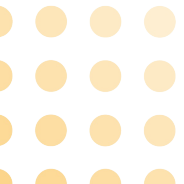


USE CASES

SYNCLATURE CONSULTANCY PVT. LTD.

12 MAY 2020





BY INDUSTRY & SECTOR

AUTOMOTIVE INDUSTRY

1. **Large Automotive Dealership** | Fraud Detection and Investigation

BANKING, FINANCIAL SERVICES & INSURANCE (BFSI)

2. **Private Indian Bank** | Cyberawareness and Digital Forensics
3. **Large Private Sector Bank** | Application Security Testing
4. **South African Bank** | Cybersecurity Framework in Bank
5. **French Bank** | Cybersecurity Framework in Bank
6. **UAE Bank** | Cybersecurity Framework in Bank
7. **Large Commodity Exchange** | Application Security Testing
8. **Commodity Exchange** | Network Security Testing
9. **Insurance Company** | IT General Controls and IT Application Controls
10. **Insurance Company** | IT General Controls and IT Application Controls
11. **Large Indian NBFC** | Endpoint Security Solution Implementation
12. **NBFC** | IT General Controls and IT Application Controls



BY INDUSTRY & SECTOR

MANUFACTURING INDUSTRY

13. **Winery** | Business Continuity Management
14. **Fast-Moving Consumer Goods (FMCG)** | Investigation of Man-In-The-Middle (MITM) Attack
15. **Online Industrial E-Marketplace** | Application Security Testing
16. **Manufacturer of Fluid Systems** | Email Security
17. **Manufacturer of Water Treatment Components and Spares** | Application Security Testing
18. **Manufacturer of Fire Retardant** | IT General Controls and IT Application Controls

PROFESSIONAL SERVICES

19. **Chartered Accountants** | Statutory Audit | IT General Controls and IT Application Controls
20. **Chartered Accountants** | Statutory Audit | Cybersecurity Framework in Bank
21. **Law Firm** | Information Security Management System
22. **Risk Advisory Firm** | Application Security Testing



INDEX

BY INDUSTRY & SECTOR

IT SERVICES

23. **Cloud Infrastructure** | Information Security Management System
24. **Digital Marketing Agency** | Website Security Testing
25. **Large IT & Cybersecurity Company** | Incident Management
26. **Security Systems and Surveillance** | Data Recovery
27. **Software & IT Services Provider** | Information Security Management System
28. **Software & IT Services Provider** | Network Security Testing
29. **System Integrator** | Information Security Management System
30. **UK-based Cybersecurity Provider** | Endpoint Security Solution Implementation

FINTECH

31. **Digital Gold Fintech Startup** | Application Security Testing
32. **Data Analytics Fintech Startup** | Application Security Testing
33. **Hospitality Data Analytics** | Information Security Management System
34. **Payment Industry Fintech** | Payment Card Industry Data Security Standard (PCS DSS)
35. **Geo-location Intelligence Fintech** | Investigation of Ransomware Incident
36. **Digital Consumer Lending Platform** | Virtual Information Security Officer (VISO)
37. **Digital Payments Service Provider** | Authentication User Agency (AUA) Audit



BY INDUSTRY & SECTOR

HEALTHCARE AND FITNESS

- 38. **Healthcare Services** | Application Security Testing
- 39. **Healthcare Revenue Solutions** | Application Security Testing
- 40. **Healthcare Services** | Application Security Testing
- 41. **Healthcare Services** | Digital Forensics
- 42. **Primary & Preventive Healthcare** | Virtual Information Security Officer (VISO)
- 43. **Fitness and Dance Academy** | Network Security Assessment
- 44. **Fitness Studio** | Network Security Assessment

MARITIME INDUSTRY

- 45. **Personnel Management Company** | Application Security Testing

PETROCHEMICAL INDUSTRY

- 46. **Large Petrochemical Company** | Assessment of Industrial Control Systems

RESTAURANT

- 47. **Fine Dine Restaurant** | Network Security Assessment



BY INDUSTRY & SECTOR

PRINTING INDUSTRY

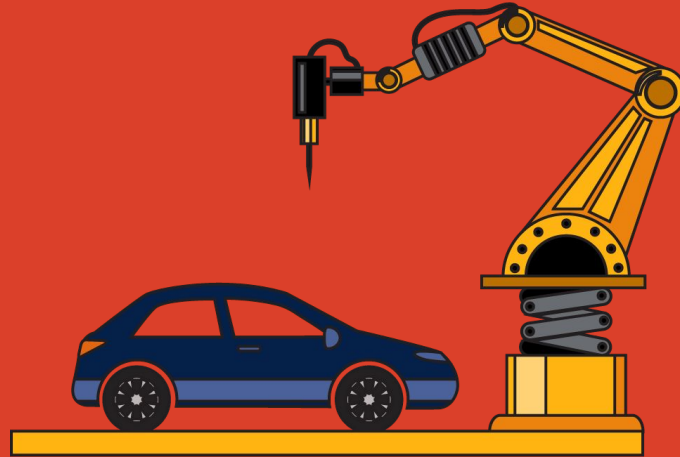
- 48. **Card Printing Press** | Information Security Management System
- 49. **Packaging Printing Press** | Ransomware Incident Investigation | Information Security Management System

TELECOM INDUSTRY

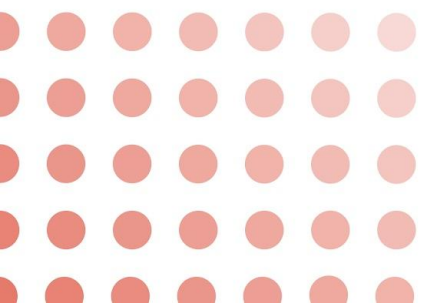
- 50. **Telecom Giant in the Middle East** | Incident Management
- 51. **Large Telecom Company in India** | Endpoint Security Solution Implementation

PHARMACEUTICAL INDUSTRY

- 52. **Pharmaceutical Trader** | Investigation of Man-In-The-Middle (MITM) Attack



AUTOMOTIVE INDUSTRY





LARGE AUTOMOTIVE DEALERSHIP

One of the largest automotive dealerships in India that has been operating for over 20 years, present in over 38 cities with multiple brands like BMW, Mercedes, Jaguar, Jeep, Fiat, Skoda etc. across the states of Gujarat, Maharashtra, New Delhi, Madhya Pradesh and West Bengal.

Fraud Detection and Investigation

- Conducted a fraud audit to discover fraudulent activity. The auditors used specific tools and data analysis techniques to discover fraud schemes and business irregularities.
- Forensic audit was conducted to discover, disclose and follow up on fraud and crime. Evidence for review by law enforcement and judicial authorities was developed.

Liaising with law enforcement

Liaising with the local law enforcement

authorities to communicate and coordinate their activities.

Litigation support

Providing information and support to the client, legal professionals concerning the case and law to aid in research efforts.

Corrective Actions

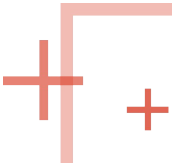
Implementing policies and procedures to establish internal controls for fraud prevention and detection.

