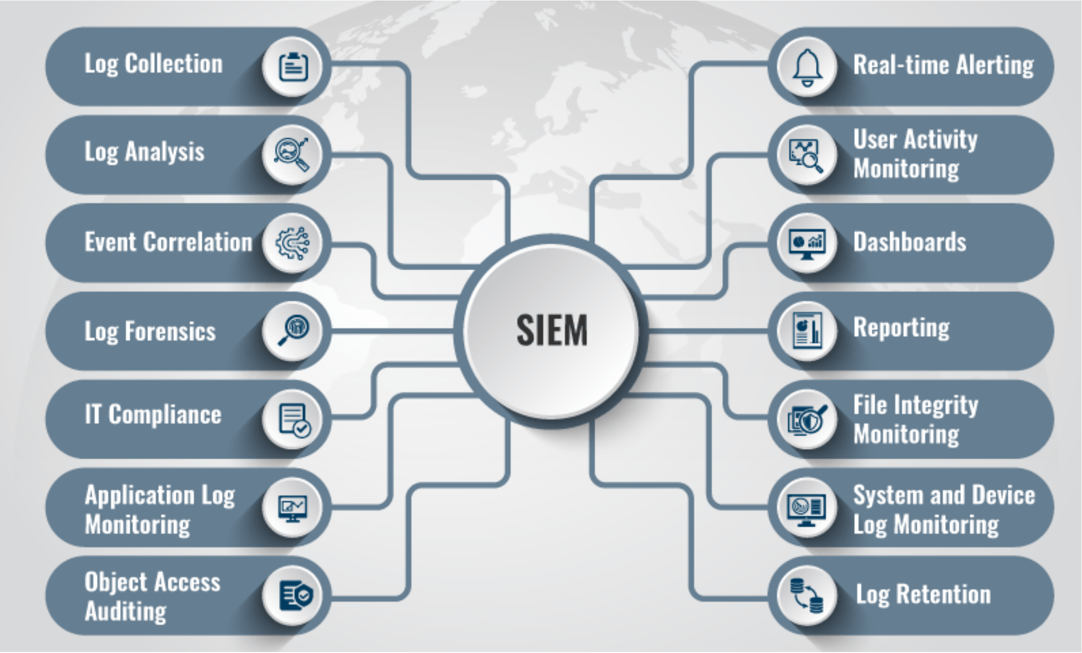
Security Information & Event Management

Discover and Prioritize real threats in real-time

tbSIEM is a cybersecurity analytics tool that has built-in threat intelligence and anomaly detection capabilities that analyses huge data streams in real time to discover non-compliant system activities, aberrant behaviour, security issues, and cyber threats. built for precise detection.

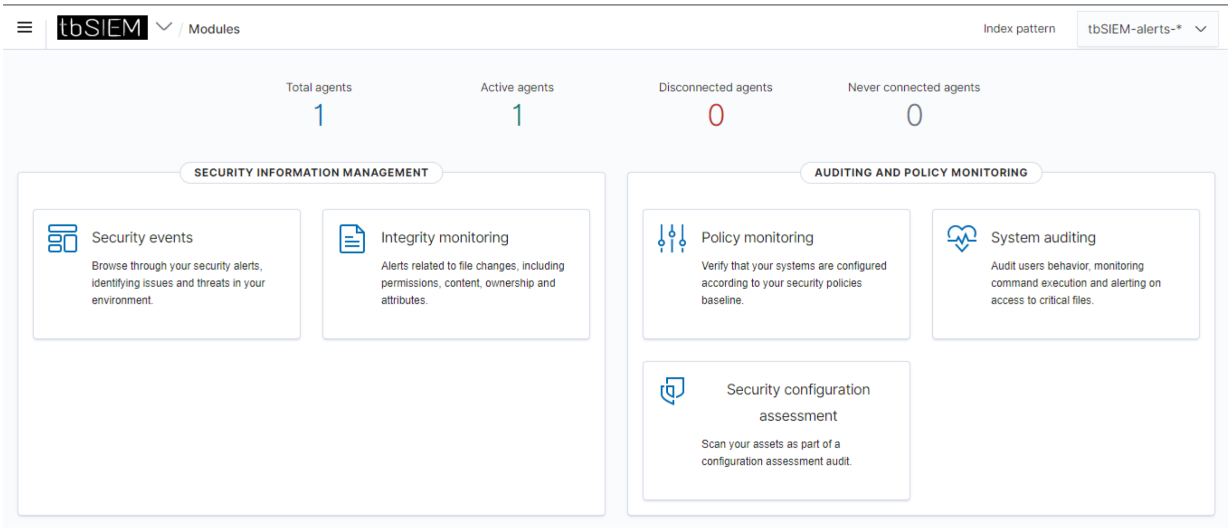
This technology provides an excellent foundation for a security operations centre (SOC). It operates quickly and independently, links to all systems and security measures, and performs as needed by stakeholders and employees. For large environments, tbSIEM is renowned for its wide-scale scalability and compliance monitoring capabilities.



