VENDOR CYBER RISK MANAGEMENT PRACTICAL EXPERIENCE

Cloud Risk Governance Consulting Rolf A. Becker

WHAT VENDORS TELL YOU

Leading in security, following or ISO 27001 certified, never had any incident, secure by design, using trusted cloud platform providers, you are the only one who ever sent us so many questions, not providing evidence as this is confidential, everybody else is happy with our security

WHAT THIS IN REALITY MEANS

They have declared their security controls but nobody has demanded evidence
They use one of the hypervisors' PaaS but nobody checked which services and in what configuration and with which features subscribed / turned on
They have not noticed that data has been leaked
i.e.
No TPAM, no MFA, shared encryption, no DLP, no data classification, logs unprotected, no own Cyber Threat & Vulnerability Management

BUT THERE IS A CATCH: HOW ABOUT YOU?

Does your sponsor understand the risks to their data and their business?
Does your sponsor understand that security does not come for free?
Is your sponsor integrated in the 3rd party risk governance?
Is your sponsor talking to your CIO?

CORE ELEMENTS OF A VENDOR CYBER RISK MANAGEMENT FRAMEWORK

Governance, Controls, Audits, Remediation, Contract

GOVERNANCE

- Integrated governance: Business, Risk, CIO, CTO, DPO, 2nd Line of Defence, Audit
- Defined Cloud Strategy
- Centrally driven of 3rd / nth Party Risk & Compliance Governance

- Educate! What can happen if…
- Architecture and technical standards compliance
- Risk and controls compliance
- Operational suitability and operating standards compliance
- Centrally managed concentration risk

CONTROLS

- CISO / DISO / DPO / 2nd LoD agreed Cloud Requirements
- Based on standard Cloud Controls Framework
- Augmented for Controls required for CID, PII

- CSA CCM
- Temp. Privileged Access Mgmt.
- Multi-Factor Authentication
- HSM backed key vault with Customer Specific Keys
- Unstructured data classification and encryption and DLP
- Log immutability
- Records immutability

DETAILS ON TPAM, LOG CONTROLS

TPAM = Temp Priv. Access Mgmt.

- No permanent admin roles
- Requires case by case a ticket to request and release an admin role, also for root.
- Two independent approvers other than requestor
- With automated role granting (not manual)
- With automated expiry after less than 8 hours
- With strict segregation of roles i.e. separate and specific roles for HSM, key vault, identity and access management, log management, database configuration, database command line interface (querying), SDLC tasks, root.
- With strong MFA enforcement (not just OTP)

Log Immutability

- There are always two copies of the logs:
  - Operative log (which is accessed for regular operations)
  - Immutable log (WORM, which is NOT accessed normally but only upon exception)
- No admin role has or can get privileges to write, modify or delete entries on the immutable log
- Log maintenance must be an automated process which cannot be modified by any privileged role
- If write / modify / delete privileges are required on the operative log, then this must only be attainable via TPAM
- Client specific logs are real time available to the client without manual intervention by vendor

AUDITS

- Assessment of SaaS via controls not questions
- Evidence must be submitted
- Evidence is reviewed and challenged
- Control failures or gaps result in findings
- No evidence = finding

- Refusal to respond to controls with concrete explanations on how they are met, or to provide evidence results in no deal
- ISO 27001 / 17 is not audited and you do not get the detailed report
- SOC2 Type 2 is audited but it is configurable. You MUST get and yourself audit the report.

REMEDIATION

- Findings must be remediated
- Remediation requires design proposals which are reviewed, challenged for effectively addressing the finding
- Closure of finding requires evidence of effective remediation and positive re-assessment of control
- No remediation = no deal
- Inappropriate remediation = back to square one

CONTRACT

- Tight standard clauses for information security and data protection
- Every finding results in remediation clauses
- Exit clause triggered by inappropriate remediation
- Contract performance is conditional on information security controls being met
- Any violation or breach automatically trigger the exit clause

EXPERIENCE AND CASE STUDIES

Persistence and perseverance can save your data

LEADING TRADING PLATFORM

Concerns

- No TPAM, no MFA, all data commingled in single database with TDE, no pen test, no SOC2
- Very “nosy” contacts
- We are the best and only platform
- Business sponsors escalated and escalated
- Audit issue raised by us

Audit & Remediation

- 1 year assessment with long list of findings
- Top management negotiations and agreement reached
- 1 year of remediation with subsequent evidences
- Implemented segregation of database, TPAM, MFA, CSK based encryption, pen test, SOC2

Incident

- Ransomware attack
- Successfully brought down the entire platform at month end trading
- Our data was not impacted due to remediation enforced

GLOBAL CONSULTANCY COMPANY

Concerns

- Multiple proposed engagements with same company
- Refusal to answer controls, provide evidence
- One large scale contract was business critical
- Very long list of findings
- Audit issue raised by us

Audit & Remediation

- Sponsor was educated about the risks by us
- Worked with Business Sponsor to engage top management at both sides
- Top management at Consultancy Company understood criticality and within 3 months presented design change proposals
- Contract locked in the proposals, delivery ok.

Business Impact

- Delay of engagement due to initial refusal to cooperate: 2 years
- There was a cost in mid 7 digit frame but this was considered adequate for the gain in information security
- Consultancy company co-invested and is now actively leveraging the enhanced security model to market their solution.

WHAT TO DO

Integrated Governance: Business, Risk, CIO, CTO, CTO, DPO, 2nd LoD, Audit Top Mgmt.

Educate repeatedly, cite examples, show risks & impact

The CIO is your friend and Audit is your best supporter

Audit controls and evidence, demand remediation, challenge vendors and your business

Enforce tough decisions: there is no free lunch

CONTROLS ENFORCEMENT

Large Corporates / Institutions

- Use an industry standard control framework such as CSA CCM, add TPAM, for PII / CID: within jurisdiction storage & processing, Location Aware Access Controls
- Demand a clean SOC2 Type 2 or CSA Star L2 with all details and controls scope, plus an independent pen test with remediation confirmation, which are renewed annually and given to you in full detail
- Audit the controls and insist on detailed feedback with supporting evidence, raise findings, ask for remediation
- Demand design change proposals and nail them in the contract with sanctions and exit clause
- Review implementation of the design changes
- Review continuously adherence to the controls and design agreed

Small & Mid Sized Entreprises

- Demand a clean SOC2 Type 2 or CSA Star L2 with all details and controls scope, plus an independent pen test with remediation confirmation, which are renewed annually and given to you in full detail
- Demand implementation with evidence of MFA, TPAM, Log Immutability, TLS encryption in transit and HSM based data at rest encrpytion
- If you process PII or CID in the SaaS: demand for and ask for proving evidence of within jurisdiction storage and processing and Location Aware Access Control for all users including support staff, including privileged / admin roles
- Nail the above concretely in your contract with sanctions and exit clause
- Annually review adherence to the controls

THE INSTRUMENTS

- Engage with external organisations active in cloud risk governance, management and control
- Join forces with others: the more you exchange experiences on governance, the more you make cooperation transparent to vendors, the more clout (not cloud) you will have

- Familiarise yourself with an industry leading controls framework, e.g. CSA CCM
- Familiarise yourself with the SOC2 Type 2 controls and audit methodology
- Familiarise yourself with pen test methodology
- Leverage existing controls and auditing frameworks:
  - Start with the 12 Golden TOMs
  - Expand into CSA CCM, SOC2 Type 2, CSA Star L2
  - On the horizon: CSA EATO Certification

THANK YOU FOR PARTICIPATING.

I WILL SUPPORT YOU IN BUILDING YOUR CLOUD RISK GOVERNANCE

Rolf A. Becker

contact@cloudriskgovernance.ch