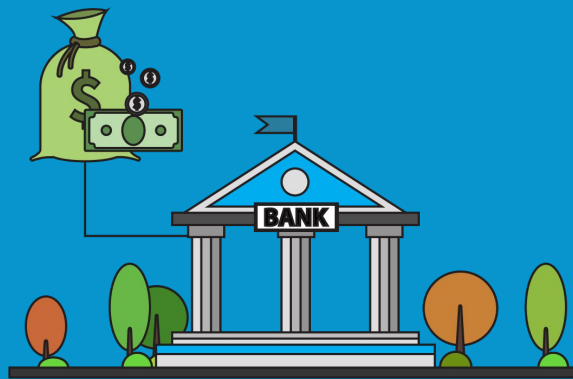
2019-20

6 months

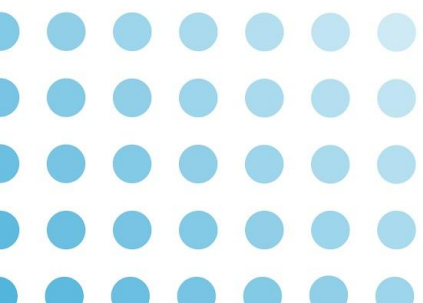


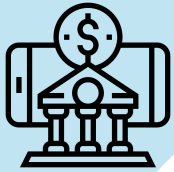
Fraud Detection and Investigation





BANKING, FINANCIAL SERVICES & INSURANCE (BFSI)





PRIVATE INDIAN BANK

A large commercial private sector bank with 334 branches across 19 states and 3 union territories catering to approximately 600,000+ customers. It has contemporary technology and infrastructure including state of the art internet banking for personal as well as business banking customers.

Information Security Awareness for Banks

Trainings and awareness for:

- Board Members
- Senior Management
- IT Teams
- Employees

Digital content to simplify the concepts of information security:

- Infographics
- Posters
- Flyers
- Videos
- Calendars
- Screensavers

- Multiple Choice Questions (MCQs)
- Bookmarks

Digital Forensics

Conduct forensic services on the bank's IT infrastructure on ad-hoc basis as a part of the bank's IR readiness framework. It involved the following activities:

- On-site imaging; evidence collection
- Analysis and Investigation
- Table-top exercises and first responders' training for employees

2017-20

Annual Retainer



Cyberawareness



Digital Forensics



LARGE PRIVATE SECTOR BANK

One of the largest private sector bank headquartered in Mumbai that offers banking products and financial services for corporate and retail customers through a variety of delivery channels and specialised subsidiaries in the areas of personal finance, investment banking, general insurance, life insurance and wealth management.

Application Security & Process Testing

The activity involved the testing of following applications:

- Workflow and Analytical tool with rules and guidelines defined by RBI for AML activities. Based on these rules, the system generates alerts in case of any suspicious transaction.
- Application for custodial business.
- Debit card management and reconciliation system.
- Application for Wealth Management business

- Application for retail liabilities for mutual fund transactions and related processes used to maintain mutual fund investments of customers
- Application for approving and clearing all trades done by Foreign Institutional Investors (FII) in F&O segment.

Benefits

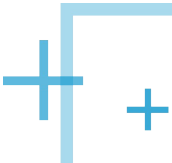
Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

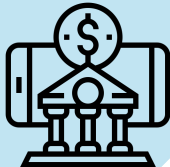
2017-18

8 months



Application Security Testing





SOUTH AFRICAN BANK

One of the largest financial services groups by market capitalisation in Africa with its corporate and investment banking arm operating in over 25 African countries, UK, India and China.

Cybersecurity assessment based on RBI Cybersecurity Guidelines

Review of the bank's IT infrastructure regarding the following aspects covered under the notification

'Cyber Security Framework in Banks'

RBI/2015-16/418

DBS.CO/CSITE/BC.11/33.01.001/2015-16

June 2, 2016:

- Cybersecurity policy
- Arrangement for continuous surveillance
- IT architecture

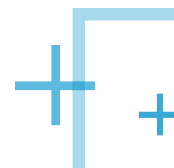
- Network and database security
- Protection of customer information
- Cyber Crisis Management Plan
- Cybersecurity preparedness indicators
- Sharing of cybersecurity incidents with the RBI
- Supervisory reporting framework
- Gap assessments
- Awareness among stakeholders, top management and board

2019

1 month



Cybersecurity
Framework in Bank





FRENCH BANK

A major player in wealth management, offering its services to a domestic and international clientele, drawing on the expertise of its specialist teams in wealth engineering, investment and financing solutions.

Cybersecurity assessment based on RBI Cybersecurity Guidelines

Review of the bank's IT infrastructure regarding the following aspects covered under the notification

'Cyber Security Framework in Banks'

RBI/2015-16/418

DBS.CO/CSITE/BC.11/33.01.001/2015-16

June 2, 2016:

- Cybersecurity policy
- Arrangement for continuous surveillance
- IT architecture

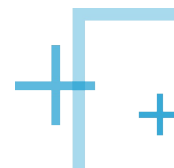
- Network and database security
- Protection of customer information
- Cyber Crisis Management Plan
- Cybersecurity preparedness indicators
- Sharing of cybersecurity incidents with the RBI
- Supervisory reporting framework
- Gap assessments
- Awareness among stakeholders, top management and board

2019

1 month



**Cybersecurity
Framework in Bank**





UAE BANK

One of the world's largest institutions, offering an extensive range of tailor-made solutions, and products and services, to provide a customised experience. Through its strategic offerings, it looks to meet the banking needs of customers across the world via its market-leading Corporate and Investment Banking and Personal Banking franchises.

Cybersecurity assessment based on RBI Cybersecurity Guidelines

Review of the bank's IT infrastructure regarding the following aspects covered under the notification

'Cyber Security Framework in Banks'

RBI/2015-16/418

DBS.CO/CSITE/BC.11/33.01.001/2015-16

June 2, 2016:

- Cybersecurity policy
- Arrangement for continuous surveillance
- IT architecture

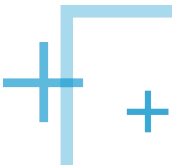
- Network and database security
- Protection of customer information
- Cyber Crisis Management Plan
- Cybersecurity preparedness indicators
- Sharing of cybersecurity incidents with the RBI
- Supervisory reporting framework
- Gap assessments
- Awareness among stakeholders, top management and board

2019

1 month



Cybersecurity Framework in Bank





LARGE COMMODITY EXCHANGE

A state-of-the-art, commodity derivatives exchange that facilitates online trading of commodity derivatives transactions, thereby providing a platform for price discovery and risk management. It operates under the regulatory framework of Securities and Exchange Board of India (SEBI).

Security Testing of 5 internal applications in accordance with OWASP ASVS 3.0 standard

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

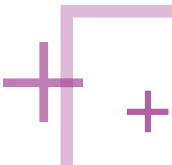
Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

2019

4 months



Application Security Testing





COMMODITY EXCHANGE

A semi-private entity responsible for clearing and settlement services of all trades executed on the exchange and is committed to provide a robust and transparent risk management platform for the collective benefit of the agro-ecosystem.

Network Security Assessment of wireless and wired LAN infrastructure

Conducted Vulnerability Assessment and Penetration Testing of the wireless network infrastructure:

- Wired LAN comprising of LAN switches and access points

Defined rational, quantifiable and business critical objectives in order to:

- Identify core issues with respect to their wired and wireless LAN.

