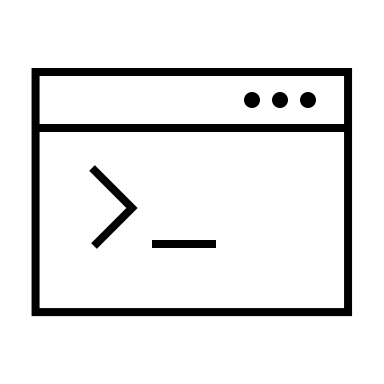
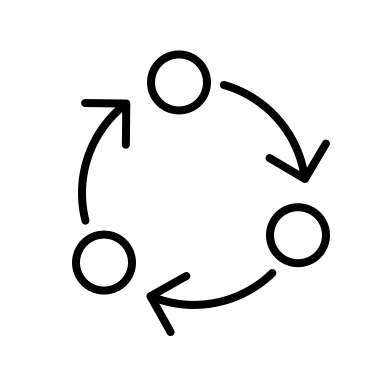
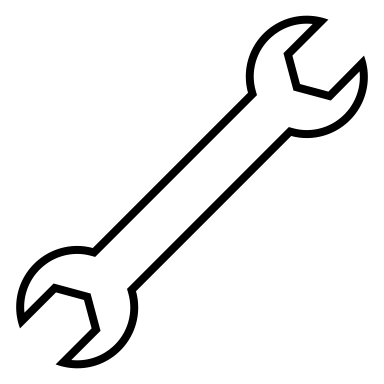
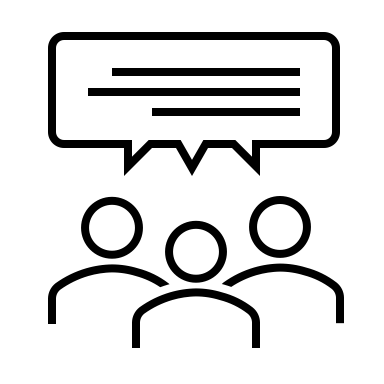
**[A blue and white sign

Description automatically generated](https://www.smartsheet.com/try-it?trp=12107&utm_source=template-word&utm_medium=content&utm_campaign=Sample+IT+Service+Desk/ITIL+Escalation+Matrix-word-12107&lpa=Sample+IT+Service+Desk/ITIL+Escalation+Matrix+word+12107)IT Service Desk / ITIL Escalation Matrix   
Template Example**



Software Installation Failure

As the initial point of contact for all IT issues, the service desk handles general inquiries and basic troubleshooting.

Tier 2 deals with more complex issues that require specialized knowledge or additional technical skills.

Tier 3 addresses high-level technical challenges involving system infrastructure or deep software problems.

**IT Service Desk (Tier 1)**

Tier X represents specialized external support or vendor-specific assistance for highly specialized issues.

**Tier 2 Support**

**Tier 3 Support**

**Tier X Support**

Network Downtime

Data Security Breach

Cloud Service Interruptions

Confirm system requirements and attempt basic reinstallation procedures.

Perform detailed diagnostics to identify conflicts or corrupt files. Test on alternative systems if necessary.

Review and rectify deep system settings or registry conflicts that could be preventing security system function.

Consult the software vendor for proprietary installation issues or to receive patches.

Check initial reports and confirm if the issue is widespread or localized. Reset routers or switches if applicable.

Analyze network logs and coordinate with internet service providers or internal network teams to pinpoint disruptions.

Implement advanced network recovery procedures and reconfigure core routing protocols.

Engage network equipment vendors for critical firmware updates or specialized diagnostics.

Log the incident, alert security teams, and initiate a preliminary data lock-down procedure.

Conduct an initial forensic analysis to assess the extent of the breach and identify compromised systems.

Lead comprehensive security audits and implement remediation strategies to secure all data points.

Work with cybersecurity firms for advanced threat detection solutions and mitigation techniques.

Verify service status with cloud providers and report outage details to users.

Assess API integrations and conduct checks on related services to ensure connectivity.

Coordinate with cloud engineers to restore services and manage data integrity checks.

Liaise with cloud service providers for detailed root cause analysis and to prevent future interruptions.

|  |
| --- |
| **DISCLAIMER**  Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk. |