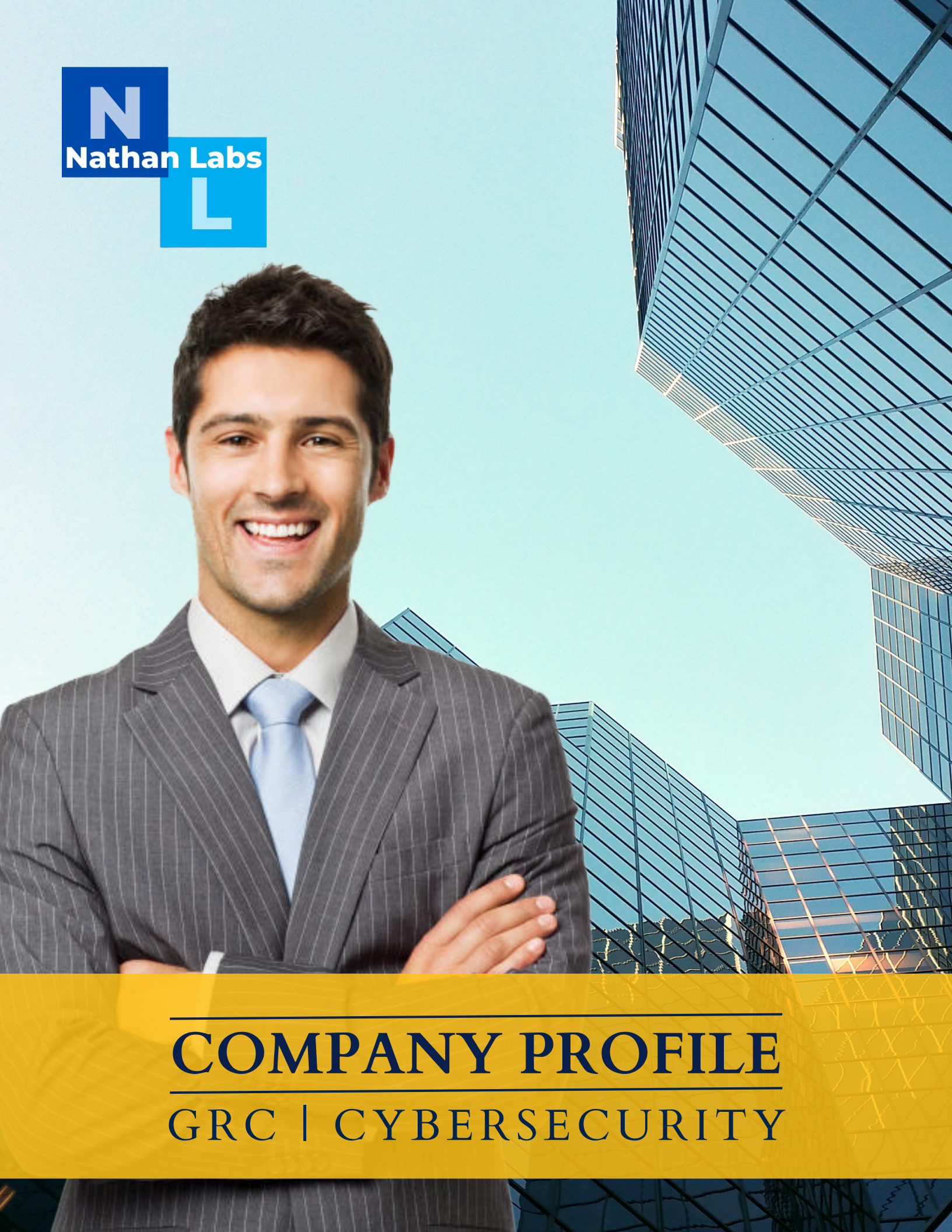
Nathan Labs



COMPANY PROFILE

GRC | CYBERSECURITY

NATHAN LABS

AT A GLANCE

Nathan Labs is a provider of GRC, cybersecurity services and compliance solutions for businesses operating in highly-regulated industries. The company offers a unique combination of services to help organizations manage IT governance, risk management, and compliance (GRC).