The assessment covered OWASP, OSSTMM, WASC and NSA security guidelines

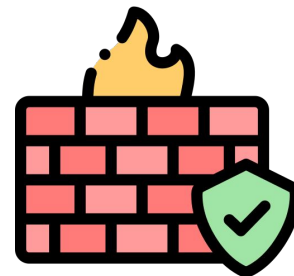
Value Addition

Compiled a concrete plan with actionable steps and execute it successfully in order to address all the core issues to attain:

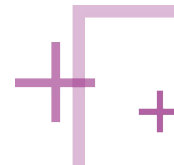
- Confidentiality, Integrity, Availability and Compliance of its information systems
- Build a highly secure and resilient WLAN infrastructure

2019

3 months



Network Security Testing





INSURANCE COMPANY

The Company offers complete range of general insurance products ranging from Motor, Health, Travel, Home and Personal Accident in the retail space and customized products like Property, Marine and Liability Insurance in the corporate space.

IT General Controls (ITGC) and IT Application Controls (ITAC) audits of clients covering, but not limited to, the following areas:

- Access Management
- Asset Management
- Change Management
- Maker-Checker Controls
- Application Security
- Backup and Restoration
- Audit Trails
- Business Continuity
- Disaster Recovery

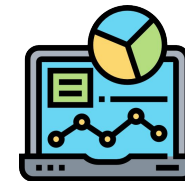
- Acceptable Usage
- Anti-virus Policy
- Email Security
- Incident Management
- License Management
- Log Management
- Password Management

Advanced Threat Prevention (ATP) solution implementation

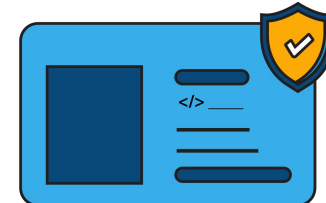
Implementation and management of endpoint security solution Advanced Threat Protection (ATP) module.

2017-20

Ad Hoc Projects



IT General Controls



IT Application Controls



INSURANCE COMPANY

The organisation constantly try to create solutions to make life insurance plans easy, affordable, and suitable for every stage of your life. At the same time, each day, they are working to make claims process quick and simpler for your family.

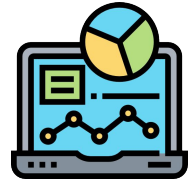
IT General Controls (ITGC) and IT Application Controls (ITAC) audits of clients covering, but not limited to, the following areas:

- Access Management
- Asset Management
- Change Management
- Maker-Checker Controls
- Application Security
- Backup and Restoration
- Audit Trails
- Business Continuity
- Disaster Recovery

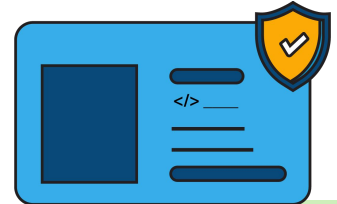
- Acceptable Usage
- Anti-virus Policy
- Email Security
- Incident Management
- License Management
- Log Management
- Password Management

2019-20

2 months



IT General Controls



IT Application Controls



LARGE INDIAN NBFC

It is a deposit-taking housing finance company, headquartered in Mumbai with branches in major cities across India. It was established to enable access to economical housing finance to the lower and middle income groups in semi-urban and rural parts of India.

On-site implementation of endpoint security solution with Advanced Threat Protection (ATP) across 2000 endpoints.

- One onsite resource with relevant technical and soft skills competent to handle the assigned project work.
- On-site support for ATP, Encryption and Authentication.
- Coordinate with teams for escalations and troubleshooting of issues.
- Single Server Deployment
- Fine tuning and future upgrade of the product during contract period.

- Troubleshoot client end issues pertaining to solution
- Installation of clients components as applicable
- On-site solutions management and support post-implementation
- Hand holding and internal training

2017-18

4 months



Endpoint Security
Solution
Implementation



NBFC

The company provides a wide range of products and services to fit all needs and demands for a better living - Two Wheeler Finance, Housing Finance, Mutual Fund, Farm Equipment Finance, Micro Loans, Real Estate Finance, Infrastructure Finance.

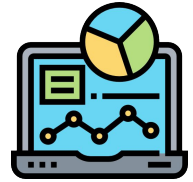
IT General Controls (ITGC) and IT Application Controls (ITAC) audits of clients covering, but not limited to, the following areas:

- Access Management
- Asset Management
- Change Management
- Maker-Checker Controls
- Application Security
- Backup and Restoration
- Audit Trails
- Business Continuity
- Disaster Recovery

- Acceptable Usage
- Anti-virus Policy
- Email Security
- Incident Management
- License Management
- Log Management
- Password Management

2019-20

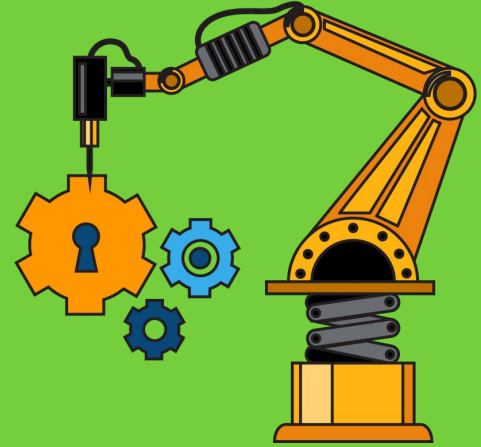
2 months



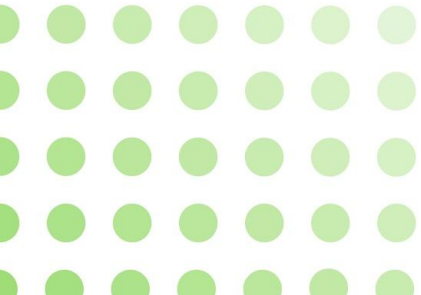
IT General Controls



IT Application Controls



MANUFACTURING INDUSTRY





WINERY

Indian subsidiary of a French conglomerate in the alcoholic beverages industry, producer of world-class, premium quality sparkling wine.

Business Continuity Management

Reviewing the existing business continuity plan and modifying it based on the current business processes covering the following functions:

- Vineyards
- Contracted vineyards
- Wine-making
- Laboratory
- Production
- Storage
- Maintenance
- Logistics
- Administration

Conducting a Process Failure Mode and Effects Analysis (PFMEA) and risk assessment to identify existing controls and treating risks as per the risk treatment plan.

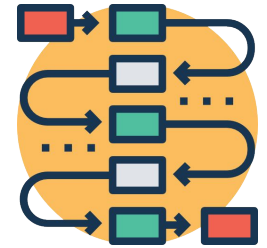
Developing the Emergency Response and Crisis Management plan for the winery.

Benefits

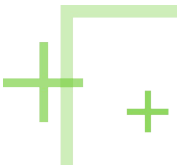
The winery found value in enhancing the process controls and being prepared for untimely disruptions with the help of business continuity plans for various scenarios.

2019

6 months



Business Continuity Management





FAST-MOVING CONSUMER GOODS (FMCG)

The company has created a moat for itself over the last two decades as India's most diversified and trusted FMCG contract manufacturers for marquee brands in India. It specializes in setting up one-stop contract manufacturing solutions and the ability to consistently deliver quality products. It offers flexible business models suitable for any size of customer and across product categories.

Investigation of Man-In-The-Middle (MITM) Attack

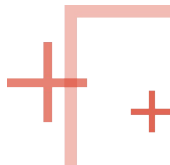
- The client was a victim of cyber attack that resulted in a transfer of a substantial amount to the attacker's account in London.
- An analysis of email/web server led to the discovery of active email forwarders. These forwarders, unknown to the client, were possibly used by the attacker which may have resulted in data leakage.
- The cpanel logs, from the email hosting provider revealed that it was accessed from multiple locations around the world. Thus we can infer that a VPN may have been possibly used by the attacker to access the cpanel.
- The analysis of email headers revealed a particular email address which can be traced back to a pharma company. This was probably used to send out phishing emails. This can be further investigated to determine the source of the attack.
- The domains used to carry out the attack were registered in different names, under different aliases. False information was used for the domain registration by the attacker.

