executed Sarbanes-Oxley IT compliance projects for Fortune 500 clients and has directly managed vulnerability assessments, penetration testing, application security audits for Fortune 100 clients. He has played a key role in setting up Computer Emergency Response Team for Government of India.

Olivier Ruch-Rosanoff, CISSP, CISM, CRISC, ISO 27001 LA

He is a technology related risk, control and information security management professional with broad expertise in the IT/IS business risk and security domains, taking advantages of over fifteen years experience in areas such as Financial Services, Individual / Family Office, Maritime / Shipping Services and Medical / Health Care industries. Specialties: Governance Framework, Control Environment, Compliance, Risk and Security Management, Project and Change Management, Operations, Service Management, Business Continuity.

R Vittal Raj FCA, CISA, CGEIT, CISM, CRISC, CISSP, CIA, CFE

He has 25+ years of experience in directing, managing projects in Information Security, IS Audit, IT Governance.

Ram Gopal Soni, Associate VP - Security Consulting, ControlCase International Pvt. Ltd.

Ram Gopal Soni is an Information Security Graduate with strong cognition and industry experience in Information Security Implementation, Assessment, Audit and Information Security Management. He is working as QSA / Associate VP - Security Consulting with ControlCase International Pvt. Ltd and is currently focused on Information Security Compliance Audit and Certification including PCI-DSS, PA-DSS and Computer Forensics, Fraud Investigation and Risk Assessment. He is also involved in execution and management of Technical Risk Assessment including Application Security, Penetration Testing and business development activities.

Ravindranath Patil, Associate Director, Risk Consulting, KPMG

He is a former IPS officer having over 9 years of experience in cyber and fraud investigation pertaining to industries such as Infrastructure, Liquor, FMCG, Telecommunication, IT, Engineering Goods, Automobile and Micro Finance. He has worked as an Assistant Director General of Foreign Trade, Ministry of Commerce, Government of India. He is a visiting faculty on cyber crime investigation at National Police Academy, National Academy of Direct Taxes and the Centre for Police Research. He is a research fellow of Centre for Police Research on "Mobile Technology".

Rishi Mehta, Sr. Vice President, Head IT Governance & Chief Information Security Officer, Religare Enterprises Limited

He is a technology manager with a commercial flair, to enable business processes while managing risk. With over 13 years of experience in the technology industry with exposure of leading diverse functions such as IT Sales, Large Program Delivery, Six Sigma Quality, Information Security, Operations, IT Risk Management, Governance & Operational Risk. He inspires employees to peak performance, balance controls with risk and cultivate profitable business relationships.

Dr. Seema Verma, Associate Professor, Banasthali Vidyapith

Dr. Verma has been working as an academician and researcher for 13 years. Currently she is a researcher in wireless networks and security. She has published many papers in refereed international journals and at reputed international conferences. She has produced 4 PhDs and is heading 3 major projects from University Grants Commission.

Sethu S Raman, Vice President & Chief Risk Officer, MphasiS an HP Company

Sethu S Raman is an ex-defence officer presently working as the Chief Risk Officer with an MNC IT services company. He is a senior risk management professional with a strong academic background (MBA, BAL [law], CRMA, CPP,CBCP,CISA, CISSP) and 21 years of versatile experience in managing risk in its 'manifold manifestation' especially in Banking and IT industries.

Sunil Bakshi MCA, CISA, CISM, CGEIT, CRISC, CISSP, PMP, CEH, AMIIB, ABCI, ISO 27001 LA, BS25999 LI

He had been working with State Bank of India for 25 years as IT Manager. He also worked as Manager in Enterprise Risk Services group of Deloitte Touché Tohmatsu India Private Limited, Mumbai and as Senior Manager in Wipro consulting services. Sunil was CISO of National Stock Exchange. Currently he is a free-lance consultant and trainer in IT governance and Information Security. He is a Senior Member of the Computer Society of India and was the Chairman of its Pune chapter.

He is also a member of ISACA and was president of its Pune chapter. He was a member of the International Membership board of ISACA, USA and CISM and CRISC Test Enhancement committee of ISACA. Currently he is working on CRISC Certification committee of ISACA International and part of QA team of CISA and CISM technical review manuals. Sunil is also member of Association of Technical Scholarships (AOTS), Japan. Sunil has written a number of articles on Information Systems Security and Audit topics in various national and International publications like Information Systems Control Journal of ISACA, USA, CSI Communications of Computer Society of India, etc. Sunil has presented various topics at many national and international conferences organized by ISACA, CSI, ICAI.

Szabolcs Hallai, CISO, CISA, CISM, CITRM, C|CISO

Szabolcs's primary goal as an auditor and/or consultant is to reconcile the everlasting dilemma of an IT/ITSEC being a business based function inside of a non-IT core business entity. By becoming a skilled expert of both worlds - business and information technology he tries to discover control and system errors and to help them correct the best possible way. Working as a team player he never lost his individual skills. Experienced in governmental / multinational / equity / financials / banking environments, multitasking, with high communication skills on senior level and with end-users. Specialities: Expertise on the field of IT Auditing, QA and Consultancy, Risk Management, Policy Compliance, ISO 27001/17799/BS7799, ITIL, COBIT, AML, MiFID, General Internal Audit, Due diligence, IT Security, Legislation compliance, IT governance

Vishal Narula, Associate Director, KPMG

Vishal has a total of over 9 years of experience in Dispute Advisory, Investigations, Fraud Risk Assessments, Risk Consulting and Internal Audit. Vishal is member of the ICC users council in India. He has worked extensively across sectors and has vast experience is a broad spectrum of industries covering infrastructure, ferrous and non ferrous metals, mining, heavy manufacturing, FMCG, financial services, media & entertainment, etc. He has worked across geographies and has gained exposure in 19 countries across the globe.

