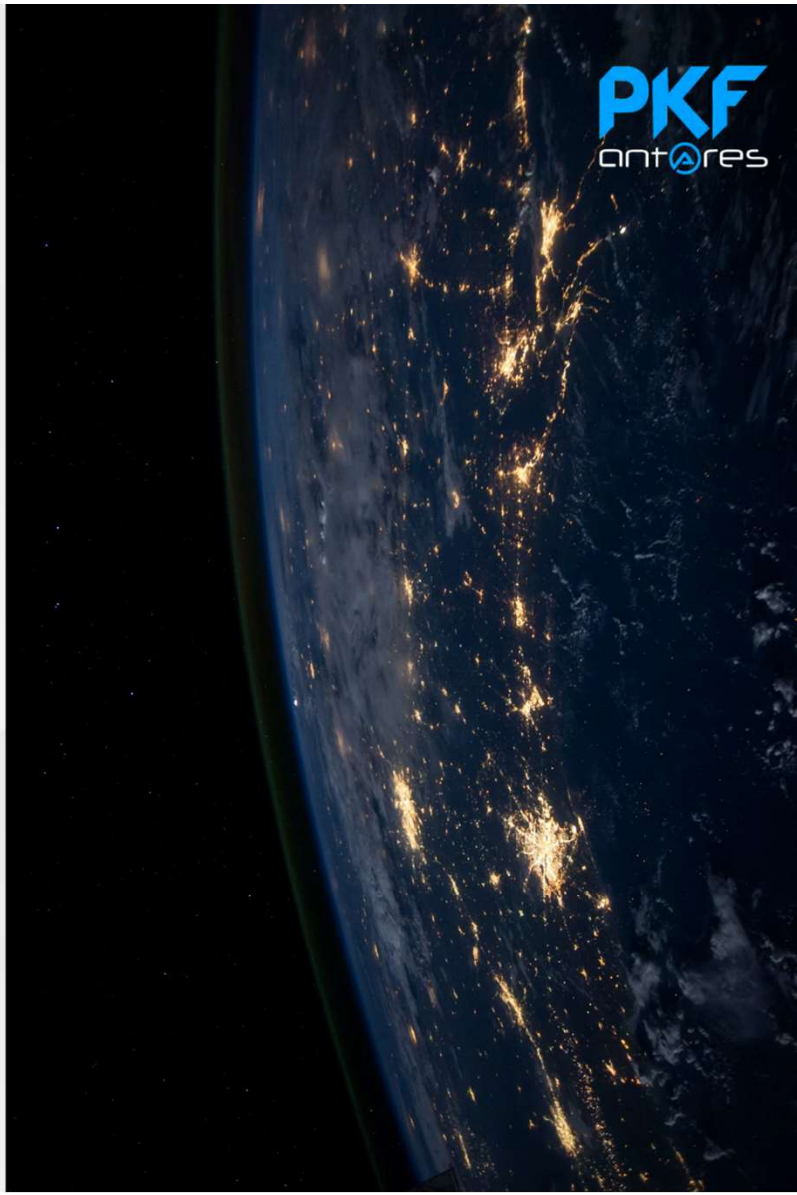
Cyber Incident Management

Mitigation, Recovery & Response

PKF Antares Advisory

Contents



Resilience and Incident Management

Cyber resilience is one of the fundamental elements in company's operations and related incident management is a mandatory process contributing towards successful business continuity.

Incidents are expensive and it could cause hinderances in business continuity by not only disrupting business operations but also, in the form of burden they place on staff.

Incidents are stressful, and they usually demand very intense intervention.

Effective incident management prioritizes preventive and proactive work over reactive work.

Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk

What is an Incident?

Incident is a multifaceted term. An Incident is any unplanned interruption, such as a ticket, a bug, or an alert.

In simplest of terms, incidents are the issues that:

- Are escalated (because they're too big to be handled alone)
- Require an immediate response
- Require an organized response

Monitoring and Alerting

Monitoring

The most common way you keep an eye over the health of the system is through Monitoring by:

- Collecting;
- Processing;
- Aggregating; and
- Displaying real-time quantitative data about a system (i.e. query counts and types, error counts and types, processing times, and server lifetimes).

