VISCHER

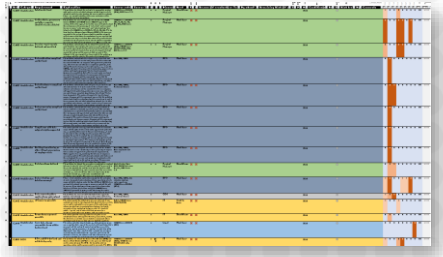
Vendor Cyber Risk Management.

The Legal Viewpoint

David Rosenthal, Partner, VISCHER Ltd.
February 27, 2024

The requirements

- **Data protection law, professional secrecy**
  - Adequate data security measures, including validation/audit trails
  - Data breach notification obligations
- **Market and product regulations**
  - Sector-specific (e.g., FINMA, EBA, BaFin, EU DORA)
  - Technology-specific (e.g., EU AI Act, Data Act)
  - Critical infrastructure (e.g., EU NIS2, EU CER, CH ISG), incl. cyber risk management, incident notification obligations
- **Good corporate governance**
  - Protection against operational and reputational risks
  - Business continuity management (BCM)



Cloud Compliance and Risk Assessment (CCRA-FI) defines **128 Requirements** to be complied with by Swiss Banks for their cloud projects

Some are more specific than others

Cybersecurity risk-management measures

1. Member
operational an
which those er
of incidents on

Taking into acc
cost of implem
information sy
shall be taken
and their sever

2. The mea
information sy

(a) policies on

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

Article 21 NIS2 Directive (part)

Both internal and external persons who can access critical data or who can change these must be selected carefully. These persons must be monitored with the help of appropriate measures[20] and given regular training in the handling of these data. Increased security requirements shall apply to persons with increased privileges[21]. In addition, a list of all persons with privileged access rights must be kept and updated on a regular basis.

Incidents that substantially impair the confidentiality, integrity or availability of critical data must be reported to FINMA without delay.

When selecting service providers that can process[22] or view critical data, due diligence must be particularly thorough. Clear criteria for assessing how service providers handle critical data must be defined and checked before entering into a contractual agreement. The service providers must be monitored and checked periodically as part of the institution's internal control system.

N 80 et seq.
FINMA Circular 2023/1
on operational risks and
resilience of banks

What we often see in practice

- **On the part of customers**
  - Contracts that require providers to have "adequate technical and organizational measures of security" with only a very generic list of TOMS
  - The adequacy of provider TOMS is usually not scrutinized, let alone verified whether they indeed exist in practice
  - No follow-up validation, not even by way of audit reports
- **On the part of vendors**
  - Those who sign anything just to get the contract
  - Those who have terms that sound great, but at closer look are full of loopholes
  - Those who stick to their own terms & TOMS ("take it or leave it")

Issue #1: Beware of smokescreens

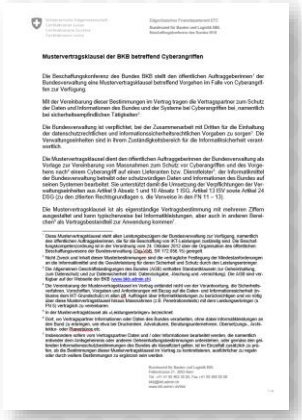
Solve with negotiation or accept the risk

- Contracts with state-of-the-art security **only at first sight**
  - Often a strategy to limit legal exposure in case of a data breach
- Real-life **examples** out of cloud service provider contracts
  - Obligation to maintain an ISMS, but not an actual security level
  - Security commitments limited to the infrastructure layer
  - Descoping of audit reports possible at any time
  - No commitment to keep customer data confidential, only to implement measures that protect customer data
  - Encryption does not always work, access is not always logged
  - Commitments only as commercially reasonable, no warranty
  - Breach notification clock starts ticking only after the internal confirmation procedure; no clarity re sub-provider breaches

Issue #2: Be specific

Have infosec experts and lawyers align themselves

- Many **security clauses** and TOMS are **too generic** (e.g., no controls) or otherwise leave too much room for interpretation
  - **Example:** The new clauses used by the Federal Government
    - *"X2. When processing federal data and information, the service provider undertakes to observe and comply with the requirements and provisions of the Data Protection Act (DPA) and the Information Security Act (ISA), including the relevant implementing ordinances and the Confederation's basic ICT protection. It shall transfer these obligations to third parties it engages (e.g. suppliers, substitutes, subcontractors)."*
- It must be **clear** what the vendor has to do (e.g., type of PAM)
  - Being specific allows them to **challenge** the vendor and **verify** compliance (updating TOMS later on is still possible)