Vishal Salvi, Chief Information Security Officer - HDFC Bank

As the Head of Information Security for HDFC Bank, he is accountable and responsible for strategy, policy, risk management and information security program management implementation for HDFC Bank. He has earlier been Head OITS at Standard Chartered Bank.

Yogesh Dange, CRISC, CPISI, BCCS, BCCP, ISO 27001, BS 25999, CEH

He has over 20 years of experience spreading across Information Technology services, Information risk management and business continuity in various geographies including Middle East, South East Asia and India. Specialties: Information Risk Management & consulting in Regulatory standards such as PCI DSS, HIPAA Implementation, ISO 27001/ISO 22301/BS 25999 implementation & compliance assessment, Information Security & Technology risk assessments, Business Continuity/DR Planning, Information Security Architecture, IT Strategy, IT governance, Contract compliance, pre-post acquisition IT due diligence.

B12. Type of questions

The examination will consist primarily of Case Study Based (Problem-Based) questions. These questions consist of a practical problem followed by several options. Candidates must apply their knowledge and skills to choose the most appropriate option. IFS-GFSU certifications use this type of questions as they allow candidates to demonstrate their practical understanding of the topic rather than requiring them to memorise information. Such questions focus on testing a candidate's skill development, require thinking and do not focus on purely theoretical knowledge.

B13. Preparation for the Exam

Case Study Based (Problem-Based) questions require candidates to study the reference material thoroughly and ensure understanding of how the information can be applied in real-life practical situations. On registering for the certification exam, you will be provided comprehensive reference material and the IFS-GFSU Guide to the Common Body of Knowledge for Information Security (CBOKIS) in electronic form.

B14. Common Body of Knowledge for Information Security (CBOKIS)

The IFS-GFSU Common Body of Knowledge for Information Security (CBOKIS) establishes a baseline for the body of knowledge for Information Security. CBOKIS is a comprehensive description of the sum of knowledge and professional practices and techniques that are generally accepted within the Information Security profession. CBOKIS is not static and will be constantly evolving as the field of Information Security develops.

B15. Administration of the Exam

Admission Pass

Approximately one week prior to the exam date, registered candidates will be emailed an electronic Admission Pass containing the date, time and exact venue of the examination. You must carry a printout of this Admission Pass along with a Government issued photo-identity card (e.g. PAN card, drivers license, passport, etc.).

Entry to the exam centre

Registered candidates must enter the exam centre 30 minutes prior to the start of the exam. Any candidate who is late will be denied entry to the exam centre and will not be permitted to take the exam. The Exam fees paid by such a candidate will be forfeited.

Special Arrangements

No food or drink is permitted at the exam centre. An exception can be made in case of medical reasons provided the registered candidate shows a doctor's certificate to this effect.

What to carry into the exam centre

Suitable pencils, eraser, sharpener, a printout of your Admission Pass and a valid Government issued photo-identity card.

What NOT to carry into the exam centre

Any reference materials, paper, books, calculator, cell-phone, laptop, tablet, etc. Do not carry any food or drinks unless you have a doctor's certificate proving the need for it.

Malpractice or cheating

The following activities will constitute malpractice and may result in the candidate being debarred from all future exams as well as prosecuted under the law:

1. carrying any reference material into the exam centre;
2. attempting to take the exam for another person;
3. using any reference material;
4. assisting another candidate in attempting the exam;
5. using any communication device;
6. leaving or entering the exam centre without authorization from the Examiner;
7. carrying the question booklet or answer sheets outside the exam centre;
8. disturbing the other candidates during the examination;

B16. Fees

Particulars	**Fee**
One-time Permanent Registration Fee	1,000
Exam Fees (For students pursuing graduation)	4,500
Exam Fees (For others)	10,000

Note:

1. In case a registrant fails the certification exam, he / she will be required to pay 50% of the current Exam Fees for subsequent attempts.

2. No fee refunds will be made to any registrant.

3. On registering for a certification, the registrant shall be provided the list of recommended reference material.

4. No contact lectures or classes shall be provided.

B17. Exam Duration

The certification exam has a length of 3 hours.

B18. Passing Score

To pass, a candidate must obtain a minimum of 70% in each of the sections of the exam.

B19. Dates

Exam date	Registration closes on
Sunday 19th January, 2014	19th December, 2013
Sunday 20th April, 2014	20th March, 2014
Sunday 20th July, 2014	20th June, 2014
Sunday 19th October, 2014	19th September, 2014

B20. Overview of Examination Syllabus

This examination is divided into the following sections:

1. End-point Security
2. Network & Internet Security
3. Information Security Incident Response
4. Regulatory & Standards Compliance
5. Data Protection
6. Information Security Testing
7. Contingency Planning

B21. Detailed Examination Syllabus

1. END-POINT SECURITY

1.1 Desktop and Laptop Security

1.1.1 Desktop & Laptop Security – *Windows, Linux computer, Macintosh*

1.1.2 Security in a BYOD environment

1.2 Cell Phone Security

1.2.1 Cell Phones - *Cellular Communications, Identity Modules, Secure usage*

1.2.2 Software Applications

1.2.3 Threats - *Loss, theft, or disposal, Unauthorized access, Malware, Spam, Electronic eavesdropping, Electronic tracking, Cloning, Server-resident data.*

