DELTA TECH AFRICA LIMITED

ISO/IEC 27018: 2019

IT SECURITY CONTROL

SUMMARY

ISO/IEC 27018:2019

The security of private information has never been more important. Many national and international organizations, including the International Organization for Standardization (ISO), the United States government, and the European Union, are working to solve this issue. The international standard ISO/IEC 27018 is one project they have in common.

ISO/IEC 27018 is a best practice guide for safeguarding personally identifiable information in public cloud services. It is designed as a supplement to the widely used and recognized ISO/IEC 27002 code of practice for information security measures.

So, what exactly does ISO/IEC 27018 provide cloud service consumers, and why is it important? Personal data exposure is at the top of the worldwide agenda. The overwhelming number of high-profile security breaches has focused people's attention on how their personal information must be safeguarded.

The extent of the problem can be seen by looking at the list of breaches and the number of persons impacted: the US Office of Personnel Management had data on almost 21 million federal workers stolen, while the attack on Carphone Warehouse in the UK affected more than 2 million of their customers.

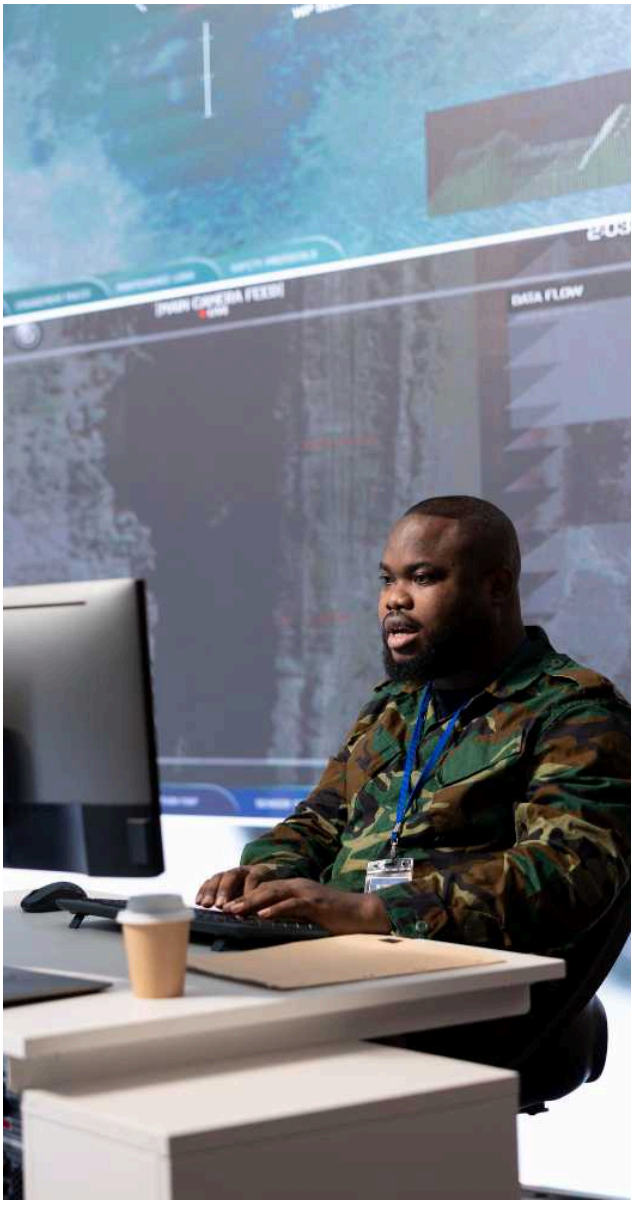
These are only the tip of the iceberg of attacks that occurred in 2015 over a three-month period. According to the Breach Level Index, $707.5 million in data records were compromised in 20151. Companies, on the other hand, are spending even more on security.

According to IDC, global IT security investment would reach $101.6 billion by 20202. While the notion of the social misfit hacker appeals to many people, most outsider assaults are carried out by sophisticated criminal gangs or state-sponsored groups, making it very difficult to prosecute them.

There is a more insidious risk: the insider who, whether knowingly or unwittingly, exposes a corporation to assault. Internal threats are frequently more deadly since they either go undetected or are covered up.

According to PricewaterhouseCoopers3 study, 75 percent of firms that suffer from employee security vulnerabilities do not contact law authorities or file any legal charges. This leaves those firms' clients exposed, and any companies who hire such individuals in the future will be uninformed of their history, leaving them vulnerable to assault.

