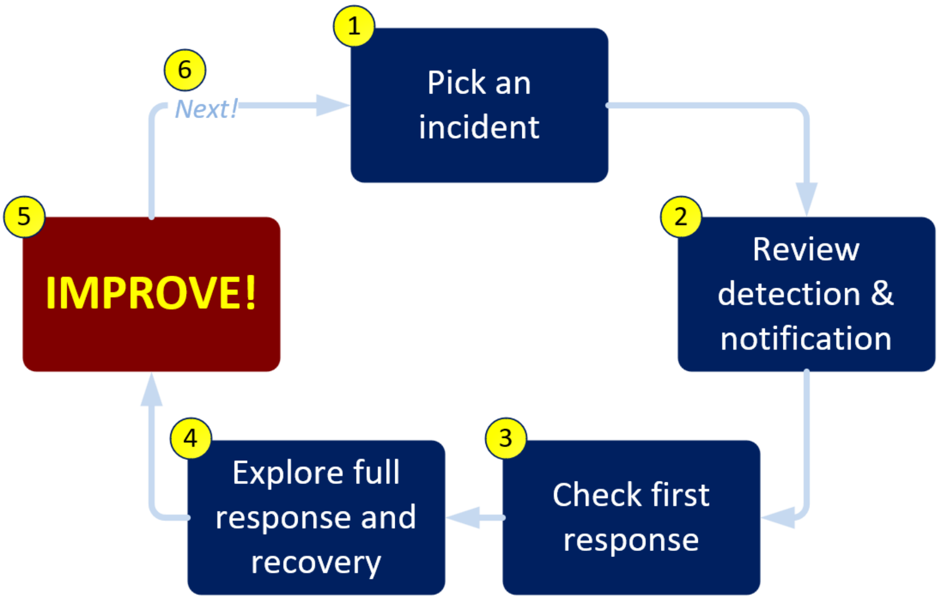
Iterative risk analysis

This pragmatic information risk analysis process or method blends risk, security, incident and problem management, creatively combining imaginary with actual data and concerns to prompt security improvements.


1
Pick an incident
2
Review detection & notification
3
Check first response
4
Explore full response and recovery
5
IMPROVE!
6
Next!

1. *Imagine* you have experienced a 'typical' incident affecting whatever [information] asset/s you are risk-assessing - such as a physical incident affecting the office computers. Consider various types of incident of differing scales and importance *e.g.* an office break-in, vandalism, professional hit, insider theft, fire, flood ... whatever. For now, pick out an example, a type of incident of greatest concern for further consideration – perhaps a recurrence of a real incident that has actually happened. Start considering the associated causes (threats acting on vulnerabilities) and effects (business impacts) and press on ...

Start the process by identifying information asset/s and risks of concern

2. Focus on the chosen incident. In that scenario, what would indicate that it had taken place? How soon would it be discovered - when, by whom and how? What detective measures would help *e.g.* alarms, warnings, indicators? Consider the possibility of gradual or non-obvious incidents (*e.g.* overloaded power cables smouldering out of sight, or occurrences where everybody is busy and assumes someone else is responsible) and deliberately concealed incidents (*e.g.* information, media or equipment thefts by workers, intellectual property theft, spying). Are you *sure* that detection is sufficiently reliable, and that such incidents would be reported quickly and efficiently?

Think about incident detection and reporting

3. What would the immediate response be? What would *you* do first? Who else should be involved or informed? What would assist or impede the response? Use the incident scenario to consider the 'first responder' phase of the incident. If it helps, run a desktop walk-though or exercise to check things out realistically, perhaps recreating the original incident. How might this stage be made better, faster, clearer?

Check the first response

4. How would the incident be stopped, investigated and resolved? Again, consider who, what, when, how, why ... What information and skills would be essential or most valuable for the investigation (*e.g*. records, logs, CCTV footage, forensics, fire investigators)? What could or would be done to minimise the damage and get things back to normal ASAP? What would be priorities for the business, and why those?

Explore the full incident response and resolution

5. Draw out and address the learning points. Thinking back to step 1, is the incident worrying enough to improve the preventive controls? Estimate how much disruption and cost this imaginary incident would have caused: minor expense and inconvenience, big trouble, expensive repairs, compliance penalties, business failure, death and destruction, cataclysm ...? Apart from workers and the organisation itself, who else would/might have been materially affected (*e.g*. other residents of the same building; customers; authorities; passers-by)? How long might these problems persist? What *else* might or should be done to prevent the incident and others affecting the same asset/s, by reducing the threats, vulnerabilities and/or impacts? Given guesstimates of the frequency (*e.g*. once a day, once a week, once a year, once a decade ...) and impacts, security improvements might be justified. Consider the possibilities, pose other questions and gather more information to firm-up the details. Do you have the basis for a business case, budget request or investment proposal?

ACT!

It is important to take action at this stage.
Don't just sit there: *do* something!

6. Pick other possible incident scenarios, assets, *etc.* on each run through the cycle. Risk management is a never-ending quest for perfection, particularly as things keep changing and risks can never be totally eliminated. Keep on knocking-out the biggest risks, time after time, getting better with practice. If it helps, time-box the process to avoid it stalling and maintain interest levels *e.g.* time-out and restart the analysis *with a different incident scenario* at the start of the next month.

Lather, rinse, repeat

This pragmatic approach was initially developed by a collaborative team from the ISO27k Forum for the Adaptive SME Security method. I have refined it a little and plan to update the adaptive method before long. Feedback welcome!

Gary Hinson January 10th 2025