1.2.4 Safeguards - *User-Oriented Measures, Organizational-Oriented Measures*

1.3 Patch and Vulnerability Management

1.3.1 Importance of Patch Management, Zero day threats, Early Warning Systems

1.3.2 Challenges of Patch Management - *Timing, Prioritization and Testing, Patch Management Configuration, Alternative Host Architectures, Software Inventory Management, Resource Overload, Installation Side Effects, Patch Implementation Verification, Application Whitelisting*

1.3.3 Enterprise Patch Management Technologies - *Components and Architecture (Agent-Based, Agentless Scanning, Passive Network Monitoring), Security Capabilities (Inventory Management Capabilities, Patch Management Capabilities, Antivirus, Configuration management, Vulnerability scanning)*

1.4 Password Management

1.4.1 Understanding Passwords and Password Management

1.4.2 Mitigating Threats Against Passwords- *Password Capturing (Storage, Transmission, User Knowledge and Behaviour), Password Guessing and Cracking (Guessing, Cracking, Password Strength, User Password Selection, Local Administrator Password Selection), Password Replacing (Forgotten Password Recovery and Resets, Access to Stored Account Information and Passwords, Social Engineering), Using Compromised Passwords*

1.4.3 Password Management Solutions - *Single Sign-On Technology, Password Synchronization, Local Password Management*

1.5 Security for Full Virtualization Technologies

1.5.1 Understanding Virtualization - *Virtualized Networking, Virtualized Storage, Guest OS Images, Server Virtualization, Desktop Virtualization*

1.5.2 Virtualization Security - *Guest OS Isolation, Guest OS Monitoring, Image and Snapshot Management, Hypervisor Security, Guest OS Security, Virtualized Infrastructure Security, Desktop Virtualization Security*

1.5.3 Secure Virtualization Planning and Deployment

1.6 Media Sanitization

1.6.1 Understanding Media Sanitization - *types of media, trends in data storage media, trends in sanitization, types of sanitization, use of cryptography and cryptographic erase, factors influencing sanitization and disposal decisions, sanitization scope*

1.6.2 Information Sanitization and Disposition Decision Making - *information decisions in the system life cycle, determination of security categorization, reuse of media, control of media, data protection level, sanitization and disposal decision, verify methods, documentation*

1.6.3 Data Leakage Prevention

2. NETWORK & INTERNET SECURITY

2.1 Intrusion Detection & Prevention systems

2.1.1 Intrusion Detection and Prevention Principles - *Uses of IDPS Technologies, Key Functions of IDPS Technologies, Common Detection Methodologies, Signature-Based Detection, Anomaly-Based Detection, Stateful Protocol Analysis, Types of IDPS Technologies*

2.1.2 IDPS Technologies - *Components and Architecture (Typical Components, Network Architectures), Security Capabilities (Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities)*

2.1.3 Management - *Implementation, Operation and Maintenance, Building and Maintaining Skills*

2.1.4 Network-Based IDPS - *Networking Overview (Application Layer, Transport Layer, Network Layer, Hardware Layer), Components and Architecture (Typical Components, Network Architectures and Sensor Locations), Security Capabilities (Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities), Management (Implementation, Operation and Maintenance)*

2.1.5 Wireless IDPS - *Wireless Networking Overview (WLAN Standards, WLAN Components, Threats against WLANs), Components and Architecture (Typical Components, Network Architectures, Sensor Locations) Security Capabilities (Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities), Management (Implementation, Operation and Maintenance)*

2.1.6 Network Behaviour Analysis (NBA) System - *Components and Architecture (Typical Components, Network Architectures, Sensor Locations), Security Capabilities (Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities), Management (Implementation, Operation and Maintenance)*

2.1.7 Host-Based IDPS - *Components and Architecture (Typical Components, Network Architectures, Agent Locations, Host Architectures), Security Capabilities (Logging Capabilities, Detection Capabilities, Prevention Capabilities, Other Capabilities), Management (Implementation, Operation)*

2.1.8 *Using and Integrating Multiple IDPS Technologies - The Need for Multiple IDPS Technologies, Integrating Different IDPS Technologies (Direct IDPS Integration, Indirect IDPS Integration), Other Technologies with IDPS Capabilities (Network Forensic Analysis Tool Software, Antivirus Technologies, Firewalls and Routers, Honeypots)*

2.1.9 IDPS Product Selection - *General Requirements (System and Network Environments, Goals and Objectives, Security and Other IT Policies, External Requirements, Resource Constraints), Security Capability Requirements (Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities), Performance Requirements, Management Requirements (Design and Implementation, Operation and Maintenance, Training, Documentation, and Technical Support), Life Cycle Costs, Evaluating Products (IDPS Testing Challenges, Performing IDPS Evaluations)*

2.1.10 Honeypots

2.2 Firewalls and Firewall Policy

2.2.1 Firewall Technologies - *Packet Filtering, Stateful Inspection, Application Firewalls, Application-Proxy Gateways, Dedicated Proxy Servers, Virtual Private Networking, Network Access Control, Unified Threat Management (UTM), Web Application Firewalls, Firewalls for Virtual Infrastructures, Host-Based Firewalls and Personal Firewalls, Personal Firewall Appliances*

2.2.2 Firewalls and Network Architectures - *Network Layouts with Firewalls, Firewalls Acting as Network Address Translators, Architecture with Multiple Layers of Firewalls*

2.2.3 Firewall Policy- *Policies Based on IP Addresses and Protocols (IP Addresses and Other IP Characteristics, IPv6, TCP and UDP, ICMP, IPsec Protocols), Policies Based on Applications, Policies Based on User Identity, Policies Based on Network Activity*