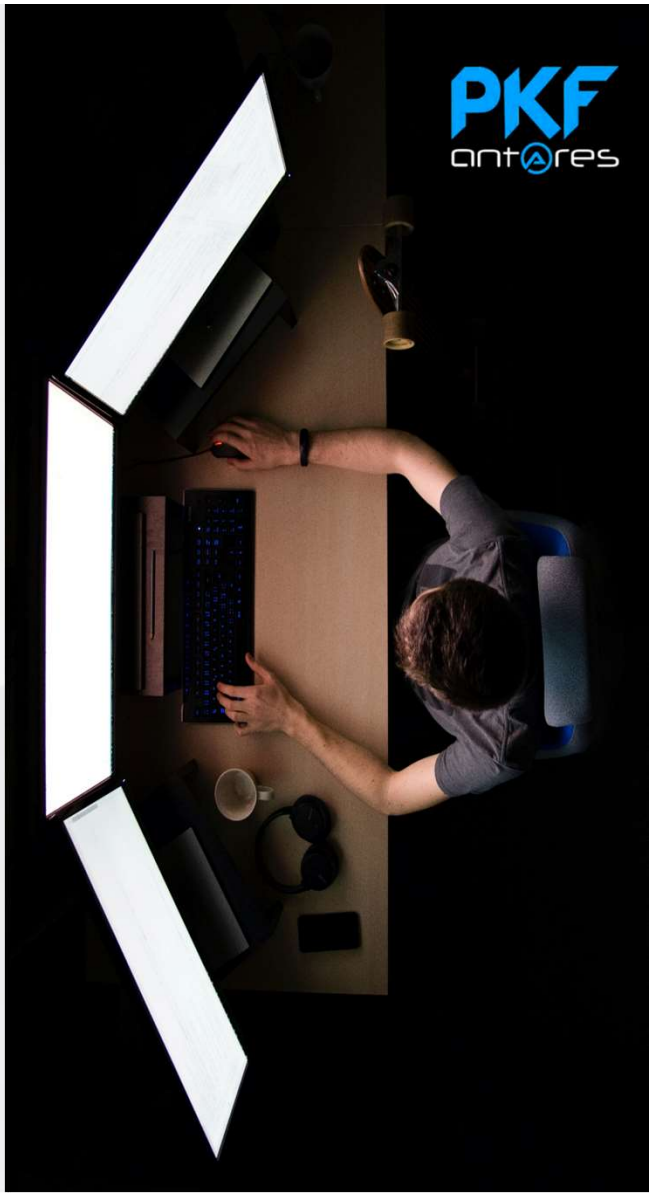
It is important that your focus is on measuring *reliability* and the *impact* on your users, instead of measuring the number of incidents that have been declared.

Alerting

Key component of monitoring: Alerting

When monitoring identifies abnormality or irregularity, the system sends an alert signal which could be:

- Something has malfunctioned and needs to be fixed; or
- Something might malfunction soon, so preventive steps need to be taken by having a assessment of the current situation.



The Importance of Actionable Alerts

The Company requires making nightly backups of your production database, so you set up a cronjob that runs every four hours to make those backups. One of those runs failed because of a transient error—the replica serving the backup had a hardware failure, and was automatically taken out of serving mode by the load balancer—and consequent runs of the backup completed successfully. A ticket is subsequently created as a result of the failed run.

Creating a ticket is unnecessary. This would only result in noise, since the system recovered itself without human interaction. This behavior is problematic, for a few reasons:

Toil
Someone had to spend time looking at the ticket, looking at graphs/reports, and deciding that they didn't need to do anything.

Alert fatigue
If 95% of the "Database backups failed" alerts are simply closed, there's a much higher risk that an actual problem will go unnoticed.

An incident is an issue with particular characteristics. An alert is merely an indicator that can be used to signal that an incident is underway. The Company might have many alerts with no incidents. In a situation like these, it doesn't mean the team needs to invoke a formal incident management techniques; however this is a planned maintenance event and the Company were expecting to receive these alerts as part of the maintenance process.

In real business scenarios, there are differences in how humans perceive **alerts** versus **incidents**:

- It's much more stressful to do formal incident management as opposed to simply fixing an alert.
- Less experienced responders are less likely to invoke an incident than more experienced responders.
- Incidents are much more likely to require additional team resources, so non-responders can more easily gauge whether they need to start looking at the active issue sooner rather than later.