> **“tbSIEM is designed to quickly and accurately detect non-compliant system activity, anomalous behavior, security issues and cyber threats”**

What tbSIEM delivers?

- Rapid incident response and resolution - advanced real-time collection, analysis and threat detection with live dashboard and alerting
- Easy to understand in-depth investigation - comprehensive business intelligence data query and reporting interface
- Reduced operational risk – process automation delivers live compliance dashboards, reporting and security workflow to streamline analyst activities
- Visibility for all stakeholders - customizable compliance reporting and dashboards for executives, auditors and customers
- Rapid identification and resolution of risks - unified security information and incident management
- Shortens time at risk - end-to-end incident tracking with active investigation and reporting
- Detection of anomalous situations - within networks, operating systems and application layers
- Significant ROI improvements - from existing security investments and operational efficiencies within the SOC environment.



Total agents 1

Active agents 1

Disconnected agents 0

Never connected agents 0

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

“tbSIEM supports a comprehensive data collection, threat detection, alert analysis, incident response and reporting lifecycle”

tbSIEM – How it works?

1. Security Monitoring & Compliance

tbSIEM is the foundation of the highly recognised Security Platform. This comprehensive security and compliance solution offers:

- Integrated incident management capabilities for incident investigation, escalation, and resolution;
- Role-based access controls, audit trails, and high levels of automation to streamline security operations;
- Detection of unknown and unknowable threats;
- Highly flexible architecture and support for high volume data throughput rates;
- Comprehensive data display, dashboard, and investigation capabilities;

In-depth data gathering, threat detection, alert analysis, incident response, and reporting lifecycles are all supported.

It has an entirely integrated incident management module that highlights events to make sure that alarms can be recorded, examined using a set methodology, escalated, and quickly handled.

2. Flexible Data Collection

To collect any data from any source, arrange it, and parse it through the analytics engines, tbSIEM offers a flexible, completely customizable interface.

- A fast, real-time, stream-based processing, correlation, and alerting engine that enables the quick detection of policy violations, security, loss, or fraud threats, and non-compliant activities.
- Complete flexibility in terms of collection, providing agent-based and agentless options for syslog, event logs, file-based, XML, database query, network traffic data, etc.
- The capacity to support third-party cloud-based services at the IaaS, PaaS, or SaaS layers, allowing total security visibility over on- and off-premise systems.
- A collection of original and normalised log files for forensic and evidentiary use.
- Unlimited off-line storage for archives, compliance, or historical analysis; infinitely scalable data model; many live/accessible repositories.

3. Advanced Analysis

The analytical engine of tbSIEM performs real-time analysis using policy-based deterministic algorithms and correlation to identify problems that require the operators' immediate attention.

- Using machine learning to give behaviorally based profile and detection, real-time anomaly detection of behaviour.
- Monitoring by security operators of several concurrent alarms from various sources.
- Monitoring the integrity of files and directories to protect sensitive company data.
- Risk and asset classification to identify threats, potential consequences on the firm, and significant business issues.
- Sets information and alarms in order of importance for manual or automated corrective action.