2019

1 month



Investigation of MITM
Attack





ONLINE INDUSTRIAL E-MARKETPLACE

An online industrial e-Marketplace is bridging the gap between buyers & sellers of excess/unused inventory by connecting them online which gives them, ease of access and maintains transparency in the whole process. Sellers recover significant amount out of their dead investment & buyers get amazing deals at best prices.

Web Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

2018

1 month



Application Security
Testing



MANUFACTURER OF FLUID SYSTEMS

Started by a young entrepreneur in 1988, today it is a world leader in the design and manufacture of mechanical fluid systems, process equipment and engineering services. They export over 70% of their products to countries around the globe and are suppliers to major Oil and Gas, Power, Chemical and Fertilizer companies.

Security of Email Services

The following recommendations were provided:

- Password management of affected user email accounts.
- Deploy Multi Factor Authentication on targeted users, privileged users, and users who access sensitive information.
- Check to see if mailbox forwarding was enabled, and if so to who (document the external addresses to verify the validity).
- Check message trace logs.

- Disable forwarding via Transport Rule, and create an alert in Security and Compliance Center when someone tries to create a forwarding inbox rule (Indicator of Compromise)
- Check if Mailbox Auditing is enabled.
- Use Message Trace to see who received emails from the attacker's email address.
- Deploy ATP Anti-Phishing
- Disable Legacy Authentication
- Disable POP/IMAP for future mailboxes and current mailboxes.

2019

1 month



Email Security



MANUFACTURER OF WATER TREATMENT COMPONENTS AND SPARES

They supply vast range of water treatment plant's components to OEMs and end users at economical and affordable rates. Also supply a variety of water treatment components, providing wide range of Components and spares gives advantage and freedom to client to choose products and spares as per their requirements.

Web Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

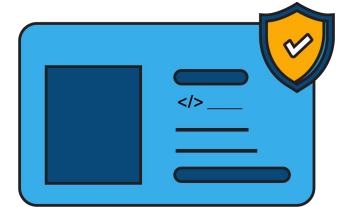
- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

2019

1 month



Application Security Testing



MANUFACTURER OF FIRE RETARDANT

One of the Largest Manufacturer of Antimony Trioxide in the domestic market. Uses Eco-friendly Thermic process. Provides Sophisticated Quality Control and R&D.

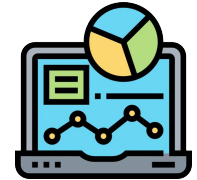
IT General Controls (ITGC) and IT Application Controls (ITAC) audits of clients covering, but not limited to, the following areas:

- Access Management
- Asset Management
- Change Management
- Maker-Checker Controls
- Application Security
- Backup and Restoration
- Audit Trails
- Business Continuity
- Disaster Recovery

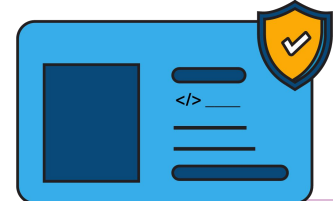
- Acceptable Usage
- Anti-virus Policy
- Email Security
- Incident Management
- License Management
- Log Management
- Password Management

2019-20

4 months



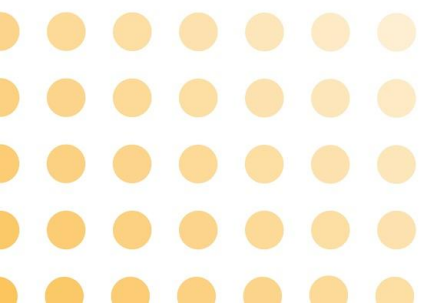
IT General Controls



IT Application Controls



PROFESSIONAL SERVICES





CHARTERED ACCOUNTANTS

One of the top five Chartered Accountancy firms in India, working in the field of Assurance, Direct Tax, Transfer Pricing, Indirect Tax and Risk Advisory.

IT General Controls (ITGC) and IT Application Controls (ITAC) audits of clients covering, but not limited to, the following areas:

- Access Management
- Asset Management
- Change Management
- Maker-Checker Controls
- Application Security
- Backup and Restoration
- Audit Trails
- Business Continuity
- Disaster Recovery

- Acceptable Usage
- Anti-virus Policy
- Email Security
- Incident Management
- License Management
- Log Management
- Password Management

Value Addition

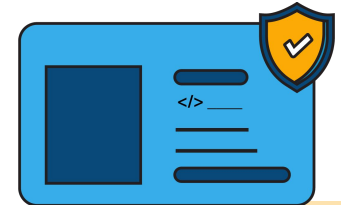
Give assurance to the chartered accountancy firm regarding the IT General Controls and Application Controls of their clients as a part of the statutory audit and compliance.

2019-20

Annual Retainer



IT General Controls



IT Application Controls



CHARTERED ACCOUNTANTS

One of the oldest accountancy firms in the country, ranking amongst the top 5 Indian chartered accountants, associated itself with other quality professionals from related fields such as lawyers, company secretaries, IS auditors, cost accountants, excise and sales tax consultants etc. providing a one stop destination for clients to address their queries.

Cybersecurity assessment of international banks based on RBI Cybersecurity Guidelines

Guidelines

Review of the bank's IT infrastructure regarding the following aspects covered under the notification 'Cyber Security Framework in Banks' RBI/2015-16/418 DBS.CO/CSITE /BC.11/33.01.001/2015-16 (June 2, 2016):

- Cybersecurity policy
- Arrangement for continuous surveillance
- IT architecture
- Network and database security
- Protection of customer information

- Cyber Crisis Management Plan
- Cybersecurity preparedness indicators
- Sharing of cybersecurity incidents with the RBI
- Supervisory reporting framework
- Gap assessments
- Awareness among stakeholders, top management and board

●

Value Addition

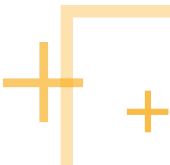
Give assurance to the chartered accountancy firm regarding the cybersecurity controls of their clients as a part of the statutory audit and compliance.

2019

3 months



Cybersecurity
Framework in Bank





LAW FIRM

Their service offerings include setting up of businesses, commercial contracts (including property documentation), mergers and acquisitions (M&A) documentation and negotiation, corporate advisory, (listed and unlisted) statutory and regulatory compliance, foreign exchange law advisory, international and domestic arbitration, disputes (including dispute avoidance), and dispute management.

Implementation of Information Security Management System (ISMS)

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security
- Asset Management

- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

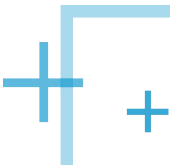
Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

2018

4 months



Information Security Management System





RISK ADVISORY FIRM

A CERT-In empanelled information security and risk advisory firm based out of Mumbai.

Security assessment of application, custom-built APIs, SDKs and mobile applications of risk advisory firm's clients

Conducted a vulnerability assessment with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered.

Value Addition

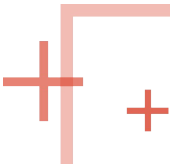
- Strategic consulting for management to achieve internal governance and business objectives.
- Identification and evaluation of security technologies.
- Support with third-party and client audits.