2.2.4 Firewall Planning and Implementation - *Planning, Configuring (Hardware and Software Installation, Policy Configuration, Logging and Alerts Configuration), Testing, Deploying, Managing*

2.3 Computer Security Log Management

2.3.1 Understanding Computer Security Logs - *The Basics of Computer Security Logs (Security Software, Operating Systems, Applications, Usefulness of Logs), The Need for Log Management, The Challenges in Log Management (Log Generation and Storage, Log Protection, Log Analysis)*

2.3.2 Log Management Infrastructure - *Architecture, Functions, Syslog-Based Centralized Logging Software (Syslog Format, Syslog Security), Security Information and Event Management Software, Additional Types of Log Management Software*

2.3.3 Log Management Planning - *Define Roles and Responsibilities, Establish Logging Policies, Ensure that Policies Are Feasible, Design Log Management Infrastructures*

2.3.4 Log Management Operational Processes - *Configure Log Sources (Log Generation, Log Storage and Disposal, Log Security), Analyze Log Data (Understanding of Logs, Prioritizing Log Entries, Comparing System-Level and Infrastructure-Level Analysis), Respond to Identified Events, Manage Long-Term Log Data Storage, Perform Testing and Validation*

2.4 Enterprise Telework and Remote Access Security

2.4.1 Overview of Enterprise Telework and Remote Access Security - *Vulnerabilities, Threats, and Security Controls, Remote Access Methods (Tunnelling, Application Portals, Remote Desktop Access, Direct Application Access)*

2.4.2 Remote Access Solution Security - *Remote Access Server Security, Remote Access Server Placement (Intermediary Remote Access Servers, Endpoint Remote Access Servers), Remote Access Authentication, Authorization, and Access Control (Authentication, Authorization, Access Control for Network Communications, Access Control for Applications), Remote Access Client Software Security*

2.4.3 Telework Client Device Security - *Securing Telework PCs, Securing Telework Consumer Devices, Protecting Data on Telework Client Devices (Encrypting Data at Rest, Using Virtual Machines, Backing Up Data on Telework Devices)*

2.4.4 Security Considerations for the Telework and Remote Access Life Cycle - *Initiation (Permitted Forms of Remote Access, Restrictions on Telework Client Devices and Remote Access Levels, Additional User Requirements), Development, Implementation, Operations and Maintenance, Disposal.*

2.5 Server Security

2.5.1 Server BIOS Protection - *System BIOS, Server Architectures, System BIOS Update Mechanisms, Threats to the System BIOS, Root of Trust for Update, BIOS Security Principles (BIOS Update Authentication, Secure Local Update, Firmware Integrity Protection, Non-Bypassability), Security Guidelines by Update Mechanism (Secure BIOS Update at Anytime, Secure BIOS Update at Reboot, Secure BIOS Update Requiring Verification at Boot), Guidelines for Service Processors (Service Processor as a Root of Trust, Non-Bypassability of BIOS Protections by Service Processor)*

2.5.2 Basic Issues in Server Security - *Server Vulnerabilities, Threats, and Environments, Security Categorization of Information and Information Systems, Basic Server Security Steps, Server Security Principles*

2.5.3 Server Security Planning - *Installation and Deployment Planning, Security Management Staff, Management Practices, System Security Plan, Human Resources Requirements*

2.5.4 Securing the Server Operating System - *Patch and Upgrade Operating System, Hardening and Securely Configuring the OS (Remove or Disable Unnecessary Services, Applications, and Network Protocols, Configure OS User Authentication, Configure Resource Controls Appropriately), Install and Configure Additional Security Controls, Security Testing the Operating System*

2.5.5 Securing the Server Software - *Securely Installing the Server Software, Configuring Access Controls, Server Resource Constraints, Selecting and Implementing Authentication and Encryption Technologies*

2.5.6 Maintaining the Security of the Server - *Logging (Identifying Logging Capabilities and Requirements, Reviewing and Retaining Log Files, Automated Log File Analysis Tools), Server Backup Procedures (Server Data Backup Policies, Server Backup Types, Maintain a Test Server), Recovering From a Security Compromise, Security Testing Servers (Vulnerability Scanning, Penetration Testing), Remotely Administering a Server.*

2.6 Electronic Mail Security

2.6.1 Background and Standards - *Multipurpose Internet Mail Extensions, Mail Transport Standards (SMTP, SMTP Extensions, Proprietary Mail Transports), Client Access Standards (Post Office Protocol, Internet Message Access Protocol, Proprietary Mailbox Access Mechanisms, Web-Based Mail Access)*

2.6.2 Signing and Encrypting Email Messages - *OpenPGP, S/MIME, Key Management, Issues with Email Encryption*

2.6.3 Planning and Managing Mail Servers - *Installation and Deployment Planning, Security Management Staff, Management Practices, System Security Plan, Human Resources Requirements, General Information System Security Principles*

2.6.4 Securing the Mail Server Operating System - *Updating and Configuring the Operating System (Patch and Upgrade Operating System, Remove or Disable Unnecessary*

Services and Applications, Configure Operating System User Authentication, Configure Resource Controls Appropriately, Install and Configure Additional Security Controls) Security Testing the Operating System

2.6.5 Securing Mail Servers and Content - *Hardening the Mail Server Application (Securely Installing the Mail Server, Configuring Operating System and Mail Server Access Controls), Protecting Email from Malware (Malware Scanning, Content Filtering, User Awareness), Blocking Spam-Sending Servers, Authenticated Mail Relay, Secure Access, Enabling Web Access*

