DRAFT Vendor Bring Your Own Key (BYOK) Solution Guidance

9 Misconceptions about Bring Your Own Key (BYOK)

1: Bring Your Own Key is an industry standard security control

The term 'BYOK' is not endorsed by any technical or governmental **standards body** (e.g. **NIST**, **IETF**, **ISO**, CSA). BYOK is a marketing term that includes a range of non-standard vendor solutions. Vendor solutions not standardised; the key import mechanisms are implemented differently and these mechanisms have different benefits and tradeoffs. It is not a standard control, and as such vendors have different approaches to the key import mechanism. Since there is no standard, our organisation may be required to use algorithms and encryption mechanisms not supported by our HSMs, requiring the use of software generated keys or exporting the keys from the HSM in order to wrap them.

2: Bring Your Own Key is an appropriate solution for all 3rd party cloud provider

Usage of vendor BYOK solutions that are not fit-for-purpose will increase the risk of data disclosure. For example, encryption material can be disclosed during exchange which will exposure data to disclosure, and accidental destruction of keys can lead service outages and data loss.

3: Our data is more secure if our organisation 'owns the encryption keys'

Ownership of encryption keys does not mean that data is protected from disclosure or compromise. Many factors influence the strength of controls provided by data encryption: secure key lifecycle management, encryption algorithm, encryption key length and the effectiveness of playbooks to respond to events that put data at risk. Our 'ownership' of keys doesn't matter if the vendor can still access them. Providing vendors with our organisation-generated keys for data encryption and decryption will provide no security benefit and could increase operational risk. The entire lifecycle of encryption keys needs to be assured to realise the benefits of data encryption

4: Vendors will not be able to read our data if we use BYOK

The most robust BYOK solutions will not always prevent vendors of malicious external parties reading our data. In cases where the vendor needs to unencrypt data to deliver their services (e.g. to process the data or to present the data), our data will remain vulnerable to insider vendor threats and external vendor compromise.

5: BYOK will mitigate 'silent subpoena' data security risks

If the vendor needs to unencrypt data to deliver service to our organisation, our data could be extracted and sent to a 4th party without our knowledge in response to a silent subpoena

6: BYOK protects our organisation data from compromise if a supplier is impacted by a security incident

If the vendor needs to unencrypt data to deliver service to our organisation, our data will remain vulnerable to insider vendor threats and external vendor compromise.

7: There is less of a need for other security controls if a vendor provides a BYOK solution

Storage and processing of our organisation data by 3rd parties will expose our organisation to a range of security threats. Data encryption will address a small number of these threats. A full range of security controls is required to reduce the operational risk of using 3rd parties to process and store our organisation data.

8: BYOK involves a single encryption key

The most robust BYOK solution designs include multiple keys that have different purposes. BYOK schemes may employ Key Exchange Keys, Key Wrapping Keys and Data Encryption Keys.

9: If BYOK is used, our organisation can decrypt and use the data if we exit a vendor relationship, or they cease operating

If this is a requirement then it should be captured as part of the contract, tested and validated to confirm this will be possible.