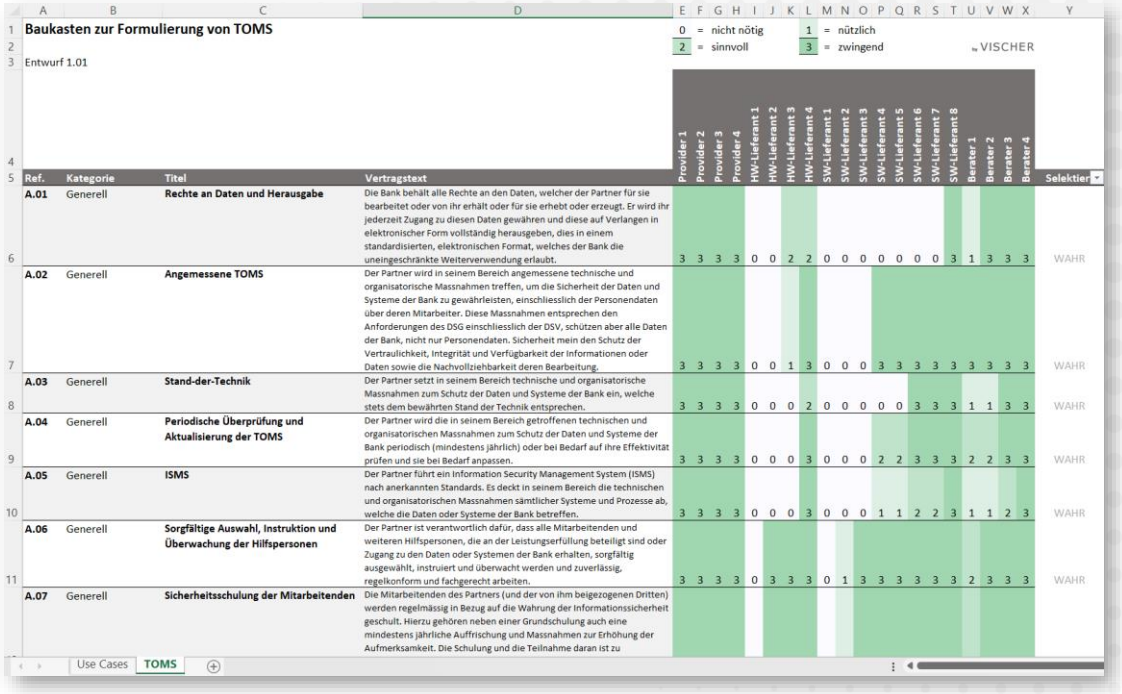


Mustervertragsklausel der BKB betreffend Cyberangriffen

https://www.bkb.admin.ch/bkb/de/home/themen/agb.html

Use-case-specific TOMS

Do not only consider IT providers and "processors" …



Baukasten zur Formulierung von TOMS

Entwurf 1.01

0 = nicht nötig; 1 = nützlich; 2 = sinnvoll; 3 = zwingend; „VISCHER

Ref.	Kategorie	Titel	Vertragstext	Provider 1	Provider 2	Provider 3	Provider 4	HW-Lieferant 1	HW-Lieferant 2	HW-Lieferant 3	HW-Lieferant 4	SW-Lieferant 1	SW-Lieferant 2	SW-Lieferant 3	SW-Lieferant 4	SW-Lieferant 5	SW-Lieferant 6	SW-Lieferant 7	SW-Lieferant 8	Berater 1	Berater 2	Berater 3	Berater 4	Selektier
A.01	Generell	Rechte an Daten und Herausgabe	Die Bank behält alle Rechte an den Daten, welcher der Partner für sie bearbeitet oder von ihr erhält oder für sie erhebt oder erzeugt. Er wird ihr jederzeit Zugang zu diesen Daten gewähren und diese auf Verlangen in elektronischer Form vollständig herausgeben, dies in einem standardisierten, elektronischen Format, welches der Bank die uneingeschränkte Weiterverwendung erlaubt.	3	3	3	3	0	0	2	2	0	0	0	0	0	0	0	3	1	3	3	3	WAHR
A.02	Generell	Angemessene TOMS	Der Partner wird in seinem Bereich angemessene technische und organisatorische Massnahmen treffen, um die Sicherheit der Daten und Systeme der Bank zu gewährleisten, einschliesslich der Personendaten über deren Mitarbeiter. Diese Massnahmen entsprechen den Anforderungen des DSG einschliesslich der DSV, schützen aber alle Daten der Bank, nicht nur Personendaten. Sicherheit mein den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen oder Daten sowie die Nachvollziehbarkeit deren Bearbeitung.	3	3	3	3	0	0	1	3	0	0	0	3	3	3	3	3	3	3	3	3	WAHR
A.03	Generell	Stand-der-Technik	Der Partner setzt in seinem Bereich technische und organisatorische Massnahmen zum Schutz der Daten und Systeme der Bank ein, welche stets dem bewährten Stand der Technik entsprechen.	3	3	3	3	0	0	0	2	0	0	0	0	0	3	3	3	1	1	3	3	WAHR
A.04	Generell	Periodische Überprüfung und Aktualisierung der TOMS	Der Partner wird die in seinem Bereich getroffenen technischen und organisatorischen Massnahmen zum Schutz der Daten und Systeme der Bank periodisch (mindestens jährlich) oder bei Bedarf auf ihre Effektivität prüfen und sie bei Bedarf anpassen.	3	3	3	3	0	0	0	3	0	0	0	2	2	3	3	3	2	2	3	3	WAHR
A.05	Generell	ISMS	Der Partner führt ein Information Security Management System (ISMS) nach anerkannten Standards. Es deckt in seinem Bereich die technischen und organisatorischen Massnahmen sämtlicher Systeme und Prozesse ab, welche die Daten oder Systeme der Bank betreffen.	3	3	3	3	0	0	0	3	0	0	0	1	1	2	2	3	1	1	2	3	WAHR
A.06	Generell	Sorgfältige Auswahl, Instruktion und Überwachung der Hilfspersonen	Der Partner ist verantwortlich dafür, dass alle Mitarbeitenden und weiteren Hilfspersonen, die an der Leistungserfüllung beteiligt sind oder Zugang zu den Daten oder Systemen der Bank erhalten, sorgfältig ausgewählt, instruiert und überwacht werden und zuverlässig, regelkonform und fachgerecht arbeiten.	3	3	3	3	0	3	3	3	0	1	3	3	3	3	3	3	2	3	3	3	WAHR
A.07	Generell	Sicherheitsschulung der Mitarbeitenden	Die Mitarbeitenden des Partners (und der von ihm beigezogenen Dritten) werden regelmässig in Bezug auf die Wahrung der Informationssicherheit geschult. Hierzu gehören neben einer Grundschulung auch eine mindestens jährliche Auffrischung und Massnahmen zur Erhöhung der Aufmerksamkeit. Die Schulung und die Teilnahme daran ist zu																					