2.6.6 Implementing a Secure Network Infrastructure - *Network Composition and Structure (Inadvisable Network Layout, Demilitarized Zone, Mail Gateways, Management Network), Network Element Configuration (Router / Firewall Configuration, Intrusion Detection and Prevention Systems, Network Switches)*

2.6.7 Securing Mail Clients - *Installing and Configuring Client Applications (Patching and Updating Mail Clients, Configuring Mail Client Security Features, Configuring Authentication and Access, Securing the Client Host's Operating System), Secure Message Composition, Plug-ins, Accessing Web-Based Mail Systems*

2.6.8 Administering the Mail Server - *Logging (Recommended Generic Logging Configuration, Log File Review and Retention, Automated Log File Analysis Tools), Backing Up Mail Servers, Recovering from a Security Compromise, Security Testing Mail Servers (Vulnerability Scanning, Penetration Testing), Remotely Administering a Mail Server*

2.7 Public Web Server Security

2.7.1 Planning and Managing Web Servers- *Installation and Deployment Planning, Security Management Staff, Management Practices, System Security, Plan, Human Resources Requirements, Alternative Web Server Platforms (Trusted Operating Systems, Web Server Appliances, Pre-Hardened Operating Systems and Web Servers, Virtualized Platforms)*

2.7.2 Securing the Web Server Operating System - *Installing and Configuring the Operating System (Patch and Upgrade Operating System, Remove or Disable Unnecessary Services and Applications, Configure Operating System User Authentication, Configure Resource Controls Appropriately, Install and Configure Additional Security Controls), Security Testing the Operating System*

2.7.3 Securing the Web Server - *Securely Installing the Web Server, Configuring Access Controls (Configuring the Permissions of the Web Server Application, Configuring Secure Web Content Directory, Uniform Resource Identifiers and Cookies, Controlling Impact of Web Bots on Web Servers)*

2.7.4 Securing Web Content - *Publishing Information on Public Web Sites, Observing Regulations about the Collection of Personal Information, Mitigating Indirect Attacks on Content (Phishing, Pharming), Securing Active Content and Content Generation Technologies (Vulnerabilities with Client-Side Active Content Technologies, Vulnerabilities with Server-Side Content Generation Technologies, Server-Side Content Generator Security Considerations, Location of Server-Side Content Generators, Cross-Site Scripting Vulnerabilities)*

2.7.5 Using Authentication and Encryption Technologies - *Determining Authentication and Encryption Requirements, Address-Based Authentication, Basic Authentication, Digest Authentication, SSL / TLS (SSL/TLS Capabilities, Weaknesses of SSL/TLS, SSL/TLS Encryption Schemes, Implementing SSL/TLS, SSL/TLS Implementations), Brute Force Attacks*

2.7.6 Implementing a Secure Network Infrastructure - *Network Composition and Structure (Inadvisable Network Layout, Demilitarized Zone, Outsourced Hosting, Management Network), Network Element Configuration (Router/Firewall Configuration, Intrusion Detection and Prevention Systems, Network Switches, Load Balancers, Reverse Proxies)*

2.7.7 Administering the Web Server - *Logging (Identifying the Logging Capabilities of a Web Server, Identifying Additional Logging Requirements, Recommended Generic Logging Configuration, Reviewing and Retaining Log Files, Automated Log File Analysis Tools), Web Server Backup Procedures (Web Server Backup Policies and Strategies, Maintain a Test Web Server, Maintain an Authoritative Copy of Organizational Web Content), Recovering From a Security Compromise, Security Testing Web Servers (Vulnerability Scanning, Penetration Testing), Remotely Administering a Web Server*

2.8 Secure Deployment of IPv6

2.8.1 Understanding IPv6 - *Limitations of IPv4, Major Features of the IPv6 Specification, IPv4 and IPv6 Threat Comparison, Motivations for Deploying IPv6, IPv6 Addressing, IPv6 Address Allocations, IPv6 Header Types, Formats, and Fields, IPv6 Extension Headers, Internet Control Message Protocol for IPv6 (ICMPv6), IPv6 and Routing, IPv6 and the Domain Name System (DNS), Multihoming, IPv6 Multicast, IPv6 Quality of Service (QoS), Mobile IPv6, Jumbograms, Address Selection, Dynamic Host Configuration Protocol (DHCP) for IPv6, IPv6 Prefix renumbering*

2.8.2 IPv6 Security - *Privacy Addresses, Cryptographically Generated Addresses, IPsec in IPv6, Secure Stateless Address Auto-configuration and Neighbor Discovery*

2.8.3 IPv6 Deployment - *Security Risks, Addressing Security, Transition Mechanisms, Dual Stack IPv4/IPv6 Environments, Tunneling, Translation, Other Transition Mechanisms, The IPv6 Deployment Planning Process for Security, IPv6 Deployment (Initiation Phase, Acquisition / Development Phase, Implementation Phase, Operations / Maintenance Phase, Disposition Phase)*

2.9 Secure Domain Name System Deployment

2.9.1 Securing Domain Name System - *DNS, DNS Infrastructure, DNS Components and Security Objectives*

2.9.2 DNS Data and DNS Software - *Zone File, Name Servers (Authoritative Name Servers, Caching Name Servers), Resolvers*

2.9.3 DNS Transactions - *DNS Query/Response, Zone Transfer, Dynamic Updates, DNS NOTIFY*

2.9.4 DNS Hosting Environment Threats, Security Objectives, and Protection Approaches - *Host Platform Threats, DNS Software Threats, Threats Due to DNS Data Contents, Security Objectives, Host Platform Protection Approach, DNS Software Protection Approach, DNS Data Content Control – Protection Approach*

