CBQA GLOBAL

WE
INSPIRE
IN TRUST

IT AUDIT

EVALUATE YOUR SYSTEM AND PROCESSES TO SECURE YOUR COMPANY DATA AND IDENTIFY METHODS TO MINIMIZE RISKS

We offer an assessment that help your organization to protect and to ensure that the information technology assets, controls, and processes are aligned with organizational goals and objectives.

By prioritizing professionalism in our work, we always provide maximum results to deliver “trust” to clients.

We will help you evaluate your system and processes to secure your company data and identify methods to minimize risks. We also ensure your information management processes comply with IT specific regulations, policies and standards.

- SOC 1 & SOC 2 Attestation
- PCI-DSS Attestation
- SWIFT Customer Security Program (CSP)
- Audit ITGC & ITAC
- HIPAA Assessment
- Digital Operational Resilience Act (DORA)
- Audit Application And Infrastructure - SPBE
- Audit IT Compliance based on Regulations
- Application & Network Performance Assessment

IT ASSURANCE & COMPLIANCE AUDIT

- Gap Assessment GDPR
- Gap Assessment UU PDP
- Record of Processing Activities (ROPA)
- Data Protection Impact Assessment (DPIA)
- Privacy Maturity - GAPP (ISACA)

PRIVACY & DATA PROTECTION

Category Product IT Audit

IT GOVERNANCE & MATURITY

- IT Maturity - COBIT 2019
- Cybersecurity Maturity Level
- Software Maturity - CMMI
- Data Governance Assessment

CYBERSECURITY ASSESSMENT

- Threat, Vulnerability, and Risk Assessment (TVRA)
- VAPT (Vulnerability Assessment and Penetration Testing)

THE DESCRIPTIONS & BENEFITS OF PRODUCT IT AUDIT

In an increasingly complex IT environment, organizations require reliable and independent assurance to protect information assets and support business continuity.

CBQA Global provides structured IT Audit services designed to help organizations assess risks, strengthen controls, and align IT processes with recognized standards and best practices.

The following outlines CBQA Global's IT Audit service offerings:

IT ASSURANCE & COMPLIANCE AUDIT

SOC 1 & SOC 2 ATTESTATION

Independent audit services to evaluate the design and operating effectiveness of an organization's internal controls. SOC 1 focuses on controls relevant to financial reporting, while SOC 2 assesses controls related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. SOC reports enhance trust for regulators, customers, and business partners.

Benefits:

- Builds trust with customers, regulators, and business partners
- Demonstrates effective internal control and system reliability
- Supports vendor due diligence and third-party assurance requirements
- Reduces operational and compliance risks

SOC REPORTS ENHANCE TRUST FOR REGULATORS, CUSTOMERS, AND BUSINESS PARTNERS.

PCI-DSS ATTESTATION

The Payment Card Industry Data Security Standard (PCI DSS) is an internationally recognized framework of security requirements aimed at protecting cardholder data and ensuring the integrity of payment transactions. This standard is essential for organizations that store, process, or transmit credit and debit card information.

For banks and financial institutions, compliance with PCI DSS is not just a best practice—it is often a mandatory requirement imposed by card networks, payment processors, and regulatory bodies. Failure to comply can lead to financial penalties, legal consequences, and reputational damage. Our PCI DSS compliance service helps your organization identify gaps, strengthen security controls, and meet all relevant obligations, ensuring your payment systems are both trusted and resilient.

Benefits:

- Ensures protection of payment card data
- Reduces risk of data breaches and financial penalties
- Strengthens customer confidence in payment security
- Supports compliance with payment network requirements

SWIFT CUSTOMER SECURITY PROGRAM (CSP)

SWIFT Attestation is an annual declaration process conducted by financial institutions that use the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network to confirm their compliance with the cybersecurity standards established under the SWIFT Customer Security Programme (CSP).

