IT-Vorfallmanagement bzw. IT-Incident Management umfasst typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. Das Spektrum möglicher Vorfälle reicht dabei von technischen Problemen und Schwachstellen bis hin zu konkreten Angriffen auf die IT-Infrastruktur. IT-Incident Management im engeren Sinne muss dabei sowohl organisatorische, als auch rechtliche sowie technische Detailfragen berücksichtigen.

Ziel des Incident-Management-Prozesses ist die schnellstmögliche Wiederherstellung der Service-Leistung (auch mit Workarounds).

Unter einem *Incident/Vorfall* versteht man nach IT Infrastructure Library (ITIL): "Ein Ereignis, das nicht zum standardmäßigen Betrieb eines Services gehört und das tatsächlich oder potenziell eine Unterbrechung dieses Services oder eine Minderung der vereinbarten Qualität verursacht."

Incidents werden mit Hilfe von Trouble Tickets dokumentiert. Für die Entgegennahme und Überwachung der Tickets ist ein Service Desk zuständig. (Quelle: Wikipedia)