2.9.5 DNS Transactions Threats, Security Objectives, and Protection Approaches - *DNS Query/Response Threats and Protection Approaches (Forged or Bogus Response, Removal of Some RRs, Incorrect Expansion Rules Applied to Wildcard RRs, Protection Approach for DNS Query/Response Threats—DNSSEC), Zone Transfer Threats and Protection Approaches, Dynamic Updates Threats and Protection Approaches, DNS NOTIFY Threats and Protection Approaches*

2.9.6 Securing DNS Hosting Environment - *Securing DNS Host Platform, Securing DNS Software, Content Control of Zone File*

2.9.7 Securing DNS Transactions - *Restricting Transaction Entities Based on IP Address, Transaction Protection Through Hash-Based Message Authentication Codes*

2.9.8 Securing DNS Query/Response

2.9.9 Minimizing Information Exposure through DNS Data Content Control

2.9.10 DNS Security Administration Operations

2.10 SSL VPNs

2.10.1 Network and Transport Layer Security

2.10.2 SSL VPN Fundamentals, Planning and Implementation

2.10.3 Alternatives to SSL VPNs

3. INFORMATION SECURITY INCIDENT RESPONSE & FORENSICS

3.1 Information Security Incident Handling

3.1.1 Organizing a Computer Security Incident Response Capability - *Events and Incidents, Need for Incident Response, Incident Response Policy, Plan, and Procedure Creation, Incident Response Team Structure, Incident Response Team Services*

3.1.2 Handling an Incident - *Preparation, Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activity*

3.1.3 Coordination and Information Sharing - *Coordination, Information Sharing Techniques, Granular Information Sharing*

3.2 Forensics & Incident Response

3.2.1 Establishing and Organizing a Forensics Capability

3.2.2 Performing the Forensic Process - *Data Collection, Examination, Analysis, Reporting*

3.2.3 Data Files as Evidence - *File Basics, Collecting Files, Examining Data Files, Analysis*

3.2.4 Operating System Evidence - *Collecting, Examining & Analyzing volatile and non-volatile data*

3.2.5 Evidence from Network Traffic - *Sources, Collecting, Examining & Analyzing network traffic data*

3.2.6 Evidence from Applications - *Collecting, Examining & Analyzing application data*

4. REGULATORY & STANDARDS COMPLIANCE

4.1 Relevant Indian regulatory framework - *Information Technology Act and related rules, regulations, guidelines, circulars*

4.2 Relevant US regulatory framework – *Sarbanes-Oxley Act, Health Insurance Portability And Accountability Act, Federal Information Security Management Act*

4.3 Relevant EU regulatory framework

4.4 Relevant ISO standards – *13335, 15408, 20000, 27000 series*

4.5 Other standards - *FIPS PUB 200, PCI DSS, COSO framework, COBIT*

5. DATA PROTECTION

5.1 Cryptography

5.1.1 Understanding Cryptography – *Symmetric & Asymmetric cryptography, Hash Functions, Digital Signatures, Steganography, Random Number Generation, Key Management, Advanced Encryption Standard (AES), Message Authentication Code (MAC Based on a Block Cipher Algorithm, MACs Based on Hash Functions), Digital Signature Standard, RSA*

5.1.2 Public Key Infrastructure (PKI) - *Security Requirements for PKI Components, PKI Architectures*

5.1.3 General Implementation Issues - *Hardware vs. Software Solutions, Asymmetric vs. Symmetric Cryptography, Key Management*

5.1.4 Assessments - *Cryptographic Module Validation Program (CMVP), National Voluntary Laboratory Accreditation Program (NVLAP), Industry and Standards Organizations*

5.1.5 Selecting Cryptography – *Initiation, Acquisition/Development, Implementation/ Assessment, Operations and Maintenance, Disposition*

5.2 Storage Encryption Technologies for End User Devices

5.2.1 Storage Security Overview - *File Storage Basics, The Need for Storage Security, Security Controls for Storage*

5.2.2 Storage Encryption Technologies - *Common Types of Storage Encryption Technologies (Full Disk Encryption, Virtual Disk Encryption and Volume Encryption, File/Folder Encryption), Protection Provided by Storage Encryption Technologies*

5.2.3 Storage Encryption Technology Planning and Implementation - *Identify Needs, Design the Solution (Cryptography, Authentication), Implement and Test Prototype, Deploy the Solution, Manage the Solution*

6. INFORMATION SECURITY RISK ASSESSMENT & TESTING

6.1 Risk Management

6.1.1 Fundamentals of risk management - *components of risk management, multitiered risk management, trust and trustworthiness, organizational culture, relationship among key risk concepts*

6.1.2 Risk management process - *framing risk, assessing risk, responding to risk, monitoring risk*

6.2 Conducting Risk Assessments

6.2.1 Fundamentals of risk assessments - *risk management process, risk assessment, key risk concepts, application of risk assessments*

6.2.2 Risk assessment process – *preparing for the risk assessment, conducting the risk assessment, communicating and sharing risk assessment information, maintaining the risk assessment*

6.3 Information Security Testing and Assessment

6.3.1 Understanding Security Testing & Examination - *Information Security Assessment Methodology, Technical Assessment Techniques, Comparing Tests and Examinations, Testing Viewpoints (External and Internal, Overt and Covert)*

6.3.2 Review Techniques - *Documentation Review, Log Review, Ruleset Review, System Configuration Review, Network Sniffing, File Integrity Checking*