You don't want to pollute these reports with all the alerts that you received. Consider the audience—alert metrics are primarily useful to the team, but incident reports will probably be read by higher-ups and should be scoped accordingly.

The Importance of Actionable Alerts

Good incident management means paying attention to the whole lifecycle of an incident. In this section, we discuss a programmatic approach to incident management

Mitigation and Recovery

01

This is the set of actions that allow a system to restore itself to a functional state. These include the urgent mitigations needed in order to avoid impact or prevent growth in impact severity. Recovery includes the systems analysis and reflection involved in conducting a postmortem. It is a written record of an incident, and it includes:

A) the actions taken;
B) impact;
C) root causes; and
D) follow-up actions needed to prevent recurrence and/or reduce future impact.

Readiness

02

This encompasses all the actions a company or team takes to prepare for the occurrence of an incident. This can include:

- *safety measures on engineering (code reviews or rollout processes);*
- *incident management training;*
- *experiments or testing exercises that are conducted to identify errors. This also includes setting up any monitoring or alerting.*

Response

03

This is what happens when the trigger causes the root cause of the hazard to become an issue. It involves:

a) responding to an alert;
b) deciding whether the issue is an incident;
c) communicating about the incident to impacted individuals.

Practicing Incident Response Readiness

Disaster Role-Playing and Incident Response Exercises

In Disaster Testing program, there might be tests deemed too risky to be executed. However, over time, by focusing on the areas exposed by these risky tests, many of these risks shall be addressed thoroughly and eventually they become automated and teams take them as business-as-usual.

Regular Testing

The most important benefit of Regular Testing is allowing the Company to observe a decrease in the number of high-risk tests. Reduction of high-risks test is a positive sign i.e. the Company have made their systems much more resilient, to the point where finding weaknesses is becoming harder and less probable.

Preparing Responders

Preparing the responders include writing a code or bot to execute a series of commands and check an expected response.

Running incident response tests can help identify such processes, assign a probability and risk factor, and instill confidence in responders. Even if a particular test did not go as planned, the participants will gain better visibility into where the weaknesses of the incident response processes.

Responders will also be better prepared technically, mentally, and emotionally for real incidents.

Nuanced Testing

Testing is now slowly shifting from fixing purely technical problems (e.g., “Do we know how to restore from a totally corrupt database?”) to a much more nuanced “Let’s fix processes” set of challenges.

Practicing Incident Response Readiness (Continued)

Writing Incident Response Tests

The starting point for writing incident response tests is to look at recent incidents. Ask these standard questions on every post-mortem:

What went wrong?

What went right?

Where did we get lucky?

What went wrong: since that's clearly an area that needs improvement. These tend to be concrete problems that are easy to fix i.e. the monitoring picked up an issue but didn't page anybody. Once the issues identified and fixed, the responders need to test the fix. This point cannot be overemphasized: merely fixing an issue is not enough; there were cases when the fix may be incomplete, or the fix has caused a regression somewhere else.

When testing for correctness, start with small, relatively simple tests. As confidence in the process increases, the Company can start looking at more complex issues, including those that aren't entirely technical in nature (i.e., human processes).

Mitigation and Recovery

In real life after an incident has occurred, the Company must start focusing on urgent mitigations.

Urgent Mitigations

To stop or lessen user impact during a service breakage, the Company would like to have certain sections ready to go to its staff and clients which allows to reduce the impact of a wide variety of outages while the team is figuring out what needs to be fixed.

The mitigations that are most applicable to the service vary, depending on the pathways by which the users can be impacted. Some of the basic building blocks are: A) the ability to roll back a binary; B) drain or relocate traffic; and C) add capacity. These Band-Aids are intended to buy more time so that the team can figure out a meaningful fix which can fully resolve the underlying issues.

SLI (Service Level Indicator)	SLA (Service Level Agreement)	SLO (Service Level Objective)

Reducing the Impact of Incidents

The customers and external users are less worried about incidents or the number of incidents. What they do they really care about is RELIABILITY.

Therefore its required to align the actions for each stage in the incident management lifecycle (readiness, response, and recovery). Its critical to think about the things that can be done before, during, and after the incident to improve the systems.

Defining Targets

While it's very subjective to measure the customer trust, there are some proxies the Company can use to measure how well the Company is providing a reliable customer experience. We call the measurement of customer experience a service-level indicator (SLI) which tells how well the service is doing at any moment in time.

