

02 - Monitoring and response

Choose what to monitor, which signals need attention and who will respond.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

1. How many devices should be monitored, and what types are they?

Include servers, firewalls, switches, access points and other supported devices. Give counts by type, vendor, model and version.

Answer

Source / owner / date

2. How many separate service checks are needed?

Count checks separately from devices. Identify each service, protocol, test location and expected result.

Answer

Source / owner / date

3. Where will monitoring data come from?

List collectors, source owners, approved read-only access and supported integrations such as SNMP or syslog.

Answer

Source / owner / date

02 - Monitoring and response

Choose what to monitor, which signals need attention and who will respond.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

4. Which business services depend on these systems?

Name their owners, important dependencies and the impact of an outage.

Answer

Source / owner / date

5. What should trigger an alert, and when is it resolved?

Give thresholds, timing, recovery rules, duplicate handling and maintenance windows.

Answer

Source / owner / date

6. How should alerts be prioritized?

Describe P1-P5 or your chosen severity levels, impact rules and who can change a priority.

Answer

Source / owner / date

02 - Monitoring and response

Choose what to monitor, which signals need attention and who will respond.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

7. What acknowledgment targets should we agree?

Give a proposed target for each severity and when its clock runs. Targets depend on the agreed coverage.

Answer

Source / owner / date

8. Who will review alerts during the required hours?

Give the staffed calendar, primary and backup contacts, handoff arrangements and team capacity.

Answer

Source / owner / date

9. What may the monitoring team do when an alert arrives?

Choose observation, notification, diagnosis or approved fixes. Specify permitted actions and who approves changes.

Answer

Source / owner / date

02 - Monitoring and response

Choose what to monitor, which signals need attention and who will respond.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

10. How should unresolved issues be escalated?

Give contact roles, channels, update timing and the route for missed targets or vendor help.

Answer

Source / owner / date

11. How much monitoring data should be kept, and where?

Estimate normal and peak event volumes. Give retention, storage location and sensitive-data restrictions.

Answer

Source / owner / date

12. How will you confirm that monitoring is ready?

Agree test events, a collector outage test, an inventory sample and the owner who will accept the results.

Answer

Source / owner / date