Organizations are required to perform either a self-assessment or an independent external assessment against the Customer Security Controls Framework (CSCF) to ensure their financial transaction systems are adequately protected from cyber threats.

Benefits:

- Enhances cybersecurity posture for SWIFT-connected environments
- Meets mandatory SWIFT security requirements
- Reduces risk of fraud and cyber attacks
- Increases confidence of correspondent banks and regulators

AUDIT ITGC & ITAC

Audit of IT General Controls and IT Application Controls to ensure system reliability, data integrity, and effective support of business processes. The audit covers access management, change management, IT operations, and application-level controls.

Benefits:

- Improves reliability of IT systems and data integrity
- Strengthens internal controls supporting business processes
- Supports financial, operational, and regulatory audits
- Reduces risk of system errors and unauthorized access

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)OPERATIONAL

The Digital Operational Resilience Act (DORA) service provides an assessment of an organization's capability to prevent, respond to, recover from, and adapt to ICT-related disruptions and cyber incidents, in line with the requirements of the European Union's DORA regulation.

This assessment evaluates the organization's ICT risk management framework, incident detection and response, business continuity and disaster recovery, operational resilience testing, and third-party ICT risk management. The service helps financial institutions and ICT service providers identify gaps, assess readiness, and develop a structured roadmap to achieve and maintain digital operational resilience.

Benefits:

- Improves digital operational resilience and ICT risk management
- Ensures readiness for EU regulatory compliance
- Enhances incident response and business continuity capabilities
- Reduces disruption from cyber and technology incidents

HIPAA ASSESSMENT

Assessment of compliance with HIPAA Security Rule and Privacy Rule for organizations in the healthcare sector. The service evaluates administrative, technical, and physical safeguards to protect Protected Health Information (PHI) and identifies compliance gaps and risks.

Benefits:

- Ensures compliance with healthcare data protection regulations
- Reduces risk of data breaches and regulatory penalties
- Protects patient privacy and sensitive health information
- Strengthens trust with patients and healthcare partners

AUDIT APPLICATION AND INFRASTRUCTURE - SPBE

The SPBE (Electronic-Based Government System) Audit is mandated under Presidential Regulation No. 95 of 2018, aiming to evaluate the integrity, reliability, and security of government digital systems. This audit covers three key areas: infrastructure, applications, and cybersecurity.

Infrastructure and application assessments are overseen by BRIN, while the security audit falls under the authority of BSSN. Our SPBE audit service helps institutions ensure their systems meet these mandated obligations by providing expert guidance and support throughout the audit process, ensuring that organization's digital systems are fully compliant and resilient. Taking this audit is essential for institutions aiming to align with national digital transformation initiatives and regulatory requirements.

Benefits:

- Fulfillment of Presidential Regularion 95/2018 and BRIN regulations related to SPBE
- Assess the extent to which applications and infrastructure meet criteria set by regulations
- Increase transparency and accountability in governance
- Provide recommendations for improvements to increase the efficiency and effectiveness of public services

AUDIT IT COMPLIANCE BASED ON REGULATIONS

IT Audit is a systematic evaluation of an organization's information technology systems, policies, and controls to ensure compliance with internal standards and external regulations. In state-owned enterprises (BUMN) and government institutions, IT audits are often mandated by national regulations such as Law No. 27 of 2022 on Personal Data Protection, Presidential Regulations on SPBE (No. 95/2018 and No. 132/2022), and directives from BSSN, the Ministry of State-Owned Enterprises, and the Ministry of Communication and Information Technology.

Meanwhile, in the financial sector, including banks and non-bank financial institutions, IT audits are critical to fulfilling compliance obligations under Bank Indonesia Regulations (PBI) and Financial Services Authority Regulations (POJK)—which emphasize the importance of IT risk management, cybersecurity, data protection, and service continuity. Across all sectors, IT audit services play a vital role in strengthening governance, reducing risk, supporting regulatory compliance, and enabling secure and resilient digital transformation.