Use Cases | TOMS

A repository of **129 TOMS** created for a large Swiss bank that can be selected based on the use case (e.g., various scenarios of hardware and software providers, online providers and advisors)

Issue #3: Require evidence

Provide for a realistic security validation method and expert Q&A sessions to get a feeling

- If the vendor signs your **tough TOMS** without pushing back, you usually have a problem …
  - Real-life **examples:** Confirmation that any operator access is logged, TPAM, obligation to have all confidential information received from the customer deleted upon the end of the contract
- Do not only **test the provider** during due-diligence, but also have an effective ongoing validation agreed (and implement it)
  - ISO 27001 is not sufficient, nor is an audit right that is not used
  - Require standardized 3rd party audit reports on actual controls and their effectiveness, 3rd party reports on penetration tests, and vulnerability assessments – and have them reviewed
- Agree on incident reporting, **remediation**, costs, consequences

Some more issues to consider

- **Cover the entire supply chain**
  - Impose obligations upon sub-processors, consider other suppliers
  - If a hyperscaler is used: How is the vendor handling it?
- **Data breach handling**
  - Only covered if related to personal data? What is the procedure?
  - How does the vendor deal with exploits that become known?
- **Risk of foreign lawful access**
  - This is often neither considered nor specifically addressed when using providers; special TOMS and risk assessments are required
- **Ability to exit if it becomes necessary**
  - Within what period of time will you be able to exit?

Final remarks

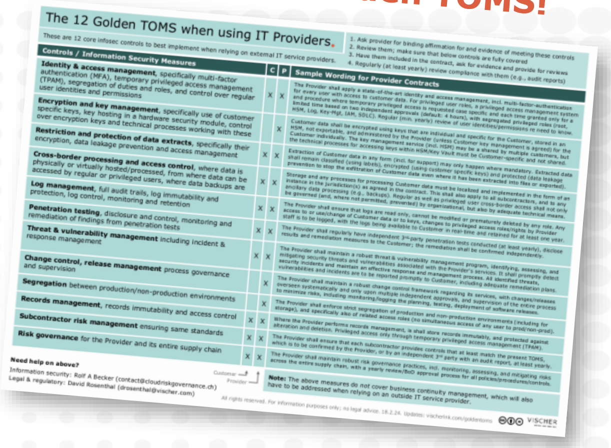
- Have a **contract** that provides for TOMS that are **specific enough** to provide for controls and adequate for the use case
- Beware of **smokescreens** and vendors that do not **push back**
- Do not forget to cover foreign **lawful access** & subcontractors
- Make sure the effective implementation of the controls in the supply chain is **verified** pre-signing and regularly thereafter
- Make sure the **adequacy** of the controls is regularly validated and improvements are made, as necessary, at the vendor's cost
- Have **issues reported**, **remedied** and remedies **verified**
- Have **non-contractual safeguards** (e.g., audits & logging) not only contractually agreed, but also utilized

VISCHER

Thank you for your attention!

Questions: drosenthal@vischer.com

Get the 12 Golden TOMS!


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.

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

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.

All rights reserved. For information purposes only; no legal advice. 18.2.24. Updates: vischerlnk.com/goldentoms VISCHER

https://vischerlnk.com/goldentoms

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com