The reliability target for an SLI is called a service-level objective (SLO). An SLO aggregates the target over time i.e it shows during a certain period the target level and how well the Company is performing against these targets.

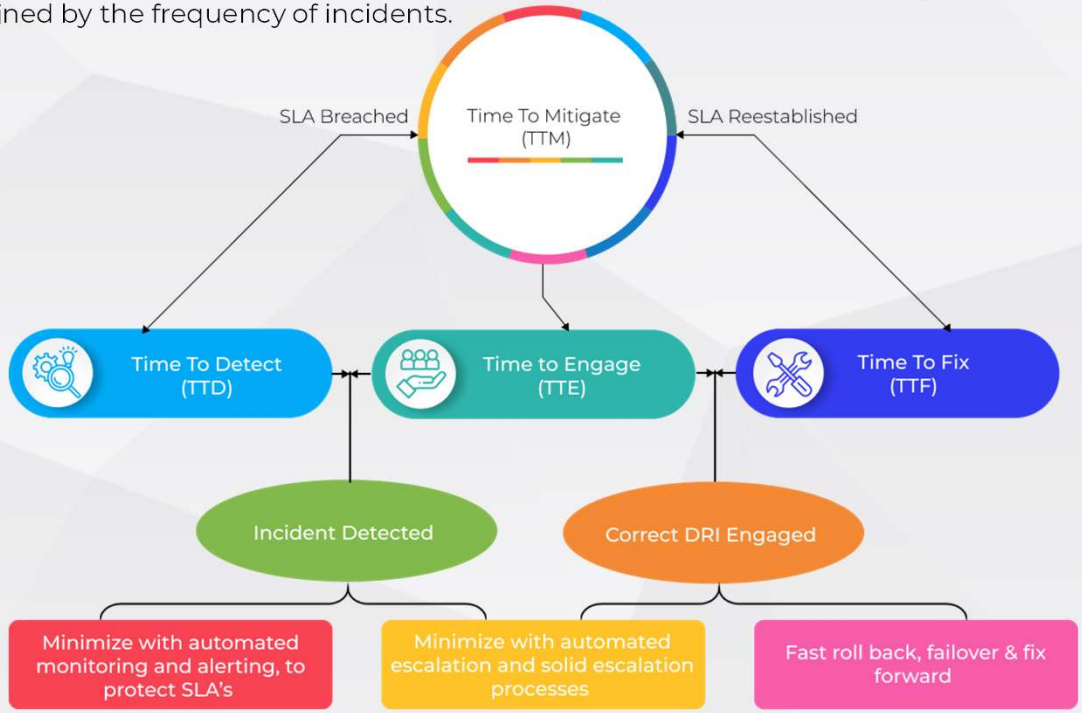
Service-level defines the level of service you expect from a vendor, laying out the metrics by which service is measured, as well as remedies or penalties that are agreed-on service levels not be achieved. In order to maintain SLA, you need SLOs to be more restrictive than your SLAs

Mitigation and Recovery (Continued)

Calculating Impact

Incidents impact the reliability target. They are affected by the quantity of failures, the length and the radius of the blast, and the "size" of these failures. Hence, its critical to understand the activities that will reduce the impact.

To measure the impact, you calculate the time that you are not reliable. This is the time it takes for you to detect that there is an impact, plus the time it takes to repair (mitigate) it. You then multiply this by the number of incidents, which is determined by the frequency of incidents.



Mitigation and Recovery (Continued)

Calculating Impact (Continued)

The key metrics are time to detect, time to repair, and time between failures:

- Time to detect (TTD) is the amount of time from when an outage occurs to some human being notified or alerted that an issue is occurring.
- Time to repair (TTR) begins when someone is alerted to the problem and ends when the problem has been mitigated. The key word here is mitigated! This doesn't mean the time it took you to submit code to fix the problem. It's the time it took the responder to mitigate the customer impact; for example, by shifting traffic to another region.
- Time between failures (TBF) is the time from the beginning of one incident to the beginning of the next incident of the same type.

Thus, reducing impact means reducing the four axes in the following equation—TTD, TTR, TBF, and impact.

This translates, to reduce the impact of incidents and enable systems to recover to a known state, you need a combination of technology and "human" aspects, such as ***processes*** and ***enablement.***

$$Unreliability = \Sigma \frac{TTD + TTR}{TBF} \times Impact$$

How PKF Can Help?