2018-20

Ad Hoc Projects

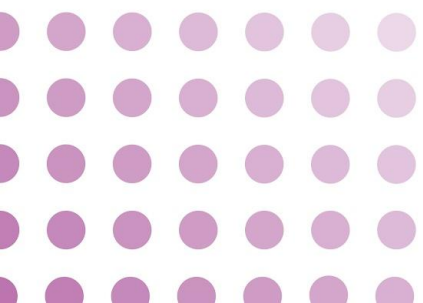


Application Security Testing





IT SERVICES





CLOUD INFRASTRUCTURE

They provide customized managed hosting solutions & innovative cloud services and to companies with a critical internet component. A medium sized system integrator with offices in Singapore, Dubai, North America and India.

Implementation of Information Security Management System (ISMS)

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security
- Asset Management

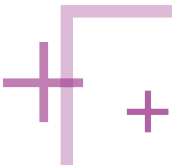
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

2019

3 months



Information Security Management System





DIGITAL MARKETING AGENCY

A mid-sized digital marketing company that serves some of the Fortune 500 companies and help them build creative, contextual and content engagement cycles for you to present yourself online to your customer.

Security Testing of web application belonging to a oil and lubricant giant

Conducted a vulnerability assessment activity for a website of the digital marketing agency's client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

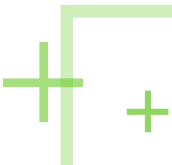
Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

2019

1 week



Website Security Testing





LARGE IT & CYBERSECURITY COMPANY

A CERT-In empanelled global IT and cybersecurity company with 8000+ customers, 500+ certifications in 30+ countries.

2019

4 months

Incident Response for client in Saudi Arabia

Information Gathering

- Team roles and responsibilities
- Incident Timeline
- Personnel Interviews

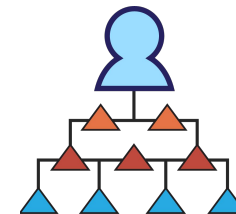
Detect

- Identify threat indicators
- Categorize incident
- Conduct Scans / Forensics

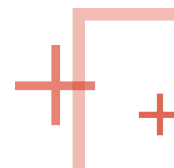
Analyze

- Define risk factors
- Log and Evidence Collection
- Data Capture

- Determine Patch Methods
- ### Contain
- Identify all systems/user credentials at risk
 - Identify services affected
 - Identify other systems/users at risk of being compromised
 - Identify lateral movement
 - Identify tools used to detect the attack
- ### Eradicate
- Triage
 - Communicate measures to client
- ### Reporting / Lesson learned
- Final Report and Cleanup Roadmap
- ### Product identification and evaluation Security technology deployment



Incident Management





SECURITY SYSTEMS AND SURVEILLANCE

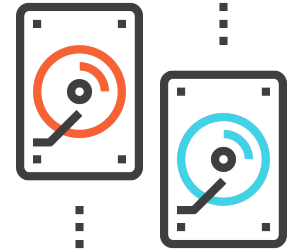
One of the largest Indian provider of IoT enabled security services. They have platform-as-a-service technologies employing AI and ML. Currently present in 4 countries and over 1100 cities.

Digital forensics and data recovery

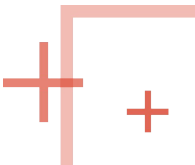
- Successfully recovered about 65% of usable data. 35% of data was corrupted because the sectors of the drive were overwritten.
- Intricate surgical process of data drive re-construction with combination tool set.
- The recovered data, along with the corrupt files, was copied to the new 2TB (destination) hard drive supplied by the client and delivered.

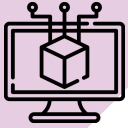
2016-17

3 months



Data Recovery





SOFTWARE & IT SERVICES PROVIDER

Medium sized customized software development company catering to clients primarily in the middle-east with end-to-end creation of technology and subsequent services, simultaneously upholding quality and integrity and reducing the customer cost.

Implementation of Information Security Management System (ISMS)

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security
- Asset Management

- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

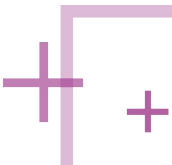
Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

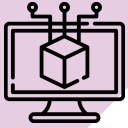
2019-20

Annual Retainer



Information Security Management System





SOFTWARE & IT SERVICES PROVIDER

Their portfolio of solutions and services includes infrastructure management services, outsourcing, system integration, Application Software development, IT consulting, IT Security Consulting, Cloud Computing, Data Science, Big Data Analytics, Industry specific products implementation & Support, Quality Assurance & Training.

Network Security Assessment of wireless and wired LAN infrastructure

Conducted Vulnerability Assessment and Penetration Testing of the wireless network infrastructure:

- Wired LAN comprising of LAN switches and access points

Defined rational, quantifiable and business critical objectives in order to:

- Identify core issues with respect to their wired and wireless LAN.

The assessment covered OWASP, OSSTMM, WASC and NSA security guidelines

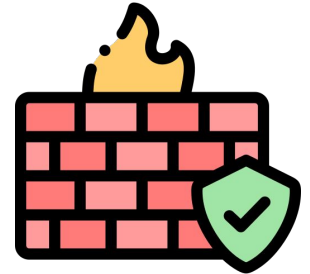
Value Addition

Compiled a concrete plan with actionable steps and execute it successfully in order to address all the core issues to attain:

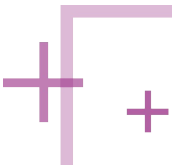
- Confidentiality, Integrity, Availability and Compliance of its information systems
- Build a highly secure and resilient WLAN infrastructure

2019

1 month



Network Security Testing





SYSTEM INTEGRATOR

IT solutions provider specializing in end to end solution in the area of IT & Telecom.

Implementation of Information Security Management System (ISMS) for client

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security
- Asset Management

- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

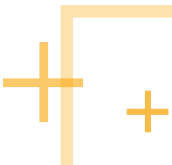
Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

2019

6 months



Information Security Management System





UK-BASED CYBERSECURITY PROVIDER

Medium sized cybersecurity solutions provider based out of England offering a unique fully managed endpoint security system that monitors network for threats in real time, backed up by a dedicated team of security analysts providing the first line of defence.

Endpoint security solution implementation with ATP and EDR

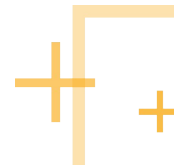
- Identify and stop malicious processes running on any device in your network
- Quarantine and infected files and allow you to track the entry point into the system, you can plug the security hole from allowing further intrusion into your network.
- Automatically disconnect machines that pose a threat of infecting more of your network allowing us to cleanse and secure your machines in isolation.
- Alert our security specialists to issues so they can manually intervene before a problem spreads.
- Immunise your machines in real time against the latest exploits and viruses in the market.
- Provide detailed reports as regularly as required to keep you abreast of the health of your network.

2018-20

Continuous

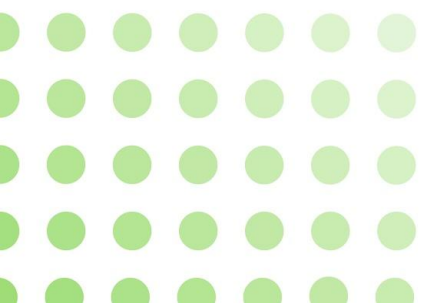


Endpoint Security
Solution
Implementation





FINTECH



SYNCLATURE 
Mitigating Business Risk



DIGITAL GOLD FINTECH STARTUP

A World Gold Council company with an online tech platform that facilitates sales of gold, digitally.

