



OUR HISTORY



Enterprise InfoSec Consultants (EIC) is a global cybersecurity service provider assisting organizations in protecting valuable information assets and achieving information security-related standards and regulatory compliances since 2016.

EIC undertakes a wide range of international missions and infosec projects. We are well known to our customers as a trusted information security service provider to international organizations, government administrations, and the private sector.

ABOUT US



With a team of industry experts, we offer a comprehensive suite of services, including professional consulting services in compliance auditing, such as PCI DSS, ISO/IEC 27001, Swift CSP Assessment, GDPR compliance, Vulnerability management, dark web analysis, and also address our customer needs for Red and Blue teams to help you meet industry standards and safeguard your systems from security threats.

Our goal is to help you navigate the complex landscape of cybersecurity with confidence and peace of mind.



WE ARE ISO 27001 CERTIFIED ORGANIZATION



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Enterprise InfoSec Consultants
House-15,Road-7
Block C, Niketon, Gulshan
Dhaka 1212
Bangladesh

Holds Certificate No:

IS 772182

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

Information security management system of Enterprise InfoSec Consultant applies to Consultancy and compliance work rendered to their customers with E-Compliance Application, GRC, Red Team, Blue Team and support functions e.g.IT, HR, Admin, Accounts and Procurement
This is in accordance with the Statement of Applicability Version 1.0, Dated 10.05.2022.

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2022-05-26

Latest Revision Date: 2022-05-26

Effective Date: 2022-05-26

Expiry Date: 2025-05-25

Page: 1 of 2



...making excellence a habit.™

OUR SERVICES



PCI DSS
Compliance

Dark Web
Analysis

Security
Operations
Centre

Information
Systems Audit

ISO 27001

Swift CSP
Consultancy &
Assessment

Pen testing

Red Teaming
Exercise

Vulnerability
Management

PCI DSS COMPLIANCE

Secure your organization, being **PCI DSS** Compliant.

The Payment Card Industry Data Security Standard (PCI DSS) defines information security requirements for all organizations that store, process, or transmit credit card data. It is an information security standard containing requirements that help organizations prevent payment card fraud.

As a leading PCI QSA organization, EIC is committed to helping businesses of all sizes meet the strict security standards set by the Payment Card Industry Data Security Standard (PCI DSS). Our team of experts stays up-to-date with the latest developments in PCI DSS to ensure that your business remains compliant and secure.



We will help your organization with –

- Preventing payment card data breaches, building customer trust, the way to avoid fines and penalties, and meeting global data security standards by following the rigid framework and being subject to constant quality checks
- Effective, practical, and simple policies to maintain the standards
- Simplified procedures ensuring the payment card data security
- End-to-end PCI DSS compliance project management until your organization achieves PCI DSS compliance certification.

RED TEAM EXERCISE

"Improve Your Security Posture with Red Teaming Exercises"

Red Teaming Exercise is a proactive and comprehensive approach to security testing that simulates real-world attack scenarios to identify vulnerabilities and weaknesses in your organization's security posture. Our team of experienced security experts at Enterprise InfoSec Consultants offers a full-spectrum Red Teaming Exercise service that provides the insights you need to protect your business.



Our experienced security experts simulate attack scenarios to identify vulnerabilities and weaknesses in your network, systems, and processes. By conducting these exercises, we help you better understand your security posture, identify areas for improvement, and provide recommendations for enhancing your overall security. Whether you need to prepare for a potential attack or meet industry regulations, our Red Teaming Exercise services are designed to give you the insights you need to protect your business.

We will help your organization with:

- Threat modeling and scenario creation
- Vulnerability assessments
- Penetration testing
- Social engineering
- Reporting and recommendations

Our Red Teaming Exercise services are designed to provide a comprehensive and realistic assessment of your organization's security posture. Whether you need to prepare for a potential attack, meet industry regulations, or want to be proactive about your security, our services are designed to give you the peace of mind and protection you need.

PEN TESTING

Secure Your Business with Our Pen testing Service

EIC provides the best offensive approach & hacker-driven penetration testing services. We apply both automated & manual analysis, cutting-edge penetration testing methodologies, the best pen testing tools, and our unique penetration testing report.