4. Effective Response

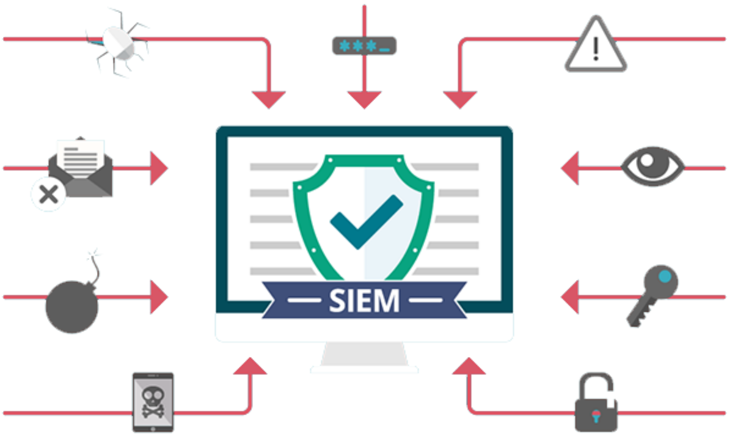
The security analyst's job does not end with the detection of potential cyber-security problems; rather, the hard work begins there. A comprehensive incident management solution that preserves case data in a single case record, alert tracking, an adaptable, context-based query interface, and automated workflow support are all features of tbSIEM. The solution delivers:

- The responses to the questions "who, what, where, when, and how" right after an occurrence.
- The capacity to take prompt action in the wake of an alarm to neutralize threats or collect any extra information to help future diagnostic procedures.
- Comprehensive alert monitoring and issue management solution with workflow support, escalation, case data management, and closure reporting.
- Integration with third-party solutions for threat reduction, SNMP/network management, ticketing, and API access.

"Detection of predicted cyberthreats is only a part of the security analyst's solution – normally, that is when the hard work starts."

5. State-Of-The-Art Visibility & Business Intelligence

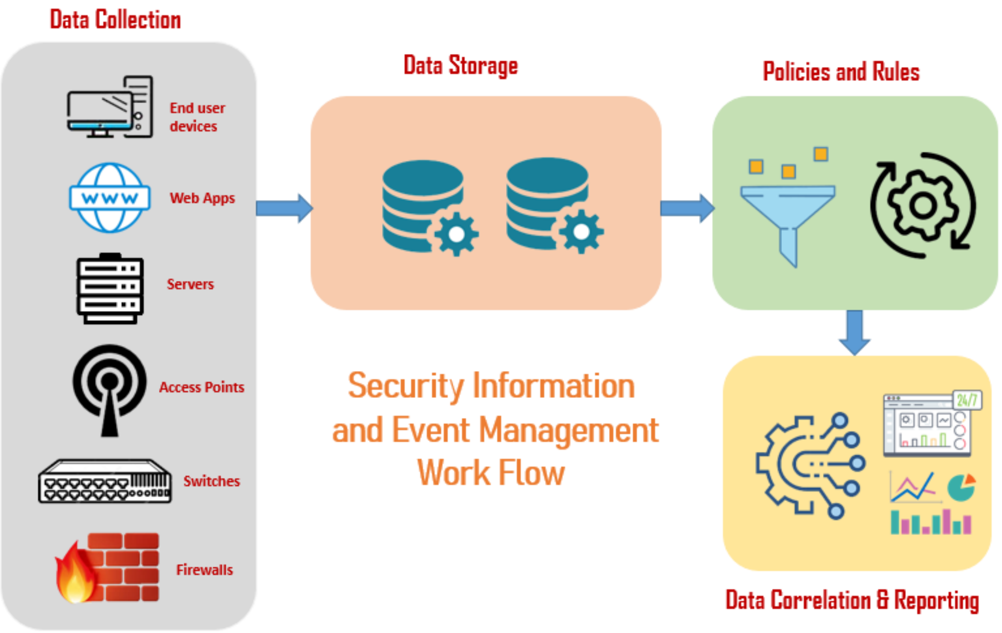
A key component of the product is access to data that (i) gives security analysts in-depth technical views to aid in incident resolution; and (ii) shows a one-page compliance summary and risk views for senior stakeholders, allowing for a quick understanding of the cyber-security and compliance posture of your business.



- Constant real-time risk and security dashboards for monitoring compliance status "as events happen."
- Business intelligence drill-down query interface with tabbed data views, interactive filtering, and ad hoc or saved context-based queries.
- A dynamic real-time view of all system activity, network connections, and user interactions.
- Scheduled and ad hoc reports that are pre-made or customized, with automatic storage and distribution to management and technical stakeholders.
- Vast library of pre-defined reports organized by source type, event type, and compliance criteria.
- A complete audit trail with trusted replay for all activity, a fully role-based and granular access control approach.

Modern visibility and business intelligence "provide security analysts detailed technical views, enabling them to quickly comprehend the cyber-security and compliance posture of your firm."