Security assessment of application platform, custom-built APIs, SDKs and mobile application

Conducted a vulnerability assessment with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered.

Value Addition

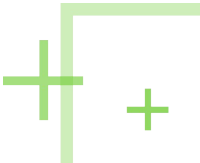
- Strategic consulting for management to achieve internal governance and business objectives.
- Identification and evaluation of security technologies.
- Support with third-party and client audits.

2017-20

Annual Retainer



Application Security Testing





DATA ANALYTICS FINTECH STARTUP

A software publishing, consultancy and supply. Software publishing includes production, supply and documentation of ready-made (non-customized) software, operating systems software, business & other applications software, computer games software for all platforms.

Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered.
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

2019

1 month

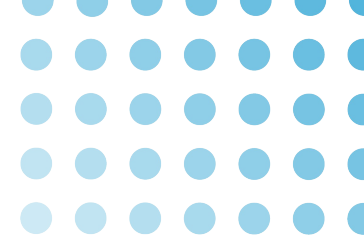


Application Security Testing



HOSPITALITY DATA ANALYTICS

A niche data analytics startup providing simplified solutions such as business intelligence, revenue optimization, cloud based intelligence to 150+ hotels, globally.



2019-20

Implementation of Information Security Management System (ISMS)

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security
- Asset Management

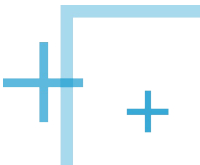
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

Annual Retainer



Information Security Management System





PAYMENT INDUSTRY FINTECH

It is a disruptive Payments & EMI Technology platform that promotes and nurtures a “deviceless” payment acceptance facility at retail outlets. The platform challenged a 3 decade old retail payment ecosystem and transformed it into a digital ecosystem thereby making it more efficient and responsive to the needs of retail outlets.

Implementation of PCI DSS and PA DSS

The following activities were part of the scope:

- Pre - Assessment Activities
- Pre - Audit Assessment Activities
- Gap Analysis Reporting
- VAPT, ASV scanning
- Remediation Assistance
- PCI Audit Training for stakeholders
- Onsite Assessment by PCI-QSA
- Discussions with stakeholders
- Remediation assistance in case of any suggestion by QSA

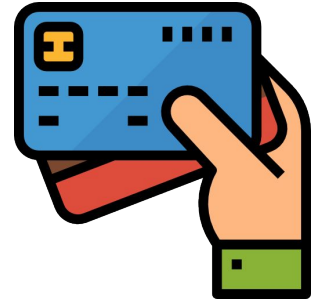
Implementing a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

Value Addition

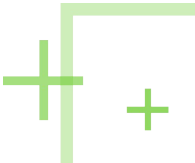
Identification and evaluation of security technologies.

2018

4 months



Payment Card Industry
Data Security Standard
(PCI DSS)





GEO-LOCATION INTELLIGENCE FINTECH

An Indo-German Joint Venture, was incorporated 2009 in Mumbai which supports various Indian Industry verticals with geo-location based intelligence, micro-market focused advanced marketing and sales technologies and individual Indian consumer data.

Investigation of ransomware incident

Conducted a vulnerability assessment activity at the client. The assignment was carried out with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

The report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Value Addition

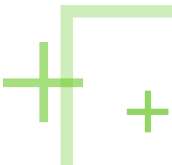
Implementation and management of endpoint security solution Advanced Threat Protection (ATP) module of BitDefender.

2018

3 months



Investigation of Ransomware Incident





DIGITAL CONSUMER LENDING PLATFORM

A digital consumer lending platform that provides consumers with easy access to affordable short-term loans. It uses intelligent data science that enables better risk-profiling of borrowers and brings consumers with no credit tracks or established credit history into the mainstream. It has an AUM (assets under management) in excess of ₹ 500 crores and has over 5.5 million registered customers with loan disbursement of over ₹ 1,100 Crores.

2019

Information Security Management System

- Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan to implement ISO 27001:2013.
- Evaluating security policies based on availability, business continuity, and compliance requirements and establishing key risk factors and security metrics.

Security Assessment

- SDK - ACR
- API
- Hybrid mobile app (APK/IPK)
- Web application
- Internal network

Virtual Information Security Officer (VISO)

- Continual security consulting
 - a. Liaising and vendor identification
 - b. Internal training and awareness for IT security
- ISMS internal audit report and certification readiness

Annual Retainer



Virtual Information Security Officer (VISO)



DIGITAL PAYMENTS SERVICE PROVIDER

It is a team of leaders with a vision to reach people from every walk of life by easy transaction solutions in banking and e-commerce, with the end goal of becoming a leading transaction service provider for all financial requirements across India.

2019

Authentication User Agency (AUA) audit based on UIDAI guidelines

The following areas were covered in the audit:

- Security Framework Policies for AUA
- Security Framework Policies for Authentication Devices
- A trusted environment must be created at the device side
- Audit logging requirements
- Aadhaar Authentication API Specification
- Best Finger Detection API Specification
- OTP Request API Specification

- Biometric Devices Specifications for Aadhaar Authentication
- Demographic Data Standards
- Biometric Data Interchange Standards
- Date & Time Format Standards
- Discovering vulnerabilities in the predefined group of information systems within the internal network.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

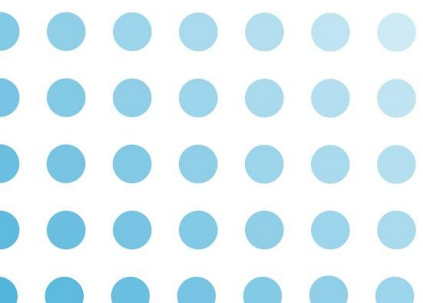
1 month



Authentication User Agency (AUA) Audit



HEALTHCARE AND FITNESS



SYNCLATURE
Mitigating Business Risk



HEALTHCARE SERVICES

The service offerings include Professional Certifications; Practice Management; EMR/EHR; Practice Marketing and Advertising; Reputation Management; Patient Engagement; Revenue Cycle Management; Private-Pay Senior Care; Compliance, Audit, Risk Management.

Web Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

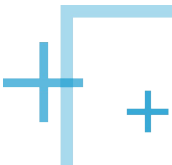
Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

2016-20

Ad Hoc Projects



Application Security Testing





HEALTHCARE REVENUE SOLUTIONS

With 40+ years of rich experience in the Healthcare, Commercial & Consumer receivables management community, our suite of services include Collections, Debt Buying, Billing, Extended Business Office, Revenue Cycle management, AR analytics, AR Technology.

Web Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

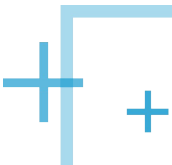
Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

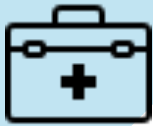
2019-20

2 months



Application Security
Testing





HEALTHCARE SERVICES

Whether it is skill development, generating employment opportunities for professionals across a broad spectrum, or reaching out a helping hand to the community; healthcare has been at the forefront of action in the decade of its existence.

Web Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information about the vulnerabilities discovered
- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

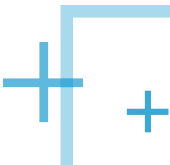
Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

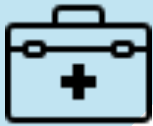
2018-19

2 months



Application Security
Testing





HEALTHCARE SERVICES

The group is forging ahead in its mission to create a better world with several upcoming projects. Currently, the group operates and manages over 1600 beds and intends to concentrate on creating a strong network of hospitals in several tier-1 and tier-2 cities across India and the sub-continent.