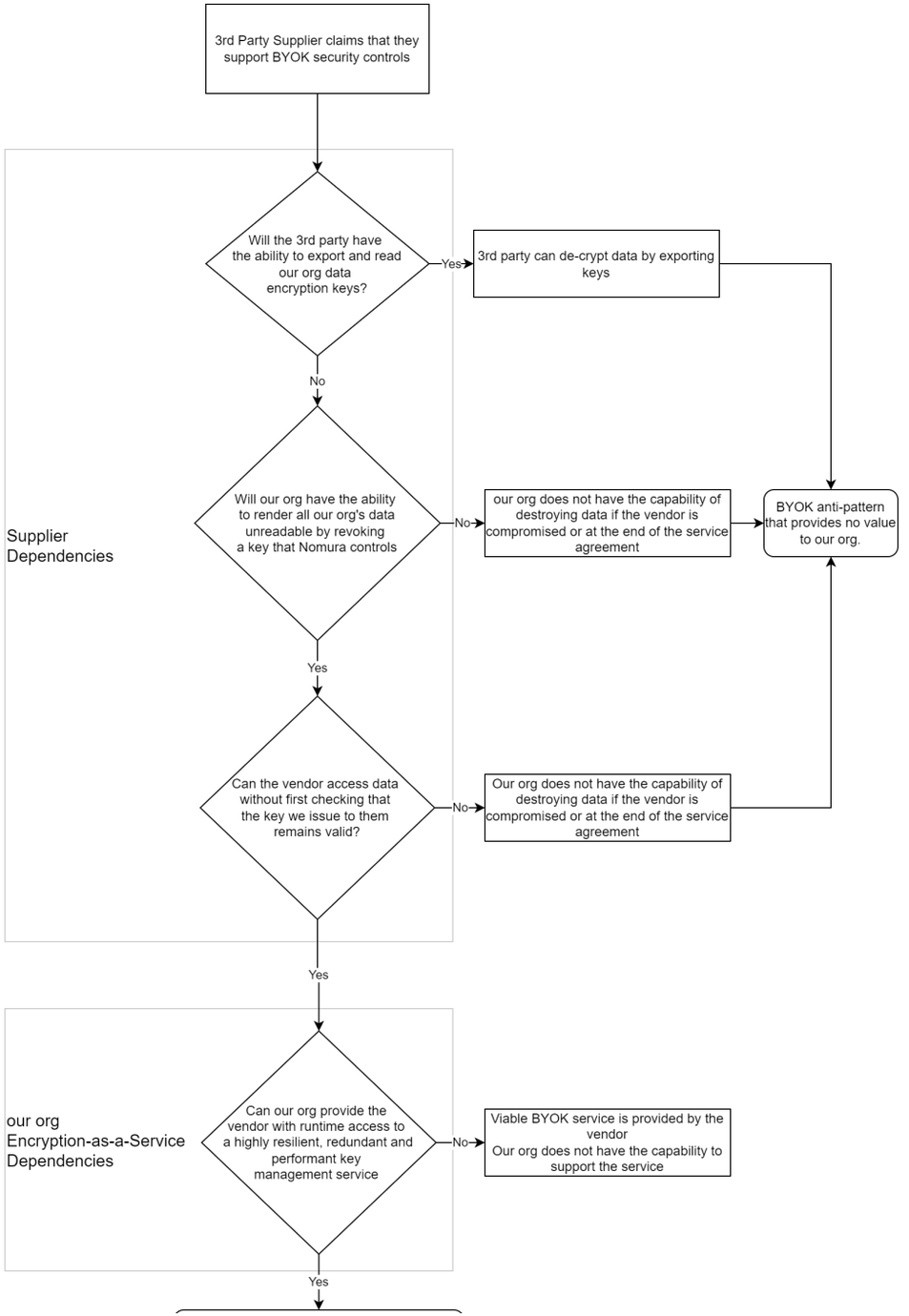
BYOK Recommendations

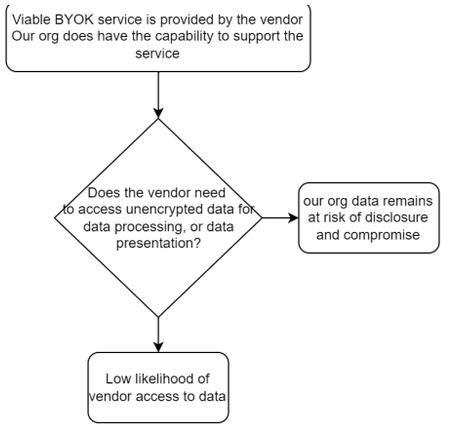
1. ***BYOK should not be mandated for all third-party cloud providers.*** BYOK is an appropriate solution for a limited number of circumstances and should only be considered if the BYOK solution has been assessed as fit-for-purpose. A security assessment and / or a threat model will determine if a vendor solution provides real security benefit for our organisation. These assessments will also identify cases where the use a vendor BYOK solution will actually increase the operational risk that our organisation is exposed to.
2. ***our organisation must challenge vendors that claim that their BYOK solutions address our security concerns***. Asking the vendor if it is technically feasible for them to access our data unencrypted will inform.
3. ***Well-implemented BYOK is a niche solution that is only appropriate for a limited number of use cases.*** A security assessment and / or a threat model will determine if a vendor solution provides real security benefit for our organisation. These assessments will also identify cases where the use a vendor BYOK solution will actually increase the operational risk that our organisation is exposed to.
4. our organisation must

Characteristics of a Robust BYOK Solution

1. The vendor does not have the ability to read or export encryption keys
2. Human handling of key material is avoided
3. our organisation can render all vendor-hosted data unreadable by revoking a key that we control

BYOK Solution Vetting Decision Tree


3rd Party Supplier claims that they support BYOK security controls
Supplier Dependencies
Will the 3rd party have the ability to export and read our org data encryption keys?
Yes
3rd party can de-crypt data by exporting keys
No
Will our org have the ability to render all our org's data unreadable by revoking a key that Nomura controls
No
our org does not have the capability of destroying data if the vendor is compromised or at the end of the service agreement
BYOK anti-pattern that provides no value to our org.
Yes
Can the vendor access data without first checking that the key we issue to them remains valid?
No
Our org does not have the capability of destroying data if the vendor is compromised or at the end of the service agreement
Yes
our org Encryption-as-a-Service Dependencies
Can our org provide the vendor with runtime access to a highly resilient, redundant and performant key management service
No
Viable BYOK service is provided by the vendor
Our org does not have the capability to support the service
Yes


Viable BYOK service is provided by the vendor
Our org does have the capability to support the service
Does the vendor need to access unencrypted data for data processing, or data presentation?
our org data remains at risk of disclosure and compromise
Low likelihood of vendor access to data