Our penetration testing services are designed to provide you with a comprehensive understanding of your security posture and identify areas for improvement. Our experts will provide a detailed report that includes findings, recommendations, and actionable steps to enhance your security posture.



EIC's penetration testing services help you quickly reduce cyber security risks and demonstrate a comprehensive penetration testing report to clients, management, and investors. Hire one of the best penetration testing firms today!

We will help your organization with:

- Network penetration testing
- Software/Application penetration testing
- Mobile application penetration testing
- Wireless network penetration testing
- Infrastructure penetration testing

VULNERABILITY MANAGEMENT

Reduce risk and compliance costs with our **Vulnerability Management** services

Managing technology infrastructure with limited resources is common in most organizations. On top of that, ever-increasing threats and a vulnerability landscape make it more difficult and expensive for every organization to manage an effective vulnerability management program. Organizational size, multiple stakeholder involvement, and increasing volume of vulnerabilities make the situation worse. In most cases, vulnerabilities remain unattended for a long time or are even unknown to management, eventually leading to massive cyber attacks.



We will help your organization with:

- Vulnerability Scanning
- Analysis
- Reporting
- Remediation
- Continuous Improvement
- Priorities vulnerabilities based on risk level and take appropriate action to remediate them.
- Regularly review and update the assessment's scope and setting to ensure it covers all the necessary assets and services.
- Coverage of the entire infrastructure or defined scope as per your business need
- Dedicated, experienced support engineer and service manager

DARK WEB ANALYSIS

Protect Yourself on the **Dark Web** - Uncover the Truth

As a cyber security consulting organization, we understand the importance of protecting a company's sensitive information from being disclosed on the dark web. Our team has extensive experience conducting dark web information disclosure analysis and can provide a comprehensive report on any potential risks to your company's sensitive information.

Our team has extensive experience conducting dark web information disclosure analysis and can provide a comprehensive report on any potential risks to your company's sensitive information. We look forward to working with you to protect your company's sensitive data from being disclosed on the dark web.



We will help your organization with:

- Identifying sensitive information
- Risk assessment
- Reporting
- Mitigation
- Follow-up

SECURITY OPERATIONS CENTRE

Protect Your Data, Protect Your Business - Security Operations Centre Services

Information security has become one of the essential considerations in technology-driven business entities, and the necessities for guaranteeing information security are now becoming stringent. Simultaneously, hackers have become more relentless, making dealing with information security events an increasingly difficult challenge. Cyber-attacks are no longer a question of 'if' but of 'when' in today's age of 'always-on' technology and inadequate security awareness on users' side. We live in an era where information security prevention is not an option but a must.

SOC is the heart of your infrastructure security, a centralized system management mechanism, and a collaboration of people and software. It is designed to detect anomalies, highlight real threats, and respond to them appropriately. A SOC also selects, operates, and maintains the organization's cybersecurity technologies and continually analyses threat data to find ways to improve the organization's security posture.



We will help your organization with:

- SOC as a service
- SOC Implementation consultancy
- Sharing SOC resource pool
- Ensure that logs are being collected from all the in-scope devices.
- Provide 24*7 Incident Management support.

INFORMATION SYSTEM AUDIT

Ensuring Secure & Reliable Information Systems

An Information Systems audit evaluates an organization's information technology infrastructure, business software & applications, business processes, data use, and management, policies, procedures, and operational processes against recognized standards or established guidelines. Audits evaluate whether the controls to protect information technology assets for ensuring integrity and controls are aligned with organizational goals and objectives.



We will help your organization with:

- Audit Planning
- Risk Assessment and Business Process Analysis
- Review System Security
- Assess Data Integrity
- Evaluate System Performance
- Analyze System Documentation
- Performance of Audit Work
- Reporting
- Verify Compliance

ISO 27001

Upscaling Information Security into International Level

ISO 27001 is a globally recognized and accepted standard for maintaining Information Security Management System (ISMS). When it comes to handling organizational data, trust is paramount. An ISO 27001 certification doubles as a trust assurance. We provide a hassle-free compliance service with affordable implementation.

Partnering with EIC for your ISO/IEC 27001 information security certification means better-performing methods, increasingly skillful talent. and more sustainable client relationships with our professionals.



We will help your organization with:

- Achieving a way to guarantee a high standard of Information Security quality by following a rigid framework and subject to constant quality checks
- Effective, practical, and simple policies maintaining the standard.
- Simplified procedures ensuring security.
- End-to-end ISO 27001 compliance project management until your organization achieves ISO 27001 compliance certification.

Swift CSP CONSULTANCY & ASSESSMENT

Swift security matters for your Business

In 2016, the Society for Worldwide Interbank Financial Telecommunication (Swift) established the Customer Security Programme (CSP), introducing the Customer Security Controls Framework (CSCF). Swift's Customer Security Programme (CSP) helps financial institutions ensure their defenses against cyberattacks are up-to-date and adequate to protect the integrity of the broader financial network.

EIC has a dynamic cybersecurity specialist team with deep expertise in Cybersecurity, IS Audit, and IT Compliance. With years of experience providing information system audits, governance, risk, and compliance services for our banking and financial clients, we understand the ever-changing challenges and threats financial organizations face. Our team of Information security and Information system auditors is skilled in providing our clients with independent and required control design and implementation over compliance framework. We work with your team at every step to ensure a successful attestation for Swift CSP.



We will help your organization with:

- Gap analysis with that of your current practice and CSP requirement's Compliance.
- Preparing Customer Security Controls Framework (CSCF) implementation roadmap.
- Implementing Customer Security Controls Framework (CSCF).
- Validating your organization's Swift CSP compliance.

PROFESSIONAL CERTIFICATIONS

Certification
Certified Information Systems Security Professional (CISSP)
PCI DSS Qualified Security Assessor (QSA)
Offensive Security Certified Professional (OSCP)
Certified Information Systems Auditor (CISA)
Certified Ethical Hacker (CEH)
ISO 27001 Lead Auditor (LA)
ISO 27001 Lead Implementer (LI)
Certified in Cybersecurity (CC)
Lean Six Sigma Black Belt (LSSBB)
Certified Fraud Examiner (CFE)
EC-Council Certified Security Analyst
Certified Threat Intelligence Analyst
MITRE ATT&CK SOC ASSESSMENT
Red hat Certified Engineer
Red Hat Certified Systems Administrator

OUR PCI DSS COMPLIANCE CLIENTS

Standard
Chartered Bank
Bangladesh



OUR ISO 27001 CLIENTS

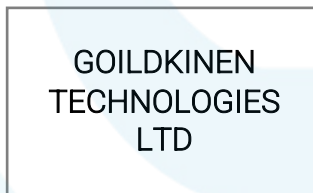
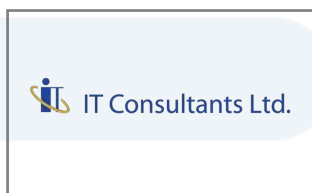
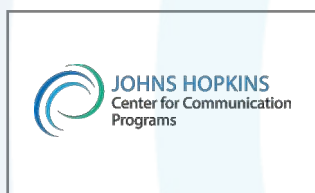
Standard
Chartered Bank
Bangladesh



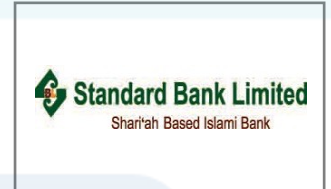
OUR VAPT CLIENTS



OUR VAPT CLIENTS



OUR SWIFT CSP ASSESSMENT CLIENTS



OUR IT AUDIT & HIPAA COMPLIANCE AUDIT CLIENTS



OUR SOC SERVICE CLIENTS





Contact Us



Corporate Office

House - 15 (5th Floor), Road - 7,
Block - C, Niketon, Gulshan,
Dhaka 1212, Bangladesh



+88 09617204204



www.eic.com.bd



info@eic.com.bd