OUR COMPANY

Established in
DUBAI
2018

Established in
INDIA
2019

Established in
USA
2022

OUR PURPOSE

Nathan Labs was founded with the purpose of providing confidence to businesses against all operational failures.

OUR VISION

Our vision is to help people and enterprises Nathan Labs their IT infrastructure in terms of security, performance, continuous regression, scalability and availability.

GRC

Governance, Risk and Security Compliance (GRC) is a framework that organizations use to manage the various aspects of their operations, including risk management, compliance with laws and regulations, and information security.

Governance refers to the systems and processes that are put in place to manage and control an organization's activities. This includes establishing policies and procedures, setting objectives, and ensuring that the organization operates in a responsible and ethical manner.

Risk management involves identifying and assessing potential risks to the organization, and developing strategies to mitigate or eliminate those risks. This can include assessing risks related to financial, operational, and reputational factors.

Security compliance involves ensuring that an organization's information systems are secure and protected against unauthorized access, theft, and other security threats. This includes implementing security controls, such as firewalls and access controls, and monitoring and testing the security of information systems.

Overall, GRC helps organizations to manage their operations in a more efficient and effective manner, while also reducing the risks of financial loss, legal liability, and reputational damage.

SERVICES OVERVIEW

Cybersecurity

- Cyber Consulting
- Cyber Defense

Training

- Cyber Security
- Data Privacy
- Payment Services
- ISACA

Compliance

- Data Privacy
- Healthcare
- Payment Industry
- USA Govt
- GCC Compliance
- ISO
- Others
- Consulting/Certification

Technology

- Block Chain Service
- Application

Risk Advisory

- Tech Advisory
- Business Advisory

Services

- VAPT
- Threat Hunting

INDUSTRIES WE SERVE

Healthcare | Startups | Small Businesses | Banking Finance Fintech | Government | Internet of Things | Manufacturing | Aviation | Hospitality | Education | Legal Creative Firms and Media | Non-Profit | Gaming | Artificial Intelligence | Automotive/ Automobile | Retail | Real Estate | Cloud Application | Ecommerce | Logistics & Transport | Power & Energy | Software, IT and Technology | BlockChain | Speech Recognition | Business Intelligence | Hello Startups | Incubator | Marketing Services

ALL SERVICES

Cyber Consulting

Nathan Labs LLC provides next-generation cybersecurity consulting services to help your organization build cyber resilience from the inside out.

Cyber Security Policy Review

A cyber security policy contains pre-approved organizational procedures that tell you exactly what you need to do in order to prevent security problems and next steps if you are ever faced with a data breach.

Forensic Audit

A forensic audit is an examination and evaluation of a firm's or individual's financial information for use as evidence. in the court of law. A forensic audit can be conducted in order to prosecute a party for fraud, embezzlement or. other financial claims.

Cyber Forensics

The science of collecting, inspecting, interpreting, reporting, and presenting computer-related electronic evidence is known as cyber forensics. Evidence can be found on the hard drive or in deleted files.

Cyber Security Assessment

Cyber risk assessments are defined by NIST as risk assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

Cloud Computing Security

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing.

Supply Chain Security

Supply chain security activities aim to enhance the security of the supply chain or value chain, the transport and logistics systems for the world's cargo and to "facilitate legitimate trade"

Cyber Defense

Cyber defense is a coordinated act of resistance that guards information, systems, and networks from cyber attacks by implementing protective procedures such as firewalls, network detection and response (NDR), endpoint detection and response (EDR) to identify, analyze, and report incidents that occur within a network.

Architecture Implementation

Implementation Architecture Focuses on how the system is built. • Which technological elements are needed to implement the system. • So ware packages, libraries, frameworks, classes, ... • Addresses non-runtime requirements & quality a ributes.