Digital Forensics

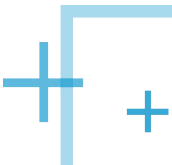
- The client was concerned about theft of confidential data and suspected one of their employees to be involved.
- The client suspected that the employee had extracted the HDD in question from the company laptop he was assigned and got it formatted due to noticeable signs of laptop back cover being opened, internal locks broken with one screw missing; local drives D and E were empty and presumed to be formatted.
- The client ran a recovery software on the source HDD and could see the directory structure and files. They tried to recover the files but were getting an error and unable to recover the said files.
- The HDD was then sent for data recovery, where a report stated that logical partitions were low level formatted. A digital forensics investigation was conducted on the hard drive, provided by the client, to extract any evidence related to data theft and erasure.

2019

3 months



Digital Forensics





PRIMARY & PREVENTIVE HEALTHCARE

It is a primary and preventive care provider that is making healthcare that much easier and convenient. They strive to make healthcare accessible to the masses through high-quality physicians and technology.

Information Security Management System

- Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan to implement ISO 27001:2013.
- Evaluating security policies based on availability, business continuity, and compliance requirements and establishing key risk factors and security metrics.

Security Assessment

- SDK - ACR
- API
- Hybrid mobile app (APK/IPK)
- Web application
- Internal network

Virtual Information Security Officer (VISO)

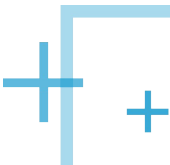
- Continual security consulting
 - a. Liaising and vendor identification
 - b. Internal training and awareness for IT security
- ISMS internal audit report and certification readiness

2019-20

Annual Retainer



Virtual Information Security Officer (VISO)





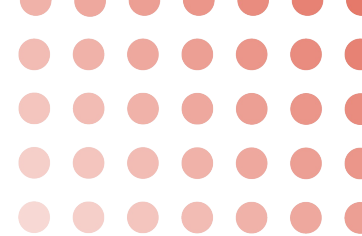
FITNESS AND DANCE ACADEMY

It is one of the most versatile dance academy in Mumbai established in the year 2005. In the very heart of Mumbai, an accomplished dance studio enriched in teaching, nurturing, and producing the finest dancers in its various dance forms of all age groups.

Network Security Assessment

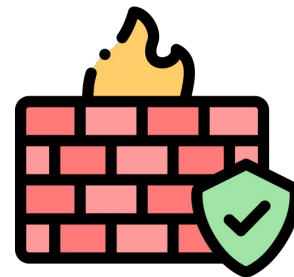
The following activities were conducted at the fitness studio:

- Network Security Assessment
- Endpoint Security Solution for prevention and detection of malware
- Active Directory: Centralization of control for all computers/laptops
- Email Service setup
- Backup of Data
- Awareness Training for Staff
- Implementation, monitoring and monthly review

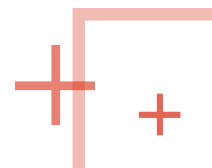


2019

Annual Retainer



Network Security
Assessment





FITNESS STUDIO

They are one of India's largest chain of health centers with over 150 ultramodern gyms spanning 80 cities across the country and a growing customer base that is currently 200,000 strong.

Network Security Assessment of wireless and wired LAN infrastructure

Conducted Vulnerability Assessment and Penetration Testing of the wireless network infrastructure:

- Wired LAN comprising of LAN switches and access points

Defined rational, quantifiable and business critical objectives in order to:

- Identify core issues with respect to their wired and wireless LAN.

The assessment covered OWASP, OSSTMM, WASC and NSA security guidelines

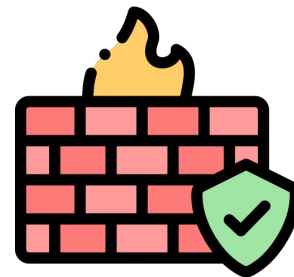
Value Addition

Compiled a concrete plan with actionable steps and execute it successfully in order to address all the core issues to attain:

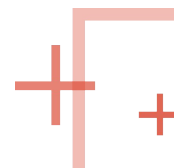
- Confidentiality, Integrity, Availability and Compliance of its information systems
- Build a highly secure and resilient WLAN infrastructure

2019

1 week

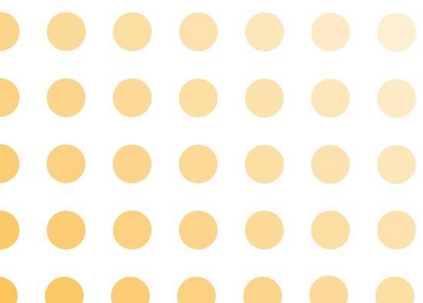


Network Security Assessment





MARITIME INDUSTRY





PERSONNEL MANAGEMENT COMPANY

A medium sized company offering services with complete personnel management of a vessel including rotational planning of ship staff, accounting, allotments, union agreements, onleave services, etc.

Web Application Security Testing

Conducted a vulnerability assessment activity for the Web Application at the client with the following goals:

- Discovering vulnerabilities in the predefined group of information systems within the web application.
- Providing a business impact arising from any discovered vulnerabilities.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities

This report contained:

- The detailed technical information

about the vulnerabilities discovered

- The risk mitigation recommendations that need to be implemented to ensure that the systems are secure from the risks arising due to the discovered vulnerabilities.

Benefits

Prevent security vulnerabilities against threats such as unauthorised access and modification during the entire application lifecycle.

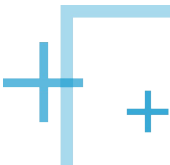
GDPR Consulting

2018

2 months

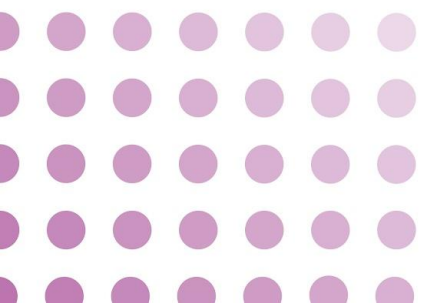


Application Security Testing





PETROCHEMICAL INDUSTRY





LARGE PETROCHEMICAL COMPANY

Based out of Kingdom of Saudi Arabia, the petrochemical giant comprises of four SBUs – Petrochemicals, Specialties, Agri-Nutrients, and Metals which support customers by identifying and developing opportunities in key end markets such as construction, medical devices, packaging, agri-nutrients, electrical and electronics, transportation and clean energy. Later acquired by ARAMCO.

On-site operational technology security assessment of 3 sites belonging to 3 listed entities in Saudi Arabia covering following standards:

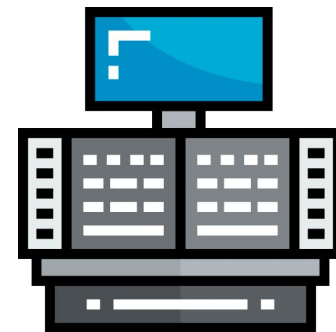
- NIST CSF
- NIST 800-82
- IEC 62443/ISA99
- HCIS Sec-12
- ISO 27001:2013

In addition, security risk assessment and grading as per client's maturity models and internal controls checklist.

Security assessment covered policy, procedures and other documentations along with testing of technical controls across IT, networks, SCADA and ICS in the client's environment.

