Event Tech Vendor **Security Questionnaire Template**

30 questions to evaluate event tech vendors on data residency, security, and compliance

How to use this checklist

This template gives procurement and IT security teams a structured way to evaluate event tech vendors on the questions that actually determine whether the vendor will pass a security review. Most vendor evaluations rely on SOC 2 reports and a general security summary. This template goes deeper into the specific operational and contractual commitments that separate vendors who have built for regulated buyers from vendors who claim compliance through marketing.

Bring this template into your vendor evaluation process. For each of the 30 questions, record the vendor's response, score it from 1 (vague or evasive) to 5 (specific, in writing, with documentation). Each question includes a "strong answer" guide and "red flags" guide so you know what to listen for.

How to read the scores

Each question is scored 1-5, with a maximum total of 150 points across all six categories. Category subtotals (each out of 25) help identify where a vendor is strong or weak. The total score matters less than the pattern: vendors who score well on data residency and contract rights but poorly on incident response are usually overselling their security posture. Vendors who score consistently across all categories are usually shipping production-grade security.

Pass/borderline/concern thresholds are defined on the summary page at the end of this template.

Vendor information

Vendor name _____

Date of review _____

Evaluator name _____

Jurisdiction requirements _____

Data Residency and Storage

QUESTION 1

Who built the integration, and who maintains it?

What a strong answer sounds like:

The vendor's own engineering team owns the integration. They can tell you when it was last updated and what is on the integration roadmap.

Red flags to watch for:

"In the cloud" or "secure data centers" without specifics. "We use AWS" without a region named.

Vendor response	
Score (1-5)	
Notes	

QUESTION 2

Is the data replicated to other regions for backup, disaster recovery, or performance, and if so, where?

What a strong answer sounds like:

Vendor lists every region where replicas exist, distinguishes between primary, backup, and read replicas, and confirms whether replicas can be opted out of for residency-sensitive deployments

Red flags to watch for:

“We replicate for performance” without naming the regions. Vague language about “global infrastructure” without a specific list.

Vendor response	
Score (1-5)	
Notes	

QUESTION 3

Under which legal jurisdiction(s) can our data be accessed, and by whom?

What a strong answer sounds like:

Honest about the dual-jurisdiction reality. Names the country where the cloud provider operates (e.g., AWS data centers in Canada are subject to Canadian law for stored data, but AWS Inc. is US-based and may receive US government data requests for that data).

Red flags to watch for:

“We’re SOC 2 compliant” used as a deflection. Refusal to acknowledge cross-border legal access risks.

Vendor response	
Score (1-5)	
Notes	

QUESTION 4

What happens to our data at contract end? What's the export and deletion process?

What a strong answer sounds like:

Defined timeline for data export (e.g., 30-60 days), specific formats (CSV, JSON), confirmation that replicas are also deleted, no additional fees for export. Documented in the master agreement.

Red flags to watch for:

Export available "for an additional fee." No specific timeline. Deletion only of primary data, not replicas.

Vendor response	
Score (1-5)	
Notes	

QUESTION 5

Where are backups stored, and how long are they retained?

What a strong answer sounds like:

Backups stored in the same region as primary data unless explicitly contracted otherwise. Retention period defined (e.g., 30 days, 90 days). Backup deletion confirmed at contract end.

Red flags to watch for:

Backups stored “wherever provides best performance” without buyer control. No defined retention or deletion practice for backups.

Vendor response	
Score (1-5)	
Notes	

Encryption and Access Controls

QUESTION 6

Is data encrypted at rest, and what encryption standard is used?

What a strong answer sounds like:

Yes, AES-256 or equivalent. Encryption enforced by the cloud provider's native encryption services. Encryption also active on backups.

Red flags to watch for:

"We use encryption" without naming the standard. Encryption optional rather than default.

Vendor response	
Score (1-5)	
Notes	

QUESTION 7

Is data encrypted in transit, and what protocol version?

What a strong answer sounds like:

Yes, TLS 1.2 minimum, with TLS 1.3 preferred. Enforced for all endpoints, including admin and API access. HTTP fallback disabled.

Red flags to watch for:

TLS 1.0 or 1.1 still supported. HTTP fallback available for legacy clients.

Vendor response	
Score (1-5)	
Notes	

QUESTION 8

How are encryption keys managed?

