CLOUD4C
A CtrlS Company

Cloud4C Confidential & Identity-Aware Computing

Cloud4C Confidential & Identity-Aware Computing Offering

CLOUD4C
A CtrlS Company

- Azure Confidential VMs (DC-Series)
- Azure Managed HSM
- Azure Key Vault Premium
- Double Encryption Enforcement
- Azure Policy Integration

Proven Business Outcomes with Cloud4C

- 100% encryption coverage across data at rest, in transit, and in use
- 40% reduction in insider risk with hardware-isolated confidential workloads
- Improved compliance readiness with GDPR, HIPAA, PCI-DSS, and ISO 27001 alignment
- Audit-ready reporting with automated policy enforcement and encryption logs
- Future-ready adoption of privacy-preserving cloud in BFSI, healthcare, and government
- Enterprise-proven deployments across BFSI, telecom, energy, and regulated industries

Cloud4C Confidential & Identity-Aware Computing Methodology

Sensitive Data & Risk Assessment

- Review workloads handling regulated or confidential data (BFSI, healthcare, government).
- Identify gaps in data-at-rest, in-transit, and in-use protection.
- Benchmark against ISO 27001, GDPR, HIPAA, and PCI-DSS requirements.

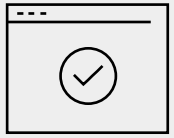
Secure Deployment & Encryption Integration

- Guided rollout of Azure Confidential VMs, Managed HSM, and Key Vault.
- Configure double encryption enforcement and key lifecycle policies.
- Enable automated governance via Azure Policy for consistent controls.

Validation & Compliance Assurance

- Validate encryption coverage across data states with audit-ready dashboards.
- Run access and key usage checks to detect anomalies and policy deviations.
- Ensure compliance reporting mapped to GDPR, HIPAA, PCI-DSS, and ISO frameworks.

Continuous Optimization & Advisory



- Advisory-led tuning of encryption and confidentiality policies.
- Integration of AI & Copilot for anomaly detection and guided remediation.
- Continuous maturity uplift for Zero Trust and privacy-preserving workloads.

Why Cloud4C for Confidential & Identity-Aware Computing?