FORTRA™

GUIDE (Titus)

# Using Data Classification To Support ISO 27001 Compliance

**Including**

- Data classification for information security
- ISO 27002 controls
- Structuring data classification
- Implementing data classification

## Introduction

Information security is not a new idea, but the ubiquity of information technology and the increasing connectedness of society, it has become an essential part of doing business. ISO/IEC 27001:2013 is the international Standard for an Information Security Management System (ISMS) and codifies a structure for promoting information security, based on best practice.

Whilst the standard has much to say on the overall structure of an ISMS, the Standard identifies the key components as performing a risk assessment and the application of controls designed to meet the risks identified. Controls are chosen based on the specific risks facing the organisation and ISO 27001 discusses a range of controls to mitigate potential risks.

Controls are processes and technologies that act to protect the organisation's information and are capable of being customised to fit with the organisation's business processes and needs. This customisation is the key to the Standard – after all, there is little point implementing an ISMS or if it fails to address risks specific to your business or the potential benefit outweighs the burden of running it.

A formally audited, certified ISO 27001 ISMS is valuable beyond the immediate realm of information security: it proves to customers, clients and partners that their information is secure with you. Implementing an ISMS is, therefore, a value-adding project and not merely a process of compliance.

### Data Classification For Information Security

In order to protect information, you should first have an appreciation of the value of that information. There is little point investing in protection for information freely available on your organisation's website but it would be foolish to forego protection for valuable intellectual property. Information security is fundamentally about identifying what you need to protect and what it needs to be protected from.

Identifying the information you hold can be a complex task, as the way 'information' is viewed is surprisingly broad. Data assets include not only raw data and files (unstructured data), but also structured data held in databases and any other form of information that has value to the organisation. For manufacturing companies, for example, this might include design drawing files for new products, which contain valuable intellectual property. In order to successfully apply an ISMS, your organisation should have a complete and comprehensive data asset register that not only records the existence of the asset, but also allows you to assess its value to your organisation at a glance.

A data classification scheme establishes a standardised set of descriptions that can be applied to all data assets. The terms your organisation uses are entirely a matter of preference and open to customisation, but may be as simple as a numbering system, or descriptive terms like 'Confidential', 'Senior Management Only' and so on. Whatever scheme you use, it should be appropriate to your needs.

### ISO 27002 Controls

Controls are used to manage the risks facing your data assets. The controls provided in Annex A of ISO 27001 describe practices that can be used to mitigate information security risks; these controls are expanded on in the companion guidance, ISO/IEC 27002:2013. There is no requirement to use these controls over any other set of controls, but they represent a range of best practices that can provide thorough coverage of a wide variety of risks.

The Annex A controls also work in a synergistic manner, by feeding into each other and thus reinforcing information security. Data classification is one of the most pervasive of the controls offered, and aside from ensuring information can be appropriately identified, it also allows the organisation to build security features around the classifications assigned. For instance, access controls can be managed by comparing the user's clearance to the classification of the data that will be accessed. Equally, your organisation could take the step of standardising access.

## Structuring Data Classification

So, how do you define a data classification scheme? The objective according to ISO 27001 is that information be "classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification", which is – again – open to interpretation by the organisation. In

any case, you should look for a standardised method, so that any given information asset can be consistently classified by any member of the organisation.Ideally, a data classification scheme should limit the number of possible classifications in order to in turn limit the number of processes you need to maintain. That is, the organisation should determine the smallest number of classification levels necessary to provide adequate, but not excessive, security. For many organisations, this need not be more than three or four.

When defining each of the classification levels, it may be useful to think in terms of how far you are willing to let the information go. Is the data suitable for release to the public in general? Is it the sort of information that could cause significant harm to the organisation? Is the organisation legally required to protect the information? With these concerns established, it should be possible to group information together under to form the classification levels.

A simple example of classification levels might look something like this:

- **Unclassified** - the information is not particularly valuable, nor is the organisation required to protect it. It can be accessed by anyone for any purpose, including release to the public or clients. This may include press releases, job vacancies, and so on.
- **Internal Only** - the information has value internally, and may have some value to competitors. It may be distributed freely to anyone within the organisation. This may include internal memos, employment data, contract information and so on.
- **Confidential** - the information has significant value and there may be legal requirements for protection, but needs to be accessible to specific roles, and in some cases is encrypted and only accessible to automated systems. Access to the information is limited to designated roles or tiers within the organisation. This may include intellectual property, customer payment details, long-term strategic planning, and so on.

Each of these classification levels can then inform other controls to ensure that the information is appropriately protected from unauthorised access, modification, distribution and destruction.

## Implementing Data Classification

There are several critical factors in implementing an effective information classification scheme: labelling, access controls and staff awareness. While each of these is separately managed through ISO 27001 and the Annex A controls, they are more or less on the same 'level' as the classification scheme.

Labels are used to identify the value of the data and to display its classification. The way labelling is handled is, once again, up to the organisation, but should be relevant to the way the information is used. For instance, hardcopies of files, removable media, and so on should have a physical label such as a sticker or printed label; digital content should include the label in the filename, document itself and metadata, which enables it to be appropriately used by other security and access control systems. A further consideration is converting digital content into hardcopies, such as when printing documents. A system should be put in place to automatically label printed or faxed information, with a default setting in case the information is not already labelled.

Access controls can draw from the labelling, metadata or file structure to permit or deny access to information based on the user's access rights. For hardcopies, this could involve filing information in specific cabinets, which can be locked or stored off-site to control access. Digital content can leverage network controls to ensure that users only have access to information they are entitled to. This can be managed on a system-by-system basis, such that information like customer payment details can be processed without providing explicit access (a payment processing system that anonymises or blocks payment card details from the user, for instance).

Finally, for any classification scheme to be effective, your personnel need to know how to classify information and the handling rules associated with it. If they use a data classification solution, this will become second nature, and handling rules can be set up to ensure that information is not sent to the wrong recipient. It is, however, sensible

to supplement this with some training and awareness, particularly when first establishing the process. Critical to ensuring that any classification scheme is effective is making sure that it is simple enough to navigate – there should not be too many classifications, the rules for handling information should be clear, and personnel should be able to reliably classify any new or unlabelled information.The final step in implementing a data classification scheme is to decide the method by which classifications are derived and applied. The choices broadly fall into the following categories, which we will consider in turn:

- **Manual** - policy guidance is circulated and training is given, but users are left to manually type classifications into their emails, documents and files. By far the cheapest method, but very risky as it's not consistent or enforceable.
- **Automated** - often provided by data governance or content-aware DLP solutions, which use software algorithms to select a classification. Although more consistent and enforceable, it can result in false positives/ false negatives and lowered trust within the user community.
- **User-Driven** - Captures the user's knowledge of the value of the data they handle, in a specialist data classification solution, so that more informed decisions can be taken about how it is managed, protected and shared. Although it presents a minor speed-bump to the user, it leads to reduced errors, increased trust and improved system performance, lowering the overall risk of sensitive data being lost.

There are many ways to implement an IT security policy, but most methods require some understanding of the content that is being processed in order to be effective. Automated classification techniques can be used to complement a user-driven classification solution. In this scenario, userdriven classification provides context for automated content detection, which in turn acts as a backstop to check that no other sensitive information has been overlooked.

The only way for data classification to meet the host of security and data management challenges that organisations face today is for it to be driven by users and informed by their knowledge of the business value of information. If organisations follow this best practice, then they stand a much better chance of protecting their data, their employees and the value of their business.

User-driven data classification solutions can bridge the gap between the more traditional perimeter IT security solutions (such as firewall protection) and information management solutions. Increasingly, data classification is becoming a best-practice feature of a layered security approach, which may include DLP, encryption and rights management.

## In Conclusion

Data Classification is an essential part of any information security system, it is clearly one of the more potent tools that organisations should consider from the outset, and build into the foundation of their layered security approach. By identifying the value of the data that organisations create and share, they can make informed decisions on how to protect more valuable or sensitive data. Unlike many other information security solutions, data classification spreads itself across people, processes and technologies, providing them with a degree of natural redundancy and reliability. Even if your organisation is not pursuing certification against ISO 27001, instituting an information classification scheme is often seen as best practice and a project that can be completed without a prohibitive investment of time or resources.

FORTRA™

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.