# Root-Cause Analysis Template

A root-cause analysis should be completed after each Tier 1 or 2 incident. Additionally, it should be completed after each penetration test.

## Purpose

Use this section to explain briefly why this report is being filled out (i.e. What incident is it addressing? Data breach, penetration test, etc.)

### General Information

|  |  |  |  |
| --- | --- | --- | --- |
| Incident Number | Root-Cause Analysis Number | Location of Incident | People Who Worked on Incident |
| Text | Text | Text | Text |
| **Start Date/Time** | **End Date/Time** | **Duration** | Text |
| Text | Text | Text | Text |

## Summary of Incident

Give a brief recap of the incident in three to five sentences.   
(This section provides a succinct description of the “5 whys” noted in the TIP below.)

### Timeline of Activities

|  |  |  |
| --- | --- | --- |
| Date | Details | Contact for Activity |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Specifics of Root Cause

Describe the following:

* Services impacted
* Duration of incident
* Type of incident
* Severity level of incident
* Incident details

**TIP: Use this section to continue to ask “Why?” Why did this incident occur? After asking “Why?” five times, you will be at the root cause of the incident.**

### Corrective Measures

Highlight the specific technical components that need to be changed or adapted for this incident type.

### Areas of Improvement

Use this section to highlight areas of improvement for the response team. Focus mainly on process elements rather than technical details.

### Incident Response Contacts

|  |  |
| --- | --- |
| **Contact** | **Contact Information** |
| **End User** |  |
| **Service Desk** |  |
| **Third Party/Vendor** |  |
| **Security** |  |
| **SOC** |  |
| **CISO** |  |
| **IT Operations** |  |
| **Legal/PR** |  |
| **HR** |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.