What a strong answer sounds like:

Keys managed by the cloud provider's KMS (e.g., AWS KMS). Customer-managed keys (CMK) available for buyers who require them. Key rotation automated.

Red flags to watch for:

Keys stored in the application alongside the data. No CMK option for sensitive buyers.

Vendor response	
Score (1-5)	
Notes	

QUESTION 9

Is multi-factor authentication enforced for admin access, and how?

What a strong answer sounds like:

MFA required for all admin accounts. Supports TOTP and hardware tokens (e.g., YubiKey). Cannot be disabled by individual admins. SMS-only MFA discouraged or unavailable.

Red flags to watch for:

MFA optional. SMS-only MFA (which is vulnerable to SIM swapping). Admins can disable MFA on their own accounts.

Vendor response	
Score (1-5)	
Notes	

QUESTION 10

What's the access control model, and how quickly are credentials revoked when employees leave?

What a strong answer sounds like:

Role-based access control with least-privilege defaults. Documented offboarding procedure that revokes access within a defined window (e.g., same day, end of next business day). Logged and auditable.

Red flags to watch for:

All-or-nothing access ("admin" vs "user"). No documented offboarding procedure. Manual credential revocation that takes days or weeks.

Vendor response	
Score (1-5)	
Notes	

Vulnerability Management and Incident Response

QUESTION 11

How often does the platform undergo vulnerability scanning, and by whom?

What a strong answer sounds like:

Continuous automated scanning (e.g., weekly or daily), plus annual third-party penetration testing by a named firm. Internal security team reviews and triages findings.

Red flags to watch for:

“Annual security review” without specifics. No third-party testing. No defined scanning cadence.

Vendor response	
Score (1-5)	
Notes	

QUESTION 12

What's the patching cadence for security vulnerabilities?

What a strong answer sounds like:

Critical vulnerabilities patched within a defined SLA (e.g., 48 hours). High-severity within 7-14 days. Documented patch management policy, applied across primary and backup systems.

Red flags to watch for:

"We patch as needed" without defined timelines. Customer must request patches. Patching dependent on next release window.

Vendor response	
Score (1-5)	
Notes	

QUESTION 13

How does the vendor detect and respond to security incidents?

What a strong answer sounds like:

24/7 monitoring with named SIEM (e.g., Splunk, Datadog). Defined incident response runbooks. Trained on-call response team. Tabletop exercises conducted at defined intervals.

Red flags to watch for:

“We monitor for security events” without specifics. No documented incident response process. No on-call coverage outside business hours.

Vendor response	
Score (1-5)	
Notes	

QUESTION 14

What's the customer notification timeline for confirmed breaches, and is it in the contract?

What a strong answer sounds like:

72 hours or less, written into the master agreement. Notification includes scope, impact assessment, affected data types, and remediation steps. Aligned with GDPR and provincial breach notification requirements.

Red flags to watch for:

"We monitor for security events" without specifics. No documented incident response process. No on-call coverage outside business hours.

Vendor response	
Score (1-5)	
Notes	

QUESTION 15

Has the vendor had any publicly disclosed security incidents in the last 24 months? If so, what was the response?

What a strong answer sounds like:

Vendor discloses any incidents transparently, describes the response and timeline, and details the changes made to prevent recurrence. If no incidents, says so directly without qualification.

Red flags to watch for:

Refuses to answer. Evasive on whether incidents have occurred. Cites confidentiality without explaining what they would disclose under NDA.

Vendor response	
Score (1-5)	
Notes	

Availability and Disaster Recovery

QUESTION 16

What's the platform's uptime commitment, and is it in the SLA?

What a strong answer sounds like:

Defined uptime percentage (typically 99.9% or higher), measured against documented criteria, with service credits or penalties for failure to meet. Public uptime dashboard available.

Red flags to watch for:

"We have high availability" without specific commitment. SLA only available on enterprise plans. No public uptime tracking.

Vendor response	
Score (1-5)	
Notes	

QUESTION 17

Are backups geographically separated from primary data?

What a strong answer sounds like:

Yes, backups in a separate availability zone within the same region (for residency-constrained deployments) or across regions (where allowed). Documented backup architecture.

Red flags to watch for:

Backups stored in the same data center as primary data. No geographic separation. Single point of failure for both primary and backup.