Product Features	tbSIEM
Data Collection and Analysis	
Continuous Monitoring	✓
Real-time Collection	✓
Correlation and Alerting	✓
Behavioral Anomaly Detection/Machine Learning Engine	✓
Network flow monitoring	✓
Threat Intelligence	✓
References tables of platforms, hosts, users for analysis	✓
Unlimited/free Agents	✓
Original log file collection	✓
File/Directory integrity monitoring	✓
Reporting and Visibility	
Query/Display Interface	✓
Operational Dashboards	✓
OOTB Compliance Packs	✓
GRC Dashboards	✓
Ad-hoc and Scheduled Reports	✓
Web-based “Business Intelligence” interface	✓
Workflow and Automation	
Incident Manager	✓
Scripted/Defined Response (Automatic or Manual)	✓
Alert tracking and workflow support	✓
Management	
Role based and granular access control	✓
Full Audit trial	✓
Asset manager Tool	✓
High Availability/Clustering	✓
Multiple on-line data repositories	✓
Automatic data backup, Aging and archive	✓
Support	
Phone/Email	✓
Onsite	✓



Use Cases

tbSIEM is used for PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) was created to secure credit cardholder data from theft and misuse. It defines 12 security areas in which companies should enhance protection for this type of data. The requirements apply to anyone involved in credit card processing, including merchants, processors, and 3rd party service providers.

tbSIEM helps PCI Compliance in the following ways:-

1. **Perimeter security –** tbSIEM detects unauthorized network connections and correlating with change management, searching for insecure protocols and services, and checking how traffic is flowing across the DMZ.

2. **User identities –** tbSIEM monitors any event that results in changes to user credentials, and activity by terminated users

3. **Real time threat detection –** tbSIEM monitors antivirus logs, monitoring insecure ports and services and correlating with threat intelligence.

4. **Production and data systems –** tbSIEM searches for dev/test or default credentials, replicas, etc. on production systems.

5. **Auditing and reporting –** tbSIEM collecting system and security logs, including specific PCI logging requirements, audits them in a format suitable for PCI reporting, and generating compliance reports.

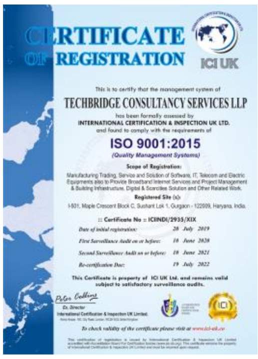
FOR MORE INFORMATION

About TechBridge

TechBridge is the World’s leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

Certificates:-

ISO 9001



CERTIFICATE OF REGISTRATION
ICI UK

This is to certify that the management system of
TECHBRIDGE CONSULTANCY SERVICES LLP
has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of
ISO 9001:2015
(Quality Management Systems)

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work.

Registered Site (s):
I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.

:: Certificate No :: ICIINDI/2935/XIX
Date of initial registration: 20 July 2019
First Surveillance Audit on or before: 10 June 2020
Second Surveillance Audit on or before: 10 June 2021
Re-certification Due: 19 July 2022

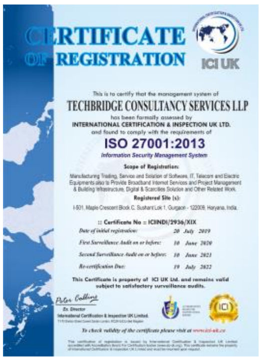
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Ex. Director
International Certification & Inspection UK Limited.
[illegible]

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

ISO 27001



CERTIFICATE OF REGISTRATION
ICI UK

This is to certify that the management system of
TECHBRIDGE CONSULTANCY SERVICES LLP
has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of
ISO 27001:2013
Information Security Management System

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work.

Registered Site (s):
I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.

:: Certificate No :: ICIINDI/2936/XIX
Date of initial registration: 20 July 2019
First Surveillance Audit on or before: 10 June 2020
Second Surveillance Audit on or before: 10 June 2021
Re-certification Due: 19 July 2022

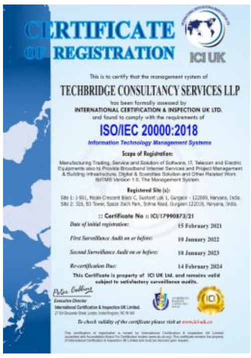
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Ex. Director
International Certification & Inspection UK Limited.
[illegible]

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

ISO 20000



CERTIFICATE OF REGISTRATION
ICI UK

This is to certify that the management system of
TECHBRIDGE CONSULTANCY SERVICES LLP
has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of
ISO/IEC 20000:2018
Information Technology Management Systems

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work. tbITMS Version 1.0, The Management System.

