Ultimate Guide to Incident Management
Incident Management: A Process

Preparations are made. Drills are run. Protocols are in place.
And then it happens—despite your organization’s best efforts, a superbug takes hold.
Seventeen patients fall ill. One dies.

The outbreak is brought under control, but now you have to deal with the costs—the impact on patients and their families… lawsuits and their fallout… reputation damage. Even simply finding out what happened and why will take time, effort and money.

But there’s good news. The whole situation—from how you prepare for the worst, to what you do when it’s happening, to how you move forward when it’s over—is a known process.

That process is called incident management.

What Is an Incident?

Incidents come in different shapes and sizes. Here are some examples of the most common types of incidents.

**Natural**
Hurricane · Flood · Earthquake

**Human-driven**
Terrorism · Fraud · Patient escape

**Uncontrolled (“accidents”)**
Fire · Personal injury · Outbreak
Preparation and Response

Incident management is your preparation for and your response to (as well as your actions after) a breach in hospital security.

It’s how you handle a server crash and what you do to minimize the risk of one happening again.

Incident management can be as small as a recurring issue with slips and falls in the parking lot, or as big as a medevac crashing on the roof.

In a nutshell, incident management is everything your organization does to identify, respond to, manage, document, analyze and correct incidents—adverse events, occurrences or situations—of any kind.
Incident Management, Stage 1

**Plan and Prepare**

There are four stages in a mature incident management process:

1. Plan and prepare
2. Respond
3. Document
4. Investigate

In the first, you’ll define the threats your hospital faces—what kinds of risks are you exposed to, what’s the likelihood that those risks could come to pass, and what impacts would you see if one or more of those threats became an actual incident?

You’ll then work to implement countermeasures, which are strategies and tactics you could implement if a risk became a reality, and safeguards—protections you put in place to try to prevent things from happening in the first place.

In addition, this first phase also encompasses measuring, in the unlikely event of an actual incident, the effectiveness of those countermeasures and safeguards. It also involves doing further planning and preparation based on what you learn or discover.

You may already be familiar with a quality improvement model called the Deming cycle, in which you Plan, Do, Check and Act as a way of constantly learning and improving. This model serves incident management well—by consistently setting goals, implementing, learning lessons and adapting, you’ll be better able to deal with any incidents that rear their heads.

**Common Incident Management Terms**

- **Threat**: any potential incident
- **Frequency**: how often the incident happens (or, if you’d like, how likely it is to happen)
- **Impact**: the costs of an incident happening (related not just to money but to people, effort, reputation, etc.)
Incident Management, Stage 2

Respond

By the time you realize you’re in the Respond stage of the incident management process, it may already be too late. (That’s why proper planning and preparation in stage 1 is so critical.)

Don’t worry, though—the reality is that capital-I Incidents are rare. Most incidents you’ll ever deal with are the farthest things from catastrophes.

Big or small, however, the process of responding is essentially the same:

1. Let your response team know that an incident is in progress (or has taken place).
2. Initiate standard operating procedures (developed ahead of time to help you keep cooler heads under pressure).
3. Send emergency notifications if necessary.
4. Mobilize response personnel if necessary.
5. Update data about the incident, either on the fly during prolonged incidents, or afterwards in the case of shorter ones.
6. “Clear” the incident when your response is finished.
Incident Management, Stage 3

Document

Stage 3 of the incident management process is about documenting what happened. In this stage, you’ll:

- Thoroughly capture a record of the event or events that took place.
- Compile statistical reports.
- Perform a root cause analysis if you can.
- Summarize any corrective actions you took.
- Share what you’ve learned with the relevant parts of your organization so others can learn from what took place.

Imagine a security breach in the maternity ward. To document the incident, you’d start by completing an incident report, noting:

- General details, including any narrative accounts you wish to include.
- Any information about linked incidents (for example, a failure of the security maglock system, or a flu that left the ward understaffed).
- A summary of the impacts of the incident, and more.

You’ll then make a decision about whether to investigate or not. If yes, it’s time to move on to the fourth stage.

With an effective incident management system, you can roll accurate incident data right into your security risk assessment program.
Incident Management, Stage 4

Investigate

In the last stage of the process, it’s time to put your detective hat on. Here you—or perhaps a dedicated investigations team—will be capturing statements from involved participants or witnesses, monitoring evidence, looking at data, and more.

In a nutshell, you’re trying here to get to the bottom of what happened, why it did, and how to prevent a similar incident from occurring again.

Occasionally this stage isn’t necessary—many incidents can be handled and resolved by first responders without escalation. Depending on the incident, however, you may indeed need an investigator or investigation team to step in to uncover more than what was initially reported.

By thoroughly investigating, your organization will be better able to determine how and why the incident happened. And as more incidents occur over a period of time, you may discover common patterns or themes, identifying a larger problem than you knew existed.

This investigation, monitoring and management of a single incident (or a group of them) will help you take preventive action to keep something similar from happening again.

Data mining, investigative queries... you need the power to determine who was involved and when, how something happened and why.
Incident Management and Risk

“Risk” is a broad term, but, generally speaking, the level of risk that your organization can be said to face is calculated this way:

the likelihood that an incident could cause damage or loss

multiplied by

the size of that potential damage or loss.

Risk management, then, is the process of determining what level of risk is acceptable, and what actions should be taken to mitigate the risks that your organization considers unacceptable.

The incident management process, in turn, is critical to risk management. Without incidents, there would be no risk, and risk management would be unnecessary. Clearly, this isn’t the case.

The goal, then, is not to eliminate incidents—but to manage them and reduce their impact.

To do so, rely on the Plan-Do-Check-Act cycle described above. After an incident—often aided by incident management software—plan and implement a countermeasure, then gauge its effectiveness while you monitor incident activity.

You can then plan how to mitigate future risk... and the cycle will continue.
Incident Management and Performance

In theory, the “perfect” risk management program would reduce all incidents—and the loss and damages caused by them—to zero.

In reality, perfection is unattainable. You can, however, examine historical data and set realistic performance goals.

For example, if your hospital has been victim to an average of 18 internal thefts per year over the last three years, with a total loss value of $50,000, you might set the following next-year goals:

- A reduction in incidents of 50%, meaning your baseline measure would be 9 events
- A reduction in loss of 70%, meaning your baseline measure would be $15,000

The math seems like common sense, but unfortunately this level of clarity can be hard to achieve. With an overwhelming volume of data available, your incident management program can quickly bog down.

Incident management software can help greatly. By enabling you to glean insight from the chaos of incident data and investigation reports, the right software can make it much easier to set—and achieve—performance targets.
Incident Management and Intelligence

Better data is the key to better performance.

But how to get it? And once you have it, how can you turn it into actual business intelligence? After the fact, investigators all too often find that the “big answer” was hiding in the data all along.

Reliably moving from identifying small insights to seeing the big picture is difficult—but it’s easier with software.

The right application can easily help you:

- Reduce guesswork by revealing complex associations hidden in your data.
- Display data visually for easier analysis and interpretation.
- Identify additional relationships between various data points.
- Turn large volumes of data into actionable intelligence that can lend clarity to complex investigations.

Again, the Plan-Do-Check-Act cycle comes into play here. By identifying the goal or target of your investigation before you collect data, using software to visualize and analyze that data, disseminating your findings for review and taking action based on what you find, you’ll more easily collect the intelligence you need to make informed risk decisions.

The more data you have the more you’ll be able to cross-reference and compare, and the more meaningful your conclusions will be.
Diving Deeper: Six Questions To Ask

Keep these six questions in mind as you move through the PDCA cycle; not only will they help you manage incidents and risk, they will themselves make moving through the cycle easier.

1. **Has the incident happened before?**
   How many times has the incident occurred? Has it continued to happen since implementing countermeasures? What was your benchmark for the number of times it was acceptable for the incident to recur?

2. **If it has, what was the impact on your organization?**
   Consider direct losses and indirect ones, both on a per-incident basis and across a full year. Remember, too, several minor incidents with a higher frequency may have a larger impact than a single major one.

3. **Is the incident likely to happen again? If so, how often?**
   What is the estimated frequency of the incident?

4. **What would the impact be?**
   What is the potential impact of the incident occurring again—either once or several times?

5. **What countermeasures are currently in place to prevent the incident from happening again?**
   How effective are they? Are they appropriate, given the level of risk associated with a recurrence?

6. **What further steps can be taken to mitigate the risk of the incident's recurrence?**
   Are your current countermeasures enough? Do you need to increase their intensity or put others in place?

The answers to these six questions will provide you with powerful tools for making knowledge-based, data-driven decisions—a key factor in the success of your incident management effort.
Diving Deeper: Why Data Matters

The right data will help you get a handle on incidents and reduce their occurrence.

That means if you’re not already collecting it, or are doing so in a way that doesn’t make it easy to analyze your numbers for insight, you should consider implementing a data collection and analysis initiative as soon as possible.

Don’t let the scope of the task intimidate you—incident management software can make gathering data orderly and convenient, and can greatly increase the ease with which you can analyze your numbers for trends.

And if you are considering software, look for these features:

• An easy interface to help users enter incidents and activities.

• The ability to visualize incident information to help you gain insight from what you’re analyzing.

• Custom alerts and business process automation enabling faster response to incidents as they happen.

• Dispatch functionality to alert and manage responders.

• Investigation management features to help you assign investigators, launch investigations, and track metrics.

When gathering data to support incident management becomes easy—and the ability to analyze it quickly and accurately is suddenly within reach—your ability to reduce incidents will increase exponentially.
Diving Deeper: From Data to Information

When mined for indicators and trends, data can help you understand why specific metrics are different from one period to another.

For example, a series of brownouts could indicate a concerning issue—unless an analysis of the data revealed the brownouts happened during a heat wave when the power grid was already overly stressed. This kind of insight can help guide decision-making; perhaps you don’t need to install new generators after all.

But turning data into information can serve another purpose—it can help you gain support for your incident management program. By giving you the ability to easily demonstrate loss reductions or a decreasing trend in security incidents, you’ll more quickly gain the organizational support, resources or recognition you deserve.
Diving Deeper: From Data to Information [continued]

How much more would your program be appreciated if you could quickly answer questions like these:

- What types of incidents are occurring the most, and how much are they costing your hospital?
- Is the hospital on track to meet incident-reduction goals in Q3?
- Are losses for a particular business area up, down or steady?
- Where are incidents occurring with the highest frequency and greatest impact?
- On what days and times might more security officers be required?
- Have countermeasures instituted in the Q1 taken effect yet?

With the right analytical software, you can easily and constantly analyze data on incidents, losses and investigations, viewing automatically generated graphs and charts. Statistics that might have taken days or weeks to prepare using conventional database queries will suddenly become instantly available.

And that means, of course, that the next time “they” ask, you’ll not only have an answer...

You’ll have an impressive one.
The Case For Incident Management Software

Incident management software, and the data collection and analysis that the software supports, serves three primary purposes:

1. Risk management
2. Performance management, and
3. Intelligence and investigations.

Arguably the most important of these is the third.

By discovering and understanding how information connects —gaining intelligence—and acting on security incidents that affect their organizations—investigating—you’ll do a better job at the other two.

That’s an increasingly easy conclusion to come to. After all, the sheer volume of data now available to today’s incident manager points to the use of software for intelligence and investigative purposes. Gathering the data, assessing it, and making sense of it—these processes have grown increasingly difficult to accomplish without appropriate tools.

The rewards to be reaped by implementing software, however, are great—the ability to see what was previously invisible can improve both operations and strategy.
Using Software For Intelligence And Investigations

Managing incidents and conducting investigations is, to some extent, guesswork—you can try to make informed decisions and take actions based on facts, but that’s not always entirely possible.

It’s a lot easier, however, when you have the best data possible. That’s why more and more professionals are using incident management and investigative software to quickly and effectively track data and analyze it in search of meaningful patterns.

Proof is elusive—a definitive conclusion built on a foundation of facts isn’t always discovered the first time around, if at all.

But using a database that draws from all areas of the organization and the right software, you can:

- Reduce guesswork by revealing complex associations hidden in your data.
- Visually display data for easier analysis and interpretation.
- Quickly identify additional relationships between large volumes of disparate data.

The result?

Actionable intelligence that brings clarity to complex investigations and scenarios.
Resolver: Your Incident Management Backbone

The foundation of good risk management is superior incident management. At Resolver, we understand that—which is why we power incident management and risk management for 1000 of the world’s largest organizations.

By focusing your efforts on what matters most and eliminating unnecessary activities, Resolver enables you to find the right balance between managing incidents and being overwhelmed by them.

In short, it helps you build the incident management program that works for your business—driving insight, and protecting value where it matters most.

For over a decade, we have provided organizations like yours with incident management, internal control, internal audit, compliance management, and risk management solutions that create efficiencies and make businesses more effective.

We make it simple for companies to manage incidents proactively—and to demonstrate and document their efforts to internal and external stakeholders.

When you partner with Resolver, you’ll leverage the power of the most complete incident management and risk management software in the cloud—and a team of risk, compliance, and security experts supporting customers across 100 countries.

Reach your full potential with Resolver. Manage incidents. Expand your insights. Make better decisions. Confidently meet and exceed your objectives.
Want to learn more? Let’s talk.

resolver.com | info@resolver.com | 1-888-891-5500

About Resolver: Over 1,000 of the world’s largest organizations use our cloud software to protect their employees, customers, supply chain, brand and shareholders. Resolver’s Integrated Risk Management platform helps plan and prepare your organization to limit the likeliness or impact of events from occurring; this includes Risk Assessment, Enterprise Risk Management, Internal Control, Internal Audit and Compliance. We also support the response and recovery process when an event does occur; including Incident Reporting, Incident Response and Investigations. Resolver’s team is comprised of security, risk and compliance experts supporting customers across 100 countries with offices in North America, United Kingdom, Asia-Pacific and the Middle East.