Financial Cyber Security

Financial cybersecurity includes risk management, data integrity, security awareness training, and risk analysis. Essential elements of risk management include risk evaluation and the prevention of harm from those risks. Data security also addresses the security of sensitive information.

Cyber Defense

Defend your enterprise from security breaches by quickly detecting, responding to and remediating attacks.

EU-U.S. Privacy Shield GDPR

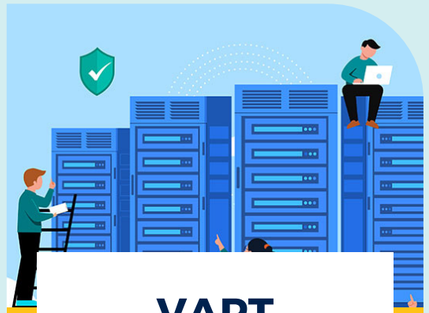
It is important to note that Privacy Shield is not a GDPR compliance mechanism, but rather is a mechanism that enables participating companies to meet the EU requirements for transferring personal data to third countries, discussed in Chapter V of the GDPR.

Cybersecurity Technical Writing

Cybersecurity Technical Writers create and oversee cybersecurity content, whether it's composing reports, synthesizing data, creating manuals, or editing cybersecurity policies to resonate with the target audience.

FAIR Risk Assessment

The Factor Analysis of Information Risk (FAIR) assessment was designed to quantify risks and define the chances of those risks becoming serious threats. A FAIR risk assessment helps companies minimize all possible chances of risks by identifying the factors contributing to them.



VAPT

VAPT describes a broad range of security assessment services designed to identify and help address cyber security exposures across an organisation's IT estate.

Penetration Testing

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities.

ALL SERVICES

VAPT Services

VAPT stands for Vulnerability Assessment & Penetration Testing. It is a security testing to identify security vulnerabilities in an application, network, endpoint, and cloud.

Application Security Testing

Application security testing (AST) is the process of making applications more resistant to security threats, by identifying security weaknesses and vulnerabilities in source code.

Infrastructure Security Testing

Infrastructure testing is a penetration test (also known as a pentest or pentesting) or vulnerability assessment of computer systems, network devices or IP address ranges to identify vulnerabilities that could be exploited.

IoT Security Testing

IoT security testing is the process of evaluating IoT devices to find security vulnerabilities in both hardware and software. The testing process must consider risks to both device & network assets to ensure secure operation & avoid unwanted access from malicious actors.

Testing for Compliance

Conformance testing — an element of conformity assessment, and also known as compliance testing, or type testing — is testing or other activities that determine whether a process, product, or service complies with the requirements of a specification, technical standard, contract, or regulation.

Red Team Exercise

An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

Managed Threat Hunting

Managed threat hunting is a proactive cybersecurity strategy that aims to identify and mitigate potential threats before they cause significant harm.

Payment Industry

Payment, or credit card, processors are companies that work in the background to provide payment processing services to merchants.

IRS E-File

E-file is a system for submitting tax documents to the US Internal Revenue Service through the Internet or direct connection, usually without the need to submit any paper documents.

SWIFT CSP Assessments

SWIFT's Customer Security Programme (CSP) helps financial institutions ensure their defences against cyberattacks are up to date and effective, to protect the integrity of the wider financial network.

FINRA

FINRA enables investors and firms to participate in the market with confidence by safeguarding its integrity.

PCI DSS

The Payment Card Industry Data Security Standard is an information security standard used to handle credit cards from major card brands.

PCI 3DS

PCI 3DS is a modern messaging protocol that enables consumer authentication with their card issuer when making online purchases. This additional layer of security helps prevent online fraud, making online shopping safer for merchants and consumers.