Registered Site (s):
Site 1: I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.
Site 2: 326, B3 Tower, Spaze Itech Park, Sohna Road, Gurgaon 122018, Haryana, India.

:: Certificate No :: ICI/17990873/21
Date of initial registration: 15 February 2021
First Surveillance Audit on or before: 10 January 2022
Second Surveillance Audit on or before: 10 January 2023
Re-certification Due: 14 February 2024

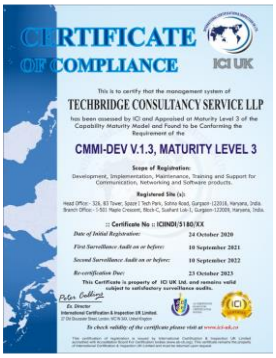
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Executive Director
International Certification & Inspection UK Limited.
[illegible]

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

CMMi L3



CERTIFICATE OF COMPLIANCE
ICI UK

This is to certify that the management system of
TECHBRIDGE CONSULTANCY SERVICE LLP
has been assessed by ICI and Appraised at Maturity Level 3 of the Capability Maturity Model and Found to be Conforming the Requirement of the
CMMI-DEV V.1.3, MATURITY LEVEL 3

Scope of Registration:
Development, Implementation, Maintenance, Training and Support for Communication, Networking and Software products.

Registered Site (s):
Head Office: - 326, B3 Tower, Spaze I Tech Park, Sohna Road, Gurgaon-122018, Haryana, India.
Branch Office: - I-501 Maple Crescent, Block-C, Sushant Lok-1, Gurgaon-122009, Haryana, India.

:: Certificate No :: ICIINDI/5180/XX
Date of Initial Registration: 24 October 2020
First Surveillance Audit on or before: 10 September 2021
Second Surveillance Audit on or before: 10 September 2022
Re-certification Due: 23 October 2023

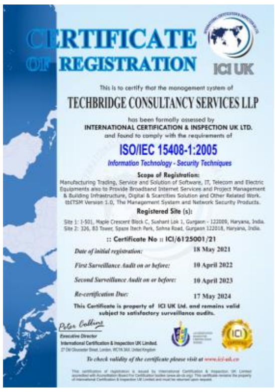
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Ex. Director
International Certification & Inspection UK Limited.
27 Old Gloucester Street, London, WC1N 3AX, United Kingdom

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

ISO 15408-1



CERTIFICATE OF REGISTRATION
ICI UK

This is to certify that the management system of
TECHBRIDGE CONSULTANCY SERVICES LLP
has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of
ISO/IEC 15408-1:2005
Information Technology - Security Techniques

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work. tbITSM Version 1.0, The Management System and Network Security Products.

Registered Site (s):
Site 1: I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.
Site 2: 326, B3 Tower, Spaze Itech Park, Sohna Road, Gurgaon 122018, Haryana, India.

:: Certificate No :: ICI/6125001/21
Date of initial registration: 18 May 2021
First Surveillance Audit on or before: 10 April 2022
Second Surveillance Audit on or before: 10 April 2023
Re-certification Due: 17 May 2024

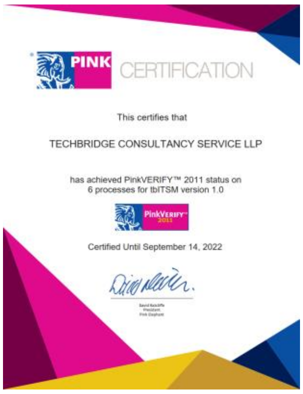
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Executive Director
International Certification & Inspection UK Limited.
27 Old Gloucester Street, London, WC1N 3AX, United Kingdom

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

PinkVERIFY



PINK CERTIFICATION

This certifies that

TECHBRIDGE CONSULTANCY SERVICE LLP

has achieved PinkVERIFY™ 2011 status on
6 processes for tbITSM version 1.0

PinkVERIFY™ 2011

Certified Until September 14, 2022

David Ratcliffe
President
Pink Elephant

Mail us at: sales@tech-bridge.biz

Address:- TechBridge Consultancy Services LLP
326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana