A fundamental part of an information systems (IS) audit and control professional’s job is to identify and analyse risk. Furthermore, risk factors need to be stated clearly and concisely to support effective management of risk. Thus, it is critical that IS audit and control professionals know how to write a good risk statement that is impactful and aligned to better practice.

A marker of a good quality risk statement is that it can answer the following questions:

• What could happen?
• Why could it happen?
• Why do we care?

Summarising risk identification and analysis in a statement is not a science and there is no specific formula to get it right; however, there is guidance provided in the ISO 31000:2009 Risk management—Principles and guidelines that can help to better articulate risk.

The key to writing a good risk statement is having a foundational understanding of risk components and their interrelationships. Understanding key risk-related terms and their definitions, as well as the business and its objectives, will result in more impactful risk articulation.

**DEFINITIONS WITH AN EXAMPLE CASE**

To illustrate the application of these definitions in practice, one can consider a fictional bank with an objective to “keep confidential customer information secure” that is implementing a change to a highly complex customer account management system that handles customer information.

The key definitions are:

• **Risk** is the effect of uncertainty on objectives.¹
• **An effect** is a deviation from the expected.² The effect in the example is the deviation from the expected condition of customer information being kept secure. Expected conditions are those conditions that are expected by the bank’s stated objectives and policies.
• **Uncertainty** is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.³ Uncertainty in the example is from not fully understanding the consequences of the change due to the customer account management system being highly complex and inherently difficult to understand. The greater the complexity of the at-risk area, the greater the inherent uncertainty. The objective in the example is for the bank to keep confidential customer information secure.

• **An event** is an occurrence or change of a particular set of circumstances and can have several causes.⁴ In the example, the event may appear to be the system change itself, but there is no direct effect on objectives if the change goes through without a problem. An event must have an effect on objectives. Data leakage related to problems with the change would be an event, as this directly affects the objective to keep confidential customer information secure.

• **A cause** is that which gives rise to any action, phenomenon or condition.⁵ It is important not to mix up the cause and the event. In the example, defective changes, such as encryption algorithms not encrypting data as expected, cause data leakage. Defective changes do not have a direct effect on the objective of safeguarding customer information in and of themselves, and so should not be seen as an event in this case, but rather a cause. Data leakage, on the other hand, does have a direct impact on objectives so it would not be a cause in this scenario. A risk statement can contain multiple causes when applicable.

• **A consequence** is the outcome of an event affecting objectives.⁶ This element of the risk statement is important because it highlights why one should care about the risk. It is crucial that this is relevant, plausible and, ideally, quantified to give this element meaning in real terms. A vague statement of “damage to reputation” is not enough. How will this damage to the organisation’s reputation impact the organisation? If the organisation is an effective monopoly, reputational damage
may not be an issue. The consequence ideally needs to be quantified using industry research data, internal management information or known cause-and-effect relationships, such as known fixed fines levied by regulators or known customer impacts for instances of customer data leakage. A good example of this is the maximum fine of UK £500,000 that can be levied by the UK Information Commissioner's Office for confidential customer data leakage incidents or alternatively customer churn of 6.4 percent derived from industry research reports.

- **Likelihood** is the chance of something happening; risk is a combination of potential events and consequences along with the associated likelihood of occurrence. In the example, “something” refers to the combination of potential events and consequences. Likelihood can be reasonably estimated through frequency analysis of similar events in the industry, specific technology from internal organisation incident or issue databases and consultation with subject matter experts. So, considering the example, the risk analyst might look at the number of loss events in the past 12 months registered in an internal loss event database, an external database such as the Privacy Rights Clearinghouse, or a media scan, where causes related to poorly controlled changes are recorded. Looking at the frequency of these events over the total number of changes made would give a basic estimation of the likelihood of the event recurring.

Based on these definitions, a risk statement should look something like:

- **Event that has an effect on objectives** caused by [cause/s] resulting in [consequence/s].

An alternative two statement version is:

- **Event that has an effect on objectives** caused by [cause/s]. This may result in [consequence/s].

The latter version is better to use if the risk statement sentence would be too long and needs to be broken up to improve clarity. This might happen, for example, if there are a large number of key risk causes.

Taking the previous example to illustrate this, if the bank's objective is to “keep confidential customer information secure” and the event is customer data leakage, corruption or unavailability caused by defective system changes, the risk statement could be:

Customer data leakage, corruption or unavailability caused by defective system changes resulting in financial fraud losses of UK £1 million and an Information Commissioner's Office fine of UK £500,000, customer churn of 6.4 percent, and regulatory sanction by the Prudential Regulation Authority.

Data leakage, corruption and unavailability are information security failure events. That is, keeping information secure (the objective) has deviated from (the effect). The unauthorised, defective or unfit changes are the causes of this effect on objectives, while the consequences are defined in terms of what happens if the organisation fails to meet its objective.

**POINTS TO NOTE**

There are different levels of objectives. A clue to selecting the right level is to look at the objectives of the organisational unit for which you are undertaking risk assessments. For example, the IT function is required to protect information assets in its care, so protecting information is one of its objectives (this may also be reflected in policy statements). To highlight this, consider the following two risk statements:

1. Customer data leakage, corruption or unavailability caused by defective system changes resulting in financial fraud losses of UK £1 million and ICO fine of UK £500,000, customer churn of 6.4 percent, and regulatory sanction by the Prudential Regulation Authority.

2. Loss of market share caused by eroded customer confidence in the organisation’s information security resulting in net revenue reduction of UK £200 million and bank share value reduced by 12 percent.

©2014 ISACA. All rights reserved. www.isaca.org
These two risk statements are valid depending on their context. The first is valid if the context relates to keeping customer information secure. The second is valid in the context of achieving the organisation’s business strategy. The first risk statement would mean more to those responsible for managing customer information systems security in that it tells them exactly what needs to be controlled (the system change process). The second statement might mean something to higher-level executives responsible for delivery of business strategy that includes maintaining market share, but these people will not generally be responsible for implementing and monitoring system change controls. The key message is to know the audience and tailor the risk statement to that audience.

It is important to not get bogged down trying to list every conceivable cause or consequence; instead, one should highlight the key causes and consequences only.

Likelihood (or probability) is a key element of risk. For risk to be risk, there needs to be that element of uncertainty. If the risk factor is 100-percent certain to happen, this is not a risk, but an issue. If the risk factor is impossible, it is irrelevant. For example, the possibility of data leakage due to defective system changes to the customer account management system is a risk. But, if this risk is certain to materialise, it is an issue that needs to be managed as such. If the risk under consideration is of a simultaneous meteor impact on two geographically distant data centres, this is close to impossible and would not be registered as a risk.

APPLICATION TO FINDINGS REPORTING
When writing up findings to report, use only the “[Event that has an effect on objectives] caused by [cause/s]” component of the risk statement for the title. If the title still will not fit, try to make it more concise. One may need to classify the causes and edit any noninstrumental causes to help clarify the finding’s title. The full risk statement should be included in the body of the finding being reported.

CONCLUSION
Risk can be more effectively understood and managed if it is clearly articulated. This can be achieved by remembering risk definitions while writing risk statements. Having an understanding of the objectives at risk is also key. The IS audit and control professional should create concise risk statements that are information-rich and relevant to the situation and the audience to ensure that the risk statements have an impact and support effective risk management.

ENDNOTES
2 Ibid.
3 Ibid.
4 Ibid.
6 Op cit, ISO, 2009
7 Ibid.