PCI PIN Service

PCI PIN is a Security Standard outlined by the PCI Council on payment security, to protect PIN data. It provides a set of requirements for secure management, processing, and transmission of PIN data during online and offline card transactions.

Health Care

It consist of medical professionals, organizations, and ancillary health care workers who provide medical care to those in need.

HIPAA / HITech Compliance

It requires healthcare organizations to use appropriate safeguards to ensure that electronic protected health information (ePHI) remains secure, and the HITECH Act, which expands the HIPAA encryption compliance requirement set, requires the timely disclosure of data breaches.

Hitrust

It helps organizations maintain a high level of data security, manage risk internally and with external vendors, and reduce the chances of a data breach.

ALL SERVICES

GCC Compliance

It provides integrated professional services to help clients meet increasingly complex business, regulatory and social challenges.

ADGM Data Protection

The Office of Data Protection is responsible for promoting data protection within ADGM, maintaining the register of Data Controllers, enforcing the obligations upon Data Controllers upholding the rights of individuals.

SAMA Compliance Saudi Arabia

The Saudi Arabian Monetary Authority (SAMA) is the central banking organization of Saudi Arabia. SAMA governs and regulates the legalities, processes, and information security strategies of all banking organizations and financial enterprises in the region.

NESA Compliance

National Electronic Security Authority (NESA), is a UAE federal authority responsible for the cybersecurity of the United Arab Emirates.

Adhics Compliance

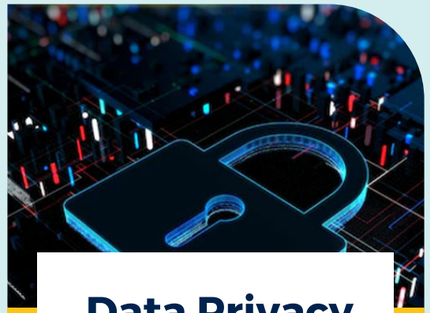
ABU DHABI HEALTHCARE INFORMATION AND CYBER SECURITY STANDARD (ADHICS) is a sector level standard by Department of Health (DoH), mandated to all healthcare entities in Abu Dhabi.

DIFC Data Protection Compliance

The DIFC law aims to safeguard the personal data of individuals whose data is processed by DIFC registered entities. It is heavily influenced by the EU General Data Protection Regulation (GDPR) as well as other world-class data protection laws.

NCEMA 7000:2015 Certification

defines a set of mechanisms and activities that will help you to secure the flow of your organization's functions and services until full recovery from an emergency, crises, or disaster is achieved.



Data Privacy

Data privacy is the right of a citizen to have control over how their personal information is collected and used. Data protection is a subset of privacy.

CCPA

The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.

NYDFS Cybersecurity Risk Assessment

The NYDFS Cybersecurity Regulation requires New York insurance companies, banks, & other regulated financial services institutions—including agencies& branches of non-US banks licensed in the New York. to assess.

EU GDPR

The General Data Protection Regulation is a Regulation in EU law on data protection and privacy in the EU and the European Economic Area.

Certification

Certification is part of Testing, inspection and certification and the provision by an independent body of written assurance that the product, service or system in question meets specific requirements.

NIST 800 Cyber Security Frame Work

The NIST Cybersecurity Framework provides comprehensive guidance and best practices that private sector organizations can follow to improve information security and cybersecurity risk management.

Anti-Money Laundering

In the most general sense, Anti-Money Laundering (AML) refers to the collection of laws, processes, and regulations that prevent illegally obtained money from entering the financial system.

MAS Cyber Hygiene Compliance of Singapore

The Notice on Cyber Hygiene sets out the measures that financial institutions must take to mitigate the growing risk of cyber threats.

Anti-Bribery Compliance

Anti-bribery guidelines prevent people and organizations from attempting to bribe others, while anti-corruption guidelines prevent public officials from accepting those bribes.

ALL SERVICES

USA Govt

In the US, compliance requirements are a series of directives US fed agencies established that summarize hundreds of federal laws and regulations applicable to federal assistance.

NIST 800-171

NIST 800-171 is a publication that outlines the required security standards and practices for non-federal organizations that handle CUI on their networks.

FedRAMP

The Federal Risk and Authorization Management Program is a United States federal government-wide compliance program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FISMA

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002.

CMMC

The Cybersecurity Maturity Model Certification is an assessment framework and assessor certification program designed to increase the trust in measures of compliance to a variety of standards published by the National Institute of Standards and Technology.

Nerc CIP

NERC Critical Infrastructure Protection (NERC CIP) is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

Sox

The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations.

Other Services

The purpose of compliance services is to help organizations remain up-to-date with governmental and industry standards. It includes services across multiple areas such as accounting, risk management, registrations, and startup compliance.

CIS Center for Internet Security

The Center for Internet Security (CIS) is a nonprofit organization focused on improving public- and private-sector cybersecurity readiness and response.

SOC 1

System & Organization Controls 1, aims to control objectives with the process area & documents internal controls relevant to an audit of a user entity's financial statements.

SOC 2

SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data.

CCPA

The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.

Crypto Currency Security Standard

CryptoCurrency Security Standard (CCSS) is a list of crypto asset management requirements that all crypto-related companies should meet.

CE Marking Services by a European Notified Body

CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health and environmental protection requirements. It is required for products manufactured anywhere in the world that are then marketed in the EU.

NERC CIP Compliance

The NERC CIP standards are the mandatory security standards that apply to entities that own or manage facilities that are part of the U.S. and Canadian electric power grid.

RBI Cyber security Framework

The RBI cyber security framework addresses three core areas: (1) Establish Cyber Security Baseline and Resilience (2) Operate Cyber Security Operations Centre (C-SOC) (3) Cyber Security Incident Reporting (CSIR).

Payment Services

Payment processing services include authorisation, funding, and settling of a transaction.

ALL SERVICES

PCI DSS Training

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that companies who accept, process, store or transmit credit card information maintain a secure environment.

Cyber Security

It consist of medical professionals, organizations, and ancillary health care workers who provide medical care to those in need.

Spear Phishing

“Spear phishing” is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.

Certified Ethical Hacker

A Certified Ethical Hacker is a professional who knows how to investigate the vulnerabilities and weaknesses of a system and try to defend it from malicious attacks.

Security Program Advisory

Security advisory professionals help small organizations that don't have the resources for an internal team and large organizations that need complex guidance and support. As data stores scale upward, security advisory providers insights to optimize cyberdefense efficiency.

ISACA

An ISACA audit is an independent assessment of a company's information systems, processes, and controls to ensure compliance with established standards.

CISSP®

CISSP is an independent information security certification granted by the International Information System Security Certification Consortium, also known as (ISC)². As of July, 2022 there are 156,054 (ISC)² members holding the CISSP certification worldwide.

CISA®

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. We are designed for collaboration and partnership. Learn about our layered mission to reduce risk to the nation's cyber and physical infrastructure.

CISM®

Certified Information Security Manager (CISM) is an advanced certification that indicates that an individual possesses the knowledge and experience required to develop and manage an enterprise information security (infosec) program.

Blockchain Services

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

Blockchain Consulting

Blockchain consultants are basically the guiding lights in the mysteriously intriguing and ever-changing blockchain landscape.

Merging with token Companies

A cryptocurrency merge or blockchain merge is when a certain blockchain network like Ethereum merges a separate blockchain with the mainnet. In simpler words, it's a replacement of an old blockchain with a new blockchain protocol.

Total Block Chain Solutions

We help both startups and enterprises leverage the decentralized network built on the Blockchain and offer all the other services in IT Consulting, Development and more.

Source Code Review

A secure code review is a line-by-line analysis of the source code of an application, usually performed to find any security risks overlooked during the pre or post-development phase.

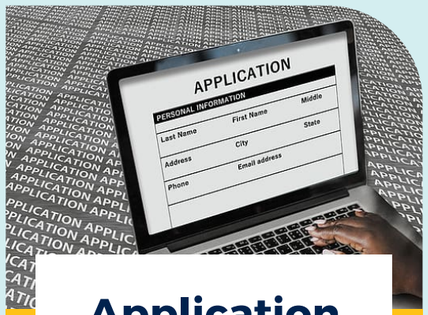
Data Privacy

Data privacy is the branch of data management that deals with handling personal data in compliance with data protection laws, regulations, and general privacy best practices.

ALL SERVICES

Certified Data Privacy Professional (CDPP)

The Certified Data Privacy Professional (CDPP) training from Infosectrain is an extensive certification course that empowers you with essential competencies to implement and manage ISO 27701 based Privacy Framework.



Application

An application, also referred to as an application program or application software, is a computer software package that performs a specific function directly for an end user or, in some cases, for another application. An application can be self-contained or a group of programs.

Mobile App Development

Mobile application development is the process of creating software applications that run on a mobile device, and a typical mobile application utilizes a network connection to work with remote computing resources.

AI App Development

Artificial intelligence in mobile apps has the potential to greatly enhance the user experience. By utilizing AI techniques, developers can create apps that are more efficient, accurate and personalized for the user. Our team is constantly looking for ways to ensure that our final solution meets your requirements.

Beta testing of software and applications

In software development, a beta test is the second phase of software testing in which a sampling of the intended audience tries the product out. Beta is the second letter of the Greek alphabet. Originally, the term alpha test meant the first phase of testing in a software development process.

AI Chatbot

At the most basic level, a chatbot is a computer program that simulates and processes human conversation (either written or spoken), allowing humans to interact with digital devices as if they were communicating with a real person.

Meta verse

Metaverse is a virtual-reality space in which users can interact with a computer-generated environment and other users.

Business Advisory

A business advisory is a professional financial service that gives business advice and helps make strategic plans with business owners or decision makers of a company or organisation.

Market Research and Intelligence

Market research deals specifically with your company, marketing strategy, and product line. Market intelligence is information about the market itself, not your specific positioning necessarily.

Business Process Re-Engineering

Business Process Reengineering is the radical redesign of business processes to achieve dramatic improvements in productivity, cycle times, quality, and employee and customer satisfaction.

3rd Party security Audit/assessment

The Third Party Security Assessment (TPSA) is a due diligence activity to gain a level of assurance with the overall security of our suppliers. It can be treated as part of the procurement process or carried out with existing suppliers.

Tech Advisory

A technical advisor works with a business when a project falls outside of their area of expertise. In this career, you may work with a team on specific projects, or you may act as a consultant on company development or expansion into a new sector.

CISO As a service

CISO as a service (vCiso) is a model that delivers third-party chief information security officer (CISO) and information security leadership services. These third-party providers manage security programs remotely, providing organizations with access to expertise they do not have in-house.

ALL SERVICES

Data protection officer as-a-service (Virtual DPO)

The DPO ensures that the organization complies with relevant data protection laws and regulations. They assess data processing activities, conduct audits, and implement appropriate policies and procedures to mitigate risks.

A smart contract Audit For Crypto companies

A smart contract audit involves a detailed analysis of the contract's code to identify security issues and incorrect and inefficient coding, and to determine ways to resolve the problems. The audit process is an important part of ensuring the security and reliability of blockchain applications.

Business Process Re-Engineering

Business Process Reengineering is the radical redesign of business processes to achieve dramatic improvements in productivity, cycle times, quality, and employee and customer satisfaction.

Cybersecurity for Fintechs

It contains policies and frameworks that can help organizations worldwide establish and maintain protected data management systems. Its policies include Cryptography, Access Control, Clear Screen, and Informational Security.

CISO As a services(Virtual CISO)

A Virtual Chief Information Security Officer is an outsourced security advisor whose responsibilities varies depending upon your business needs. A virtual CISO can be a cost-effective approach to having the access your company needs to high-end cybersecurity professionals.

Open Source Scanning (OSS)

Open source scanning is the process of using open source scanning tools to find vulnerabilities in systems and software. These tools are run on a device to: Identify the device's operating system. Identify software installed on the device. Identify accounts, open ports, and other details as specified.

ISO SERVICES

ISO (International Organization for Standardization) is an independent, non-governmental, international organization that develops standards to ensure the quality, safety, efficiency of products, services, and systems.

ISO 27001

Information Security

ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes and technology.

ISO 20000-1

IT Services

ISO/IEC 20000-1 provides a framework and a systematic approach to plan, implement, operate, review, maintain and improve an IT service management system.

ISO 27701

Privacy Information Management System

Two main objectives of ISO 27701 are to protect private information assets and to demonstrate compliance with privacy and data protection regulations – regardless of location or industry.

ISO 22301

Business Continuity

ISO 22301 is designed to help organizations prevent, prepare for, respond to and recover from unexpected and disruptive incidents.

ISO/IEC 19770-1:2017

IT Asset Management System

ISO/IEC 19770-1:2017 specifies requirements for an IT asset management system within the context of the organization.

ISO 44001

Collaborative Business Relationship Management Systems

The behaviour, organisational culture & management processes providing a common platform to underpin sustainable business relationships & harness the benefits of collaborative working.

ISO 24143:2022

Information Governance

It applies to organisations of all sizes in all sectors, including public and private companies, government entities, and not-for-profit organisations.

ISO/IEC 23053:2022

Artificial Intelligence (AI) Systems Using Machine Learning (ML)

This document establishes an Artificial Intelligence (AI) and Machine Learning (ML) framework for describing a generic AI system using ML technology.

ISO/IEC/IEEE 12207:2017

Systems and Software Engineering

This is a common framework for software life cycle processes, with well-defined terminology, that can be referenced by the software industry.

ISO 55001

Asset Management

ISO 55001 is an asset management system standard, the main objective of which is to help organizations manage the lifecycle of assets more effectively.

ISO 44001

Data Center Facilities and Infrastructures

The international standard ISO/IEC 22237 lays the basic groundwork for data centers being planned, built and operated in future based on the same principles worldwide.

ISO/IEC 38500

IT Governance standard

International standard for the corporate governance of information technology, and provides guidance to those advising, informing or assisting directors on the effective and acceptable use of information technology (IT) within the organisation.

OUR CLIENTS

Drake & Scull

EY

KPMG

TENDERD

مستشفى برايم
PRIME HOSPITAL

MESOFT
Business Solutions

thyssenkrupp

BEINEX

مدرسة الإبداع العلمي الدولية
INTERNATIONAL SCHOOL OF CREATIVE SCIENCE
MUWAILEH

tncGROUP
BLOCKCHAIN IT SOLUTIONS

GEMS
EDUCATION

MARC ELLIS

GROUP MAG
Since 1978

Gargash

ARMANI / CASA

CHEC
China Harbour Engineering Company Ltd.

الإمارات للمزادات
EMIRATES AUCTION

مبادلة
MUBADALA

SIRVA®

IHS
Towers of strength

SAIPEM

ALUCOR

CIC

ROVE
HOTELS

CLAX® Italia

novomed

CONTACT US

USA

Nathan Labs LLC
3166 Geary Street,
#1027 San Francisco,
CA 94108,
United States.

DUBAI

Nathan Labs LLC
Suite 29, Marina plaza,
Dubai Marina, Dubai,
United Arab Emirates.
P.O. Box: 79998
M: (+971) 50 258 5024

INDIA

Nathan Labs LLC
The Executive Zone,
Shakti Towers – 1,
766, Anna Salai,
Chennai - 600002.
Tamil Nadu, India.