We come in as domain experts who assess your incident management lifecycle in terms of - preparedness, response, and recovery

If you already have a Security Incident & event management, solution we bring in our experts to establish correlations that adapt as per your changing business needs, making Cyber security more pragmatic for your businesses.

We help executives develop a cyber risk program in line with the strategic objectives and risk appetite of the organization.

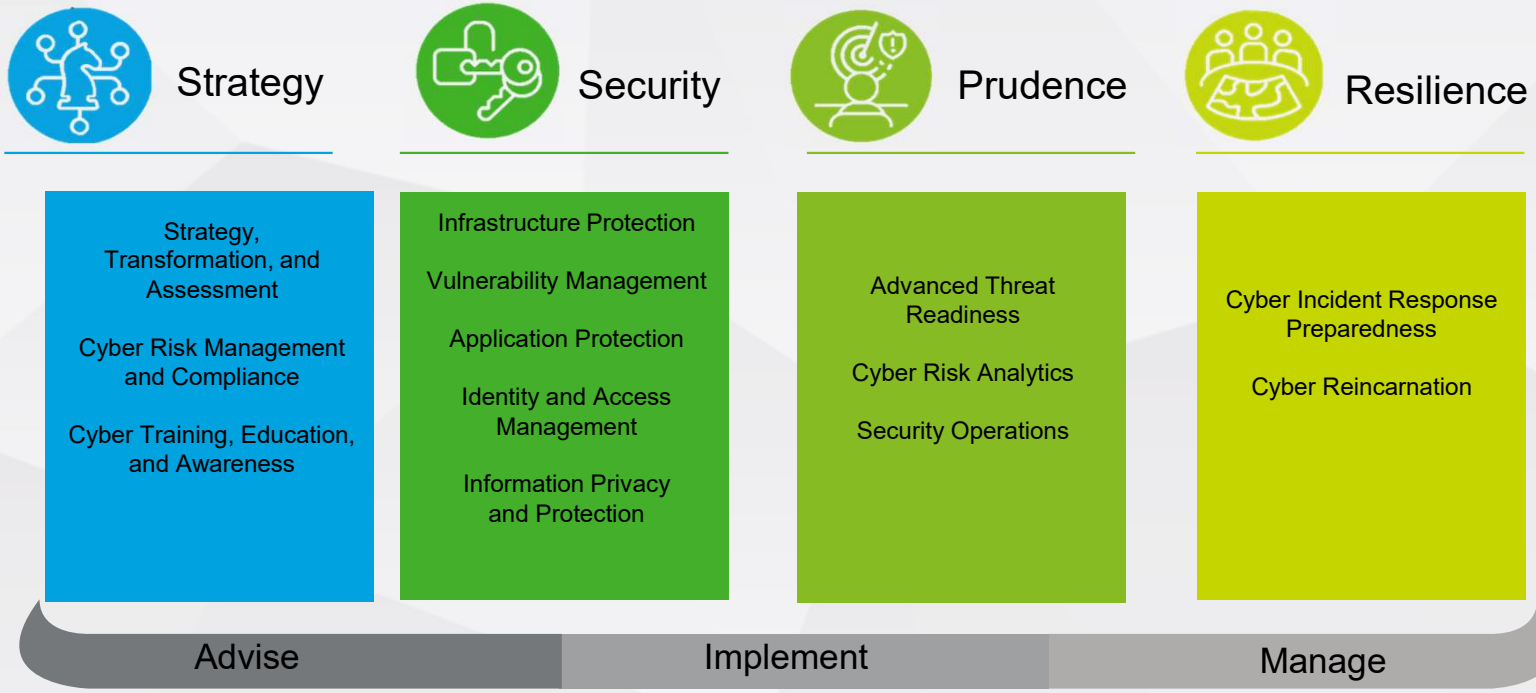
We focus on establishing effective controls around the organization's most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth, and cost optimization objectives.

We combine proven proactive and reactive incident management processes and technologies that help customers rapidly adapt and respond to cyber disruptions whether from internal or external forces.

How PKF Can Help?

PKF's Cyber Management Portfolio

PKF delivers its promise, through a thoughtfully curated portfolio of services, spanning across 4 key pillars of **Strategy, Security, Prudence & Resilience**



Delivery Channels