Benefits:

- Ensures compliance with applicable laws and regulations
- Identifies compliance gaps before regulatory reviews
- Reduces legal and regulatory exposure
- Strengthens governance and accountability

APPLICATION & NETWORK PERFORMANCE ASSESSMENT

Assessment of application and network performance tailored to deliver faster, more reliable applications with end-to-end performance insight and optimization. The service ensures IT systems can effectively support operational and business demands.

Benefits:

- Improves system stability and reliability
- Identifies performance bottlenecks and capacity issues
- Root-cause analysis of poor system performance
- Enhances user experience and service availability
- Supports business growth and scalability

PRIVACY & DATA PROTECTION

GAP ASSESSMENT UU PDP

Our compliance verification service is designed to evaluate your organization's readiness in processing Personally Identifiable Information (PII) in accordance with UU PDP No. 27 Tahun 2022. We assess your data protection policies, systems, procedures, and its implementation to ensure full regulatory compliance.

More than fulfilling a legal obligation, this service is a critical step in safeguarding your company from the risk of government-imposed sanctions due to data breaches or non-compliance. A single incident of data leakage can severely damage your company's reputation and erode customer trust. By engaging our service, you take a proactive approach to strengthen your data governance, demonstrate accountability, and build public confidence—before issues arise.

Benefits:

- Identifies gaps in GDPR compliance
- Reduces risk of regulatory sanctions and fines
- Strengthens personal data protection practices
- Provides a clear GDPR compliance roadmap

GAP ASSESSMENT GDPR

Assessment of gaps against the General Data Protection Regulation (GDPR) to identify privacy risks, compliance deficiencies, and improvement areas. The results support the development of a structured GDPR compliance roadmap.

Benefits:

- Identifies gaps in GDPR compliance
- Reduces risk of regulatory sanctions and fines
- Strengthens personal data protection practices
- Provides a clear GDPR compliance roadmap

RECORD OF PROCESSING ACTIVITIES (ROPA)

Development and review of Records of Processing Activities (ROPA) as formal documentation of personal data processing. ROPA supports regulatory compliance and provides transparency over data processing activities and responsibilities.

Benefits:

- Provides clear visibility of personal data processing activities
- Supports regulatory compliance and audits
- Improves accountability and data governance
- Enables better privacy risk management

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Privacy risk assessment for high-risk personal data processing activities. DPIA identifies potential impacts on data subjects' rights and defines appropriate mitigation measures prior to processing.

Benefits:

- Identifies and mitigates privacy risks early
- Protects data subjects' rights and freedoms
- Supports regulatory expectations for high-risk processing
- Reduces likelihood of privacy incidents

PRIVACY MATURITY - GAPP (ISACA)

Assessment of an organization's privacy governance maturity based on Generally Accepted Privacy Principles (GAPP). The service provides insights into current maturity levels, gaps, and a roadmap for continuous improvement.

Benefits:

- Measures the effectiveness of privacy governance
- Identifies maturity gaps and improvement priorities
- Aligns privacy practices with international best practices
- Supports long-term privacy program development

IT GOVERNANCE & MATURITY

IT MATURITY - COBIT 2019

The application of information technology in work systems in various types of organizations is designed to enhance performance, achieve goals, objectives, and improve the organization's competitive advantage.

Benefits:

- Aligns IT governance with business objectives
- Identifies governance gaps and improvement areas
- Provides a structured IT improvement roadmap
- Supports management and board-level oversight

CYBERSECURITY MATURITY LEVEL

A Cybersecurity Maturity Level Audit assesses an organization's ability to protect its information by evaluating its cybersecurity practices against structured maturity levels, determining its security posture relative to its risk environment.

Benefits:

- Measures cybersecurity readiness and capability
- Identifies strengths and weaknesses in security posture
- Supports strategic cybersecurity planning
- Enhances resilience against cyber threats

SOFTWARE MATURITY - CMMI

Assessment of software development process maturity based on the Capability Maturity Model Integration (CMMI). This service helps organizations improve software quality, consistency, and development efficiency.