2018

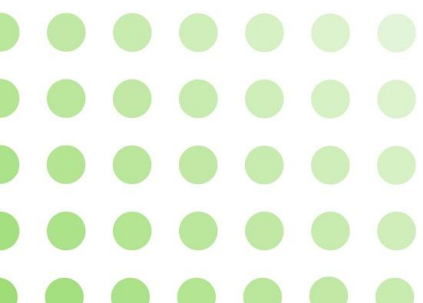
4 months



Assessment of
Industrial Control
Systems



RESTAURANT





FINE DINE RESTAURANT

Fine dine restaurant located in the suburbs of Mumbai.

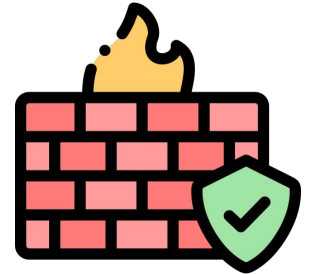
Network Security Assessment

The following activities were conducted at the fitness studio:

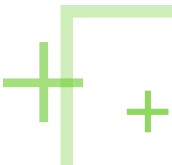
- Network Security Assessment
- Endpoint Security Solution for prevention and detection of malware
- Active Directory: Centralization of control for all computers/laptops
- Email Service setup
- Backup of Data
- Awareness Training for Staff
- Implementation, monitoring and monthly review

2019

1 week

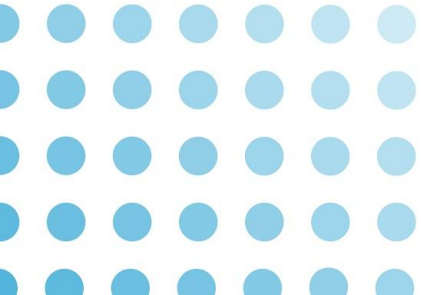


Network Security
Assessment





PRINTING INDUSTRY





CARD PRINTING PRESS

Actively involved in production and manufacturing of plastic cards for both local and foreign consumption as also associated services such as card personalization, embossing etc. One of the primary government contractors for printing several identity cards for citizens including PAN, ABPYY etc.

Implementation of Information Security Management System (ISMS)

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security
- Asset Management

- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

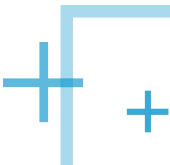
Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

2019-20

Annual Retainer



Information Security Management System





PACKAGING PRINTING PRESS

One of the oldest printing press in the country whose business is constantly evolving to meet the demands of the new generation of packaging. Specializing in carton printers, and have many other advanced technology and concepts to offer.

Ransomware incident investigation and implementation of Information Security Management System (ISMS)

Understanding the business processes and creating a risk assessment and treatment plan. Creating information security awareness in the organisation. Conducting an internal audit of the information systems and driving the corrective action plan.

Implementing ISO 27001:2013 by establishing and continually improving the following areas:

- Information Security
- Organization of Information Security
- Human Resource Security

- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Supplier Relationship
- Incident Management
- Business Continuity Management
- Compliance

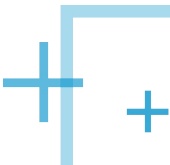
Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

2019-20

Annual Retainer

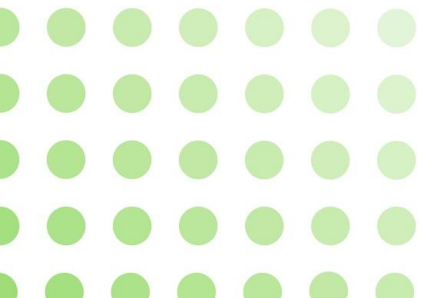


Information Security Management System





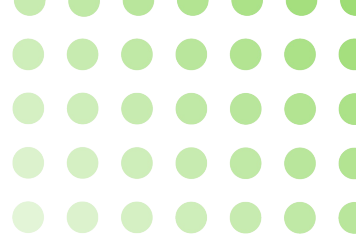
TELECOM INDUSTRY





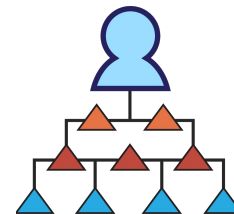
TELECOM GIANT IN THE MIDDLE-EAST

One of the largest government telecommunications company providing a variety of ICT solutions and digital services in several categories including telecommunication, IT, financial technology, digital media, cybersecurity, and other advanced digital solutions, leading the digital transformation nationally and regionally.



2019

3 months



Incident Management

Digital Forensics, Incident Response, EDR deployment and Threat Intelligence for client in Saudi Arabia

Information Gathering

- Team roles and responsibilities
- Incident Timeline

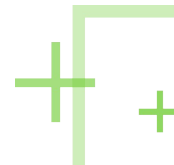
Detect

- Identify threat indicators
- Categorize incident
- Conduct Scans / Forensics

Analyze

- Define risk factors
- Log and Evidence Collection
- Data Capture

- Determine Patch Methods
- Contain**
- Identify all systems/user credentials at risk
 - Identify services affected
 - Identify other systems/users at risk of being compromised
 - Identify lateral movement
 - Identify tools used to detect the attack
- Eradicate**
- Triage
 - Communicate measures to client
- Reporting / Lesson learned**
- Final Report and Cleanup Roadmap
- Product identification and evaluation Security technology deployment**





LARGE TELECOM COMPANY IN INDIA

One of India's leading telecom service provider for voice and data across 2G, 3G and 4G platforms.

On-site implementation of endpoint security solution with Advanced Threat Protection (ATP) across 2000 endpoints.

- One onsite resource with relevant technical and soft skills competent to handle the assigned project work.
- On-site support for ATP, Encryption and Authentication.
- Coordinate with teams for escalations and troubleshooting of issues.
- Single Server Deployment
- Fine tuning and future upgrade of the product during contract period.

- Troubleshoot client end issues pertaining to solution
- Installation of clients components as applicable
- On-site solutions management and support post-implementation
- Hand holding and internal training

2017-18

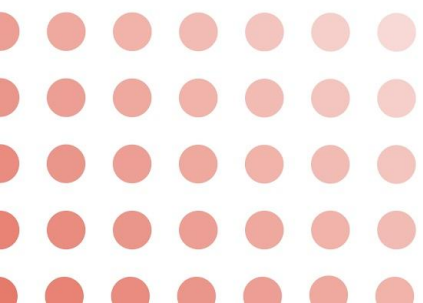
3 months



Endpoint Security
Solution
Implementation



PHARMACEUTICAL INDUSTRY



SYNCLATURE 
Mitigating Business Risk



PHARMACEUTICAL TRADER

A company catering to the entire spectrum of pharmaceutical trade starting from wholesale, tender supplies, orphan drugs, hard to find lines, cold chain lines, biologics, biosimilars, vaccines and name patient supplies. Exports to over 180 countries.

Investigation of email MITM attack

- The client was a victim of cyber attack that resulted in a transfer of a substantial amount to the attacker's account

Strategic cybersecurity consulting

- Strategic consulting for identifying, evaluating and deploying cybersecurity technologies.

Email server security

- Security assessment for email server and recommendations for email services.

Endpoint security assessment

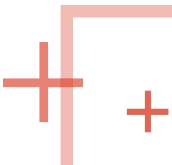
Implementation and management of endpoint security solution Advanced Threat Protection (ATP) module.

2016-17

4 months



Investigation of MITM Attack



THANK YOU



Synclature Consultancy Pvt. Ltd.
(CIN: U74999MH2016PTC282067)

Rise, 1902B, Peninsula Business Park,
G. K. Marg, Lower Parel,
Mumbai, MH 400 013.
inquiry@synclature.com

