



Dilip Buildcon Limited

ISMS Framework



ISO 27001: 2022

Certification Obtained for Dilip Buildcon Limited (DBL)

Zero

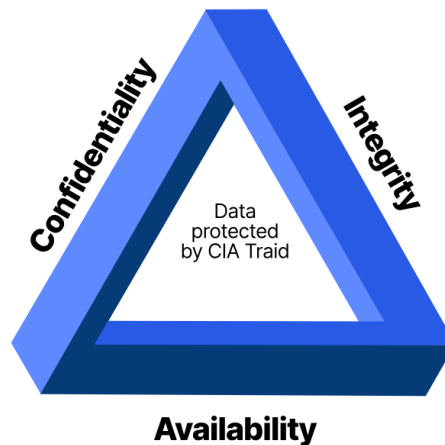
Incidents or loss of data or Information

Dilip Buildcon Limited (DBL) is a prominent Engineering, Procurement, and Construction (EPC) company in India, with a proven track record of delivering complex infrastructure projects on time and with precision

DBL ISMS Focused Areas

- Leverage industry best practices and advanced technology absorption
- Proactive management of information security incidents
- Modernize IT architecture to enhance its resilience, improve business processes
- Focus on Artificial Intelligence

DBL is committed to protecting information and information systems from unauthorized access, disclosure, alteration, loss, or disruption. Information security is a fundamental business requirement that supports customer trust, legal and statutory compliance, secure business operations, and business continuity. The organization protects information based on the principles of Confidentiality, Integrity, and Availability (CIA).



- Confidentiality ensures that information is accessed only by authorized individuals and systems.
- Integrity ensures that information remains accurate, complete, and protected from unauthorized modification.

- Availability ensures that information and systems are accessible when required for business and production operations.

Information security controls are implemented using a risk-based approach, considering information sensitivity, environment type, customer requirements, legal and statutory obligations, and operational impact. Where multiple requirements apply, the most stringent controls are followed.

DBL is committed to meeting all applicable customer, legal, regulatory, and statutory information security requirements relevant to its business operations. Information security controls are designed and implemented to protect customer and customer-owned information, fulfill contractual obligations, and comply with applicable laws, regulations, and certification requirements. This includes adherence to ISO/IEC 27001 : 2022

ISMS & Security Framework



ISO/IEC 27001 : 2022 Alignment: DBL structures its internal security controls, risk assessments, and management systems around ISO 27001 : 2022 requirements to safeguard enterprise and client data.

- **Information Security Group (ISG):** An dedicated internal organization that drives security culture, enforces standardized policies, and manages global security operations.
- **Risk & Metrics Program:** Evaluates compliance continuously, drives business process integration, and uses specific, measurable metrics rather than treating security as a one-time audit.
- **External Audits:** Undergoes annual **ISO 27001** certification audits, alongside other regular account audits.

Cornerstones of DBL Information Security Strategy

- Adherence to industry best practices
- Comprehensive employee trainings
- Investments in advanced technology

Governance Risk and Compliance (GRC)

GRC plays a crucial role in cyber security, providing a framework for managing third-party risks and regulatory compliance. It helps mitigate associated risks, ensures compliance with regulatory requirements and internal controls, and fosters a secure and compliant environment.

Board Level

Oversees and reviews corporate policies, plans and programmes related to enterprise cyber security and data protection risks associated with the Company and its IT infrastructure

Business Level

The Chief Information Security Officer (CISO) is responsible for implementing systems and procedures Ensures safeguarding Organisational assets by optimizing efficiency and effectiveness of security processes and infrastructure through effective implementation of ISO 27001 Controls



- **Organizational:**

Covers governance, policies, risk management, and supplier relationships. It focuses on how security is managed at a strategic and process level within the organization.

- **People**

Focuses on human-related security aspects such as employee responsibilities, awareness, and training. It ensures that individuals understand their role in maintaining security.

- **Physical**

Addresses physical security controls, including protection of facilities, equipment, and environmental safeguards. It ensures that physical access and environmental risks are properly managed.

- **Technological:**

Covers technical controls such as access control, cryptography, system security, and monitoring. This category focuses on protecting systems and data through technology-driven measures.