Vendor response	
Score (1-5)	
Notes	

QUESTION 18

What's the documented Recovery Time Objective (RTO) for service restoration after a major outage?

What a strong answer sounds like:

Specific time commitment (e.g., 4 hours for full service restoration). Demonstrated in past incidents or DR testing. Customer-specific RTO available for larger deployments.

Red flags to watch for:

"We can restore quickly" without a specific commitment. No RTO documented in the contract.

Vendor response	
Score (1-5)	
Notes	

QUESTION 19

What's the Recovery Point Objective (RPO) for data loss in a major incident?

What a strong answer sounds like:

Specific time commitment (e.g., 15 minutes maximum data loss). Achieved through frequent backup or transactional replication. Tested through DR exercises.

Red flags to watch for:

"Minimal data loss" without specifics. Daily backup as the only data protection mechanism (which means up to 24 hours of data loss is acceptable to the vendor).

Vendor response	
Score (1-5)	
Notes	

QUESTION 20

How are planned maintenance windows scheduled and communicated?

What a strong answer sounds like:

Maintenance windows scheduled with at least 7 days notice. Performed during low-traffic hours for the customer's region. Status page updates throughout the window. Emergency maintenance defined and communicated separately.

Red flags to watch for:

Maintenance with no advance notice. No status page. Maintenance windows during business hours for the customer's region.

Vendor response	
Score (1-5)	
Notes	

Privacy Compliance and Data Handling

QUESTION 21

Which privacy regulations does the vendor's platform comply with (GDPR, PIPEDA, US state laws, HIPAA, etc.)?

What a strong answer sounds like:

Specific list of regulations with the compliance posture for each (e.g., "GDPR compliant as a data processor, can sign DPA"). Documented in a public privacy posture statement. Updated as new laws come into force.

Red flags to watch for:

"We comply with all major regulations" without specifics. Refusal to sign DPAs. Privacy posture documented only on request.

Vendor response	
Score (1-5)	
Notes	

QUESTION 22

Can the vendor provide a current list of all sub-processors, and how are sub-processor changes communicated?

What a strong answer sounds like:

Documented retention schedule by data type. Customer-configurable retention for jurisdiction-specific requirements (e.g., Canadian buyers can set Canadian retention rules; EU buyers can apply GDPR-compliant retention).

Red flags to watch for:

Single global retention policy with no customization. Indefinite retention by default. No mechanism to enforce jurisdiction-specific retention.

Vendor response	
Score (1-5)	
Notes	

QUESTION 23

How does the vendor handle data subject requests (access, deletion, portability)?

What a strong answer sounds like:

Documented process for handling DSRs within statutory deadlines (e.g., 30 days for GDPR). Customer self-service tools for DSR fulfillment where possible. Audit trail of DSR responses.

Red flags to watch for:

DSRs require a support ticket and human review. No SLA on response time. No customer-side tooling for DSR fulfillment.

Vendor response	
Score (1-5)	
Notes	

QUESTION 24

How does the vendor handle data subject requests (access, deletion, portability)?

What a strong answer sounds like:

Documented process for handling DSRs within statutory deadlines (e.g., 30 days for GDPR). Customer self-service tools for DSR fulfillment where possible. Audit trail of DSR responses.

Red flags to watch for:

DSRs require a support ticket and human review. No SLA on response time. No customer-side tooling for DSR fulfillment.

Vendor response	
Score (1-5)	
Notes	

QUESTION 25

For Canadian customers specifically, is there a process for handling Quebec Law 25 impact assessments?

What a strong answer sounds like:

Vendor has a documented Law 25 compliance posture. Can support customer impact assessments with required information about cross-border transfers (if any), the legal basis for processing, and applicable safeguards.

Red flags to watch for:

“We’re GDPR compliant so Law 25 is fine” (these are different frameworks). No specific guidance for Quebec customers. No support for impact assessments.

Vendor response	
Score (1-5)	
Notes	

Contract and Audit Rights

QUESTION 26

Does the vendor support security audit rights in the contract?

What a strong answer sounds like:

Customer right to audit included in the master agreement, either directly or via third-party auditors. Reasonable notice required (e.g., 30 days). Cost-sharing terms defined based on findings.

Red flags to watch for:

Audit rights not included in the master agreement. Audits only allowed via SOC 2 report review. Customer-initiated audits require separate negotiation.

