The 12 Golden TOMS when using IT Providers.

These are 12 core infosec controls to best implement when relying on external IT service providers.

1. Ask provider for binding affirmation for and evidence of meeting these controls
2. Review them; make sure that below controls are fully covered
3. Have them included in the contract, ask for evidence and provide for reviews
4. Regularly (at least yearly) review compliance with them (e.g., audit reports)

Controls / Information Security Measures	C	P	Sample Wording for Provider Contracts
Identity & access management, specifically multi-factor authentication (MFA), temporary privileged access management (TPAM), segregation of duties and roles, and control over regular user identities and permissions	X	X	The Provider shall apply a state-of-the-art identity and access management, incl. multi-factor-authentication for every user with access to customer data. For privileged user roles, a privileged access management system and procedure where temporary privileged access is requested case specific and each time granted only for a limited time based on two independent approvals (default: 4 hours), with segregated privileged roles (root, HSM, Log, Key-Mgt, IAM, SDLC). Regular (min. yearly) review of user identities/permissions re need to know.
Encryption and key management, specifically use of customer specific keys, key hosting in a hardware security module, control over encryption keys and technical processes working with these		X	Customer data shall be encrypted using keys that are individual and specific for the Customer, stored in an HSM, not exportable, and administered by the Provider (unless Customer key management is agreed) for the Customer individually. The key management service (incl. HSM) may be a shared by multiple customers, but the technical processes for accessing keys within HSM/Key Vault must be Customer-specific and not shared.
Restriction and protection of data extracts, specifically their encryption, data leakage prevention and access management	X	X	Extraction of Customer data in any form (incl. for support) may only happen where mandatory. Extracted data shall remain classified (using labels), encrypted (using customer specific keys) and protected (data leakage prevention to stop the exfiltration of Customer data even where it has been extracted into files or exported).
Cross-border processing and access control, where data is physically or virtually hosted/processed, from where data can be accessed by regular or privileged users, where data backups are	X	X	Storage and any processes for processing Customer data must be localized and implemented in the form of an instance in the jurisdiction(s) as agreed in the contract. This shall also apply to all subcontractors, and to any ancillary data processing (e.g., backups). Regular as well as privileged user cross-border access shall not only be governed (and, where not permitted, prevented) by organizational, but also by adequate technical means.
Log management, full audit trails, log immutability and protection, log control, monitoring and retention	X	X	The Provider shall ensure that logs are read only, cannot be modified or prematurely deleted by any role. Any access to or use/change of Customer data or to keys, changes to privileged access roles/rights by Provider staff is to be logged, with the logs being available to Customer in real-time and retained for at least one year.
Penetration testing, disclosure and control, monitoring and remediation of findings from penetration tests	X	X	The Provider shall regularly have independent 3rd-party penetration tests conducted (at least yearly), disclose results and remediation measures to the Customer; the remediation shall be confirmed independently.
Threat & vulnerability management including incident & response management	X	X	The Provider shall maintain a robust threat & vulnerability management program, identifying, assessing, and mitigating security threats and vulnerabilities associated with the Provider's services. It shall promptly detect security incidents and maintain an effective response and management process. All identified threats, vulnerabilities and incidents are to be reported promptly to Customer, including adequate remediation plans.
Change control, release management process governance and supervision		X	The Provider shall maintain a robust change control framework regarding its services, with changes/releases overseen systematically and only upon multiple independent approvals, and supervision of the entire process to minimize risks, including monitoring/logging the planning, testing, deployment of software releases.
Segregation between production/non-production environments		X	The Provider shall enforce strict segregation of production and non-production environments (including for storage), and specifically also of related access roles (no simultaneous access of any user to prod/non-prod).
Records management, records immutability and access control	X	X	Where the Provider performs records management, is shall store records immutably, and protected against alteration and deletion. Privileged access only through temporary privileged access management (TPAM).
Subcontractor risk management ensuring same standards	X	X	The Provider shall ensure that each subcontractor provides controls that at least match the present TOMS, which is to be confirmed by the Provider, or by an independent 3rd party with an audit report, at least yearly.
Risk governance for the Provider and its entire supply chain	X	X	The Provider shall maintain robust risk governance practices, incl. monitoring, assessing, and mitigating risks across the entire supply chain, with a yearly review/BoD approval process for all policies/procedures/controls.

Customer
Provider

Note: The above measures do *not* cover business continuity management, which will also have to be addressed when relying on an outside IT service provider.

Need help on above?

Information security: Rolf A Becker (contact@cloudriskgovernance.ch)
Legal & regulatory: David Rosenthal (drosenthal@vischer.com)

VISCHER
SWISS LAW AND TAX