Benefits:

- Improves software development quality and consistency
- Reduces defects and rework costs
- Enhances delivery predictability and efficiency
- Supports continuous process improvement

DATA GOVERNANCE ASSESSMENT

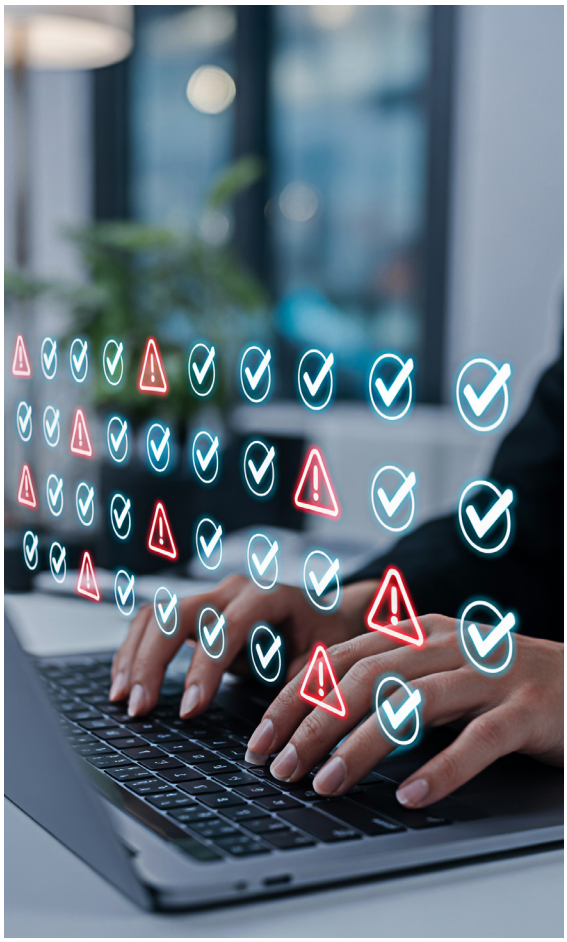
Assessment of organizational data governance to ensure data is managed securely, effectively, and in compliance with regulations. The service covers governance structure, policies, data quality, and the strategic use of data as a business asset.

Benefits:

- Improves data quality, security, and compliance
- Strengthens accountability and data ownership
- Enables better data-driven decision making
- Maximizes the value of data as a strategic asset

IT GOVERNANCE & MATURITY

THREAT, VULNERABILITY, AND RISK ASSESSMENT (TVRA)



A TVRA Audit is a formal assessment process that identifies potential threats, evaluates vulnerabilities, and determines risks faced by critical systems, infrastructure, or facilities — commonly applied in financial, transportation, and public service sectors. The objective is to recognize possible security threats, assess system weaknesses, and determine risk levels, allowing the organization to implement appropriate mitigation measures and security controls.

Benefits:

- Provides a holistic view of cybersecurity risks
- Supports risk-based decision making
- Helps prioritize security investments
- Improves overall risk management effectiveness

VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING)

Technical security testing to identify, validate, and exploit vulnerabilities in applications, networks, and infrastructure. VAPT provides a realistic view of system security from an attacker's perspective.

Benefits:

- Identifies exploitable security weaknesses
- Simulates real-world cyber attacks
- Reduces likelihood of successful breaches
- Strengthens technical security controls

SCHEDULE YOUR IT AUDIT WITH US !!!

www.cbqaglobal.com

WE
INSPIRE
IN TRUST

YOUR TRUSTED PARTNER

CONTACT US

(62) 21 2781 4200

(62) 811 8468 777

info@cbqaglobal.com

FOLLOW US

cbqaglobal

cbqaglobal

CBQAGlobalIndonesia