Vendor response	
Score (1-5)	
Notes	

QUESTION 27

What third-party audit reports does the vendor provide, and how recent are they?

What a strong answer sounds like:

Current SOC 2 Type II report (within the last 12 months) available under NDA. ISO 27001 certification or similar if applicable. Penetration test summary available. Reports refreshed annually.

Red flags to watch for:

SOC 2 report older than 18 months. No third-party reports available. Reports available only on extended request.

Vendor response	
Score (1-5)	
Notes	

QUESTION 28

How quickly does the vendor respond to security questionnaires during the customer relationship (not just procurement)?

What a strong answer sounds like:

Documented response SLA for security questionnaires (e.g., within 10 business days). Dedicated security questionnaire resource or platform. Faster response for existing customers.

Red flags to watch for:

Questionnaires routed through sales and answered ad hoc. Long delays during active customer relationship. No SLA on response time.

Vendor response	
Score (1-5)	
Notes	

QUESTION 29

What security provisions are required to be included in the master agreement?

What a strong answer sounds like:

Vendor's standard MSA includes data processing agreement, breach notification, audit rights, sub-processor restrictions, security warranties, and termination for cause. Customer can negotiate enhancements.

Red flags to watch for:

Security provisions require separate negotiation. Vendor's MSA has weak default security terms. Standard MSA does not include a DPA.

Vendor response	
Score (1-5)	
Notes	

QUESTION 30

What are the exit and data portability terms in the contract?

What a strong answer sounds like:

Documented exit process. Defined data export formats (CSV, JSON). Customer-controlled migration timeline. No exit fees. Deletion verification within a defined window after termination.

Red flags to watch for:

Exit fees apply. Vendor-controlled migration timeline. No data deletion verification. Export formats limited or proprietary.

Vendor response	
Score (1-5)	
Notes	

Scoring Summary

Question	Score (1-5)
DATA RESIDENCY AND STORAGE	
Q1: Where is data physically stored?	
Q2: Replication to other regions?	
Q3: Legal jurisdictions for data access?	
Q4: Export and deletion at contract end?	
Q5: Backup storage and retention?	
Data residency and storage subtotal (out of 25)	
ENCRYPTION AND ACCESS CONTROLS	
Q6: Encryption at rest standard?	
Q7: Encryption in transit protocol?	
Q8: Encryption key management?	

Q9: MFA enforced for admin access?	
Q10: Access control and offboarding?	
Encryption and access controls subtotal (out of 25)	
VULNERABILITY MANAGEMENT AND INCIDENT RESPONSE	
Q11: Vulnerability scanning cadence?	
Q12: Patching cadence and SLA?	
Q13: Incident detection and response?	
Q14: Breach notification timeline?	
Q15: Past security incidents and response?	
Vulnerability management and incident response subtotal (out of 25)	
AVAILABILITY AND DISASTER RECOVERY	
Q16: Uptime commitment and SLA?	

Q17: Backup geographic separation?	
Q18: Recovery Time Objective?	
Q19: Recovery Point Objective?	
Q20: Planned maintenance communication?	
Availability and disaster recovery subtotal (out of 25)	
PRIVACY COMPLIANCE AND DATA HANDLING	
Q21: Privacy regulation compliance?	
Q22: Sub-processor list and notification?	
Q23: Data retention customization?	
Q24: Data subject request handling?	
Q25: Quebec Law 25 support?	
Vulnerability management and incident response Privacy compliance and data handling subtotal (out of 25)	

CONTRACT AND AUDIT RIGHTS	
Q26: Security audit rights in contract?	
Q27: Third-party audit reports?	
Q28: Questionnaire response SLA?	
Q29: MSA security provisions?	
Q30: Exit and data portability terms?	
Contract and audit rights subtotal (out of 25)	
OVERALL SCORE (out of 150)	

Pass / Borderline / Concern Thresholds

120+	Pass	Vendor meets the security review bar. Most categories scored 4 or 5. Move forward with the evaluation.
90-119	Boderline	Vendor has gaps in one or more categories. Identify which categories scored below 15 and have a follow-up conversation on those specifically before moving forward.
Below 90	Concern	Vendor is unlikely to pass a serious security review. Other options should be evaluated. If this is the only viable vendor, expect a long compliance remediation cycle.

Observation and Decision Notes