6.3.3 Target Identification & Analysis Techniques - *Network Discovery, Network Port and Service Identification, Vulnerability Scanning, Wireless Scanning (Passive Wireless Scanning, Active Wireless Scanning, Wireless Device Location Tracking, Bluetooth Scanning)*

6.3.4 Target Vulnerability Validation Techniques - *Password Cracking, Penetration Testing (Penetration Testing Phases, Penetration Testing Logistics), Social Engineering*

6.3.5 Security Assessment Planning - *Developing a Security Assessment Policy, Prioritizing and Scheduling Assessments, Selecting and Customizing Techniques, Assessment Logistics (Assessor Selection and Skills, Location Selection, Technical Tools and Resources Selection, Assessment Plan Development, Legal Considerations)*

6.3.6 Security Assessment Execution - *Coordination, Assessing, Analysis, Data Handling (Data Collection, Data Storage, Data Transmission, Data Destruction)*

6.3.7 Post-Testing Activities - *Mitigation, Reporting, Remediation / Mitigation*

7. CONTINGENCY PLANNING

7.1 Understanding contingency planning

7.1.1 Contingency Planning and Resilience

7.1.2 Types of Plans - *Business Continuity Plan (BCP), Continuity of Operations (COOP) Plan, Crisis Communications Plan, Critical Infrastructure Protection (CIP) Plan, Cyber Incident Response Plan, Disaster Recovery Plan (DRP), Information System Contingency Plan (ISCP), Occupant Emergency Plan (OEP)*

7.2 Information System Contingency Planning Process

7.2.1 Developing the Contingency Planning Policy Statement

7.2.2 Conducting the Business Impact Analysis (BIA) - *Determine Business Processes and Recovery Criticality, Identify Resource Requirements, Identify System Resource Recovery Priorities*

7.2.3 Identifying Preventive Controls

7.2.4 Creating Contingency Strategies - *Plan Backup and Recovery, Backup Methods and Offsite Storage, Alternate Sites, Equipment Replacement, Cost Considerations, Roles and Responsibilities*

7.2.5 Testing, Training, and Exercises - *Testing, Training, Exercises, Plan Maintenance*

7.3 Information System Contingency Plan Development

7.3.1 Supporting Information

7.3.2 Activation and Notification Phase - *Activation Criteria and Procedure, Notification Procedures, Outage Assessment*

7.3.3 Recovery Phase - *Sequence of Recovery Activities, Recovery Procedures, Recovery Escalation and Notification*

7.3.4 Reconstitution Phase

7.3.5 Plan Appendices

7.4 Technical Contingency Planning Considerations

7.4.1 Common Considerations - *Use of the BIA, Maintenance of Data Security, Integrity, and Backup, Protection of Resources, Adherence to Security Controls, Identification of Alternate Storage and Processing Facilities, Use of High Availability (HA) Processes*

7.4.2 Client/Server Systems - *Client/Server Systems Contingency Considerations & Solutions*

7.4.3 Telecommunications Systems - *Telecommunications Contingency Considerations & Solutions*

7.4.4 Mainframe Systems - *Mainframe Contingency Considerations & Solutions*

C. The IFS-GFSU Continuous Education Program

The IFS-GFSU Continuous Education Program (CEP) is designed to keep your expertise and skills updated. You are required to obtain 120 CEUs (Continuing Education Units) every 3 years to maintain your GFSU certification.

You are required to submit documentary evidence every 3 years of CEUs earned by you. Enclose administrative fee of Rs 2,000 plus taxes along with the documentary evidence of CEUs.

#	Activity	CEUs earned	Documentary Evidence to be submitted	Maximum CEUs in a 3 year period
1	Teaching, training or instructing in a relevant field	3 CEUs per hour of actual teaching, training or instructing	1. Description of content covered 2. Delivery date(s) 3. Number of attendees	42 CEUs
2	Delivering an Industry Presentation in a relevant field	3 CEUs per hour of actual presentation	1. Description of content covered 2. Delivery date(s) 3. Number of attendees 4. Copy of presentation	42 CEUs
3	Participation in a GFSU approved Industry Event, Seminar, Workshop or Conference	1 CEU for each hour spent in a relevant session	1. The type of activity attended (event, seminar, workshop or conference) 2. Description of the activity 3. Date of Activity 4. Proof of completion provided by activity host (where applicable)	42 CEUs
4	Work Experience	1 CEU for each month in a relevant profile	Following details on employer letterhead: 1. Current job title 2. Brief description of work profile 3. Duration in this job (start and end dates) 4. Confirmation by employer that the candidate is meeting the expectations 5. Signature of the candidates supervisor	36 CEUs
5	Publishing of a relevant professional Article, White Paper or Book	4 CEUs per article or white paper; 20 CEUs per published book	Description of the content covered Link to or copy of the published work	42 CEUs
6	Active membership of a GFSU approved relevant Committee / Board / Chapter / Association	0.25 CEU for each month of membership	1. Committee / Board / Chapter / Association details 2. Proof of membership 3. Timeframe of active membership	9 CEUs

D. About GFSU

This certification is provided by Institute of Forensic Science, Gujarat Forensic Sciences University (GFSU).

GFSU is established by the Government of Gujarat, under the flagship of the Home Department - Government of Gujarat.

The GFSU is a highly specialized higher education institution that came into existence through an Act: No. 17, passed by the Gujarat State Legislative Assembly, dated the 30th of September 2008.

The University runs in parallel association with the Directorate of Forensic Science (DFS) - Gujarat State, to provide hands-on training.

DFS - Gujarat State is a state-of-the-art; NABL accredited; ISO-IEC 17025:2005 certified laboratory, maintaining international standards in terms of infrastructure and facilities for Computer Forensics, Narco-analysis and Polygraph Examination, Brain Electrical Oscillation Signature Profiling.

