QUICK GUIDE

Supplier or cloud provider reports a security issue - what now?

Seven questions for the first steps

A software vendor reports a critical vulnerability. A cloud provider reports a cyber incident. A supplier points to an affected component.

These notifications come from outside your organisation. The decisive questions arise inside it: Does this affect us specifically? What do we know for certain? What information is missing? And who needs to take ownership now?

This Quick Guide helps you structure the initial intake.

It structures the first information before you move into a detailed technical, contractual, regulatory or product-specific assessment.

7	QUESTIONS	1	INITIAL INTAKE	2	FOLLOW-UP PATHS

Information status: September 2026

Free Quick Guide · no registration required

IMPORTANT FIRST

For an acute incident, use your incident / emergency process

STOP NOTICE

If an active attack, major outage, acute threat or a possible security incident affecting your own organisation is already present, this Quick Guide must not delay your existing incident or emergency process.

THE SEVEN QUESTIONS AT A GLANCE

1. **What exactly was reported?**
2. **Which service, product or component is affected?**
3. **Where do we use it?**
4. **What is confirmed - and what is still unclear?**
5. **What information do we still need from the provider?**
6. **Who needs to take ownership internally?**
7. **What do we need to document - and when do we review again?**

SCOPE BOUNDARY

The guide does not replace technical incident response, legal advice or a case-specific CRA, NIS2, data protection or other reporting assessment.

QUESTIONS 01-02

Secure the incoming signal and the concrete context

01 What exactly was reported?

Start with the original information - without jumping to conclusions.

CAPTURE / CHECK

- Date and time received
- Sender and source
- Supplier or provider
- Type of notification
- Advisory ID, ticket or CVE, if available
- Urgency stated by the provider
- Original notification or link

GUIDING QUESTION

Is this a vulnerability, a confirmed incident, a precautionary warning, a patch notice or general information?

GOAL: Be able to distinguish the original notification from internal conclusions.

02 Which service, product or component is affected?

A general warning becomes actionable when it can be linked to a concrete technical or contractual context.

CAPTURE / CHECK

- Product, service or platform
- Affected component
- Version, build or firmware
- Hosting or service variant
- Region, environment or tenant, where relevant

GUIDING QUESTION

Is the exact variant we use affected - or does the notification concern a different product or version?

QUESTIONS 03-04

Separate your own exposure from the information status

03 Where do we use it?

This is where an external notification becomes a question of your own exposure.

CAPTURE / CHECK

- Affected application or business process
- Your own product or technical solution
- Site, business unit or customer
- Relevant data or interfaces
- Connected or dependent systems
- Critical business function

GUIDING QUESTION

Which specific dependency of our own could be affected if the notification applies?

GOAL: Do not stop at knowing that the provider is affected; understand your own use and dependency.

04 What is confirmed - and what is still unclear?

Separate confirmed facts, assumptions and open information.

CONFIRMED

- affected version known
- patch available
- specific service confirmed
- specific variant confirmed unaffected

ASSUMPTIONS

- "We probably use a different version."
- "Our data is probably not affected."
- "The provider will fully resolve this."

OPEN

- no exact version information
- exploitability unclear
- no statement on subcontractors
- no data / time-period statement
- no next update date

RULE OF THUMB

Missing information is not positive security evidence.

QUESTIONS 05-06

Missing provider information and internal ownership

05 What information do we still need from the provider?

Not every situation requires the same depth of assessment. Depending on use and criticality, relevant information can include:

CAPTURE / CHECK

- Exact affected products, services or versions
- Technical description of the vulnerability or incident
- Timing, duration and known exploitation
- Patches or mitigation measures
- Possible impact and affected data / services
- Subcontractor or component involvement
- SBOM / VEX information
- Next provider update and closure information

GUIDING QUESTION

Which missing information do we need for our own assessment or decision?

06 Who needs to take ownership internally?

A provider email should not get lost between inboxes.

CAPTURE / CHECK

- IT / Information Security
- Product Security / Development
- Procurement / Supplier Management
- Data Protection
- Quality / Compliance
- Incident Management
- Product Owners
- Management or approval authority

GUIDING QUESTION

Who has the necessary subject-matter information - and who can decide on measures, risk, approval or escalation?

GOAL: Assign one clear owner instead of merely forwarding the message.

QUESTION 07

Document, decide and review again

07

What do we need to document - and when do we review again?

A case is not complete just because the first email has been answered.

CAPTURE / CHECK

- Incoming signal
- Provider, service or component
- Your own context and dependency
- Confirmed facts
- Open questions
- Information requested
- Responsible owner
- Immediate measures initiated
- Decision or escalation
- Next review date
- Closure information once available

GUIDING QUESTION

How will we be able to show later why we made this decision - and whether new information should trigger reassessment?

INITIAL INTAKE COMPLETE?

A controlled initial status does not mean that the case is professionally closed.

- A clear owner has been assigned
- Your own use or dependency has been identified
- Confirmed facts and information gaps are separated
- A next measure or escalation has been defined
- A review date or closure criterion is known

REMEMBER

New provider information, a changed version, a patch, an additional incident finding or a regulatory assessment can trigger reassessment.

WORKSHEET

Initial intake

Compact working block for completion or printing.

Event / notification

Date / time

Supplier / provider

Affected service / product / component

Version / configuration

Owner

Our use / dependency

Confirmed facts

Assumptions

Open questions / missing evidence

Immediate measures

Next review

Status / closure

NEXT TOPIC PATH

Which path is relevant next?

The initial intake helps move the case into the appropriate context for further work.

A · SUPPLIER / SAAS / CLOUD / SERVICE

Supplier and third-party cybersecurity

If the main issue is an operational dependency on an external provider, the next step typically covers:

- Criticality
- Supplier assessment
- Contractual requirements
- Evidence
- Vulnerability / incident interfaces
- Monitoring and changes
- Exit and resilience

Learn more about Supplier Cybersecurity

B · THIRD-PARTY COMPONENT IN YOUR PRODUCT

Cyber Resilience Act

If software, firmware or a component is part of your own product with digital elements, relevant topics can include:

- Product and version context
- Product security
- Vulnerability assessment
- Security updates
- Evidence
- Where applicable, CRA reporting

Learn more about the Cyber Resilience Act

BOUNDARY

Both paths can overlap. The key distinction is whether the security notification primarily concerns an external dependency of your organisation or whether the affected third-party component is part of your own product with digital elements.

LIMITS AND NEXT STEPS

When is this Quick Guide not enough?

Use the appropriate internal process or specialist support if, for example:

- an active attack or major security incident may be underway
- the technical impact cannot be assessed
- critical systems or services are unavailable
- sensitive or personal data may be affected
- a statutory, regulatory or contractual reporting obligation may apply
- an actively exploited vulnerability is involved
- supplier information remains contradictory or materially incomplete
- an approval or continued-operation decision is required despite significant unresolved risks

NEXT STEP

Continue with Supplier Cybersecurity

For suppliers, SaaS and cloud services, software vendors and other external dependencies.

www.sp-services-gmbh.de/en/supplier-cybersecurity/

Cyber Resilience Act for your own product case

If the affected software, firmware or component is part of your own product with digital elements.

www.sp-services-gmbh.de/en/cyber-resilience-act/

NOTE

This Quick Guide is intended for structured initial intake. It does not replace technical incident response, individual legal advice or a case-specific CRA, NIS2, data protection, contractual or other specialist assessment.