It also has Suspect Detection System (SDS), Audio Video Tape Authentication System, Voice Spectrograph, Speech Lab, Integrated Ballistics Identification System, Computerized Petroleum Testing Facilities, Fully Automated Alcohol Estimation System (GC-HS) FT-Raman, LC-MS, GC-MS, FT-IR for Narcotic/Explosive/Poisons Analysis, Computerized Photographic Image Analysis System, Video Spectral Comparator for Document Examination, Accredited Cow-meat testing mobile laboratories, Accredited Mobile Investigation Vans, Ballistics Data Acquisition System (Computerized firing range) and Automated Fingerprint Identification System.

GFSU is the only university across the world, dedicated to Forensic & Investigative Science.

The GFSU has an ultramodern campus, near the DFS premises, on a government allocated land of 50,000 Square Meters.

The University is headed by its Director General Dr. J. M. Vyas (M.Sc., Ph.D., LL.B.). Dr. Mohinder Singh Dahiya (M.Sc., Ph.D.) is the Director for the Institute of Forensic Science, Gujarat Forensic Sciences University. Shri Mehul K. Dave is the first Registrar of the Gujarat Forensic Sciences University.

The university has been granted recognition by the University Grants Commission wide its letter no. F.9-7/2011 (CPP-I/PU) dated 16th May 2011.

E. Application Form for Permanent Registration Number for IFS-GFSU Certification Programs

GUJARAT FORENSIC SCIENCES UNIVERSITY

To,
Director,
Institute of Forensic Science,
Gujarat Forensic Sciences University,
Gandhinagar

I am desirous of appearing for IFS-GFSU (Institute of Forensic Science, Gujarat Forensic Sciences University) certifications and therefore request for allotment of Permanent Registration Number. My personal information is as under:

Please paste your recent passport size colour photograph in this box.

DO NOT STAPLE

A. NAME

First

Middle

Last

B. DATE OF BIRTH

Day *Month* *Year*

C. OCCUPATION

*(In case you are a **student**, mention details such as College, course, year etc.)*

D. GENDER

Female ☐ *Male* ☐

E. ADDRESS FOR COMMUNICATION

Apartment / House Number & the Name of the Building

Street / Road / Boulevard

Town / City

State

Country

PIN Code / ZIP

Email Address

Cell / Mobile number

Phone number (with ISD / STD code)

F. FEE DETAILS

Bank Draft number _____ Dated_____ for **Rs. 1,000** (non-refundable)

Bank Name _____ Branch _____

Favouring: "**The Registrar, Gujarat Forensic Sciences University**" Payable at **Gandhinagar**, Gujarat

G. ADDITIONAL QUALIFICATIONS (IF ANY)

H. DOCUMENTS

Please enclose self-signed photocopies of the following documents:

1. Proof of identity: (any one)

☐ *Driving license* ☐ *Passport* ☐ *PAN Card* ☐ *College ID card*

2. Proof of educational qualification (any one)

☐ *Mark sheet* ☐ *Degree* ☐ *Other (pl specify)*

I. ADDITIONAL INFORMATION

Have you ever been convicted of a cognizable offence or a Court Martial in military service?
If yes, provide details.

Have you ever had a professional license, certification, membership or registration revoked?
If yes, provide details.

The Application Form, duly completed, is submitted along with the relevant fee and supporting documents. All the information provided is true to the best of my knowledge and belief. Please acknowledge receipt of the same and confirm my registration.

Regards,

(Applicant's Signature) Date

UNDERTAKING

1. IFS-GFSU may, at its sole discretion, make inquiry of persons or documents directly or indirectly referenced in this application to verify the accuracy and completeness of the information provided by me. I agree to cooperate in any such investigation by IFS-GFSU regarding the information I have provided.

2. I understand that my non-cooperation in such investigation or my providing any information that is fraudulent, misleading or false may result in the refusal of IFS-GFSU to issue a credential to me. It may also lead to my being barred from ever holding a IFS-GFSU credential.

3. I undertake to inform IFS-GFSU, without delay, of matters that can affect my capability to fulfil the certification requirements. I shall comply with the relevant provisions of the certification scheme.

4. I undertake not to release confidential examination materials or participate in fraudulent test-taking practices.

5. I agree to comply with the certification requirements and to supply any information needed for the assessment.

6. In the event of suspension of my certification, I shall refrain from further promotion of the certification while it is suspended. In the event of withdrawal of my certification, I shall refrain from use of all references to a certified status.

7. I shall make claims regarding certification only with respect to the scope for which certification has been granted.

8. I shall not use the certification in such a manner as to bring IFS-GFSU into disrepute, and shall not to make any statement regarding the certification, which IFS-GFSU considers misleading or unauthorized.

9. I shall discontinue the use of all claims to certification that contain any reference to IFS-GFSU or certification upon suspension or withdrawal of certification, and to return any certificates issued by IFS-GFSU.

10. I shall not use the certificate in a misleading manner.

11. I understand that any action arising out of any application, examination, certification, etc. conducted by IFS-GFSU is subject to the courts of Gandhinagar, Gujarat, India.

I have read and understood the statements above and agree to be legally bound by them.

Regards,

(Signature) Date

Submit the filled-in application form, bank draft and documents to:

Dr. MS Dahiya,
Director, Institute of Forensic Science,
Gujarat Forensic Sciences University,
DFS Head Quarters, Sector 18-A
Near Police Bhavan, Gandhinagar-382007
Gujarat - India

Phone: (079) 65735503