With identity theft accounting for 64% of data breaches in the first half of 20161, it's no surprise that there's so much concern about how personal data is safeguarded, and, in particular, why there's so much concern about using cloud computing and entrusting data to Cloud Service Providers (CSPs).



For these reasons, the European Union, for example, has enacted new data protection legislation (the General Data Protection Regulation, or GDPR) in an effort to standardize the legal position throughout the continent. In Europe, there are several country-specific data privacy rules, making it particularly challenging for cloud service companies to operate. Cloud computing spans international borders, however, data security rules are mostly country-specific.

Part of the problem has also been the manner in which corporations store data - there is a legal distinction when it comes to cloud service providers. They collect data on behalf of their clients, but the consumer is legally responsible for what happens to that data.

This is where the concerns about CSPs really arise: while all CSPs are happy to talk about their security expertise, the amount they spend on data protection, and the physical barriers they put in place to prevent breaches, there are underlying concerns about whether CSPs will treat personal and confidential data in the same way their customers would. While the European Union is introducing some coherence into the data protection arena, the US has to contend with a different situation.

In the US, there’s no national law regulating how personal data is handled. The different polices of the individual states can cause a degree of confusion. This is exacerbated by various regulatory demands across different industries. All these factors combine to make formulating a coherent data policy rather difficult. In an effort to start to address this deficiency, in August 2015, the National Institute of Standards Technology advised Federal agencies to “use relevant international standards for cybersecurity, where effective and appropriate, in their mission and policy making activities.”4 As agencies for the US government implement these standards, they will demand their contractors and supply chains also conform.

ISO/IEC 27000

From an international standpoint, ISO has created a family of information security standards that serve as a foundation for enterprises to design processes and procedures to handle information security risks. The most generally recognized standard for securing sensitive information against unintended release and illegal access is ISO/IEC 27001.

ISO/IEC 27001 and the closely related ISO/IEC 27002, with its 114 controls, can decrease the risks associated with information collection, storage, and distribution by:

- Allowing organizations to develop while ensuring that all of their personal information will be kept private.
- Providing firms with the ability to comply with rising government regulation and stringent industry-specific standards.
- Defining the prerequisites for a successful information security management system.

The ISO/IEC 27018 Standard

ISO/IEC 27001 can only take you so far. In the fall of 2014, ISO issued a new standard, ISO/IEC 27018, to address the extra risks related to the processing of personal data utilizing cloud computing. This standard is being adopted by CSPs in order to reassure their clients about the security of their data. ISO/IEC 27018, an extension of ISO/IEC 27001 and ISO/IEC 27002, gives recommendations to companies concerned about how their cloud providers operate. are entrusted with personally identifiable information (PII). It's a bit of a legal labyrinth for corporations, which is why the EU GDPR took so long to agree on, but certain definitions had to be set first.

What Is Included In ISO/IEC 27018?

The standard has various objectives. These are, according to the ISO text:

- To assist the public cloud service provider in meeting applicable requirements while operating as a PII processor, whether such obligations fall directly on the PII processor or through contract.
- To enable the public cloud PII processor to be transparent in important topics, allowing cloud service consumers to choose well governed, cloud-based PII processing services.
- To help the cloud service client and the public cloud PII processor in reaching a contract.
- To provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities when individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment may be technically impractical and may increase risks to those physical and logical network security controls in place.

While these are the fundamental concepts, when we consider the implications of what they imply and how they might benefit consumers, we can see that, for the first time, there is a genuine structure for dealing with personal data in public cloud services. ISO/IEC 27018 builds on the wide set of security measures outlined in ISO/IEC 27002 and expands them in two ways. To begin, current security measures are expanded in a number of areas to address the issue of splitting duties between the cloud service client and the cloud service provider.

Second, to follow the privacy principles stated in the ISO/IEC 29100 privacy framework standard, a new set of security controls is implemented.

Extensive security precautions include the following:

- Requirements for PII encryption in motion, storage, and on any removable physical medium.
- When PII is no longer necessary, it is deleted within a specific time frame..
- That PII is solely handled for the reasons specified in the cloud service agreement.
- To collaborate in dealing with PII principals' rights to view and modify their PII, as required by various regulations.

ISO/IEC 27018 assures that a cloud service provider has adequate PII handling processes in place. It can also aid in the creation of more robust cloud service agreements. The standard specifies how CSPs can educate their employees about PII, as well as the documentation methods that must be observed and the principles that must be followed.

ISO/IEC 27018 strives to provide true transparency for cloud service customers, so that they have a clear knowledge of what the cloud service provider is doing in terms of personal data security and protection. When applying the standard, a business must pay special attention to three areas:

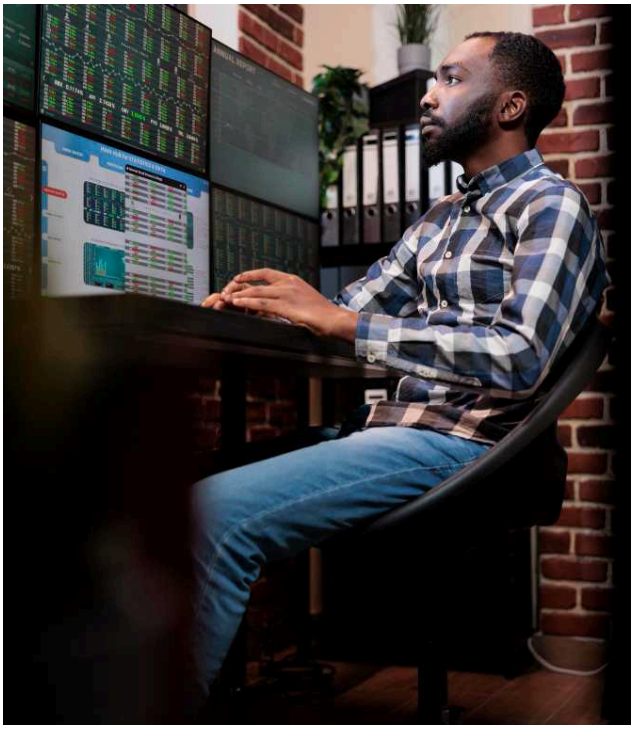
- Existing legal and legislative obligations, including any industry specific rules and regulations, that a company must obey.
- Is there any additional risk to the organization from adhering to ISO/IEC 27018? Will the standard's adoption need changes to the organization's corporate policies and business culture?

Conclusion

There is no question that the cloud sector needs standards in order to ensure acceptable and effective information security. According to a Trust poll conducted in 2015, 92 percent of British web users were concerned about their privacy. The most serious problem is that customers are unaware of how personal information obtained about them online is utilized, as well as the prospect of corporations exchanging personal information. Consumers are increasingly asking that businesses be more upfront about the acquisition, usage, and security of their internet data.

ISO/IEC 27018 assists in focusing the industry's attention on providing enhanced security to protect PII. Some major cloud providers have already certified ISO/IEC 27018, including Microsoft Azure, IBM Soft layer, Google Apps for Work, Amazon Web Services, and Dropbox. A slew of new CSPs is on the way. Organizations will progressively migrate information and processing to cloud services to benefit from the increased flexibility of technology as well as less demand on resources, but adoption will be strong only if security, notably privacy issues, are addressed. The European GDPR guarantees that a fresh attitude to privacy will be the norm.

ISO/IEC 27018 contributes to the development of a set of rules for establishing proper PII protection for both clients and cloud service providers. ISO/IEC 27018 is not a replacement for national and international rules, and widespread acceptance does not imply that providers will automatically comply with legal requirements, but it is a crucial step in the right direction.



Secure Personal Information With ISO/IEC 27018

- Globally, the yearly cost of cybercrime is estimated to be $445 billion.
- In 2013, an estimated $800 million data records were lost.
- **69%** of US CEOs are concerned about the impact of cyber risks on growth.
- **88%** of respondents say their information security does not adequately satisfy the demands of their firm.

Traditional businesses are being transformed by the use of cloud technology, using it to deliver cost savings and efficiencies. But with innovation comes concerns; transparency, control and confidentiality are key issues for many users when using cloud technology.

Used in conjunction with ISO/IEC 27001, Information Security Management Systems, ISO/IEC 27018 provides guidance for cloud service providers that process Personally Identifiable Information (PII).

The standard aims to address the risks of public cloud computing and help build confidence in public cloud computing providers. It offers a set of controls which Cloud Service Providers (CSP) need to implement in order to address the specific risks and gives guidance on what CSPs need to achieve in terms of contractual and regulatory obligations.

Benefits

- **Builds trust in your company** - by assuring consumers and stakeholders that their data and information is secure.
- **Competitive edge** - proves that strong data protection policies are in place.
- **Protects your brand** - minimizes the danger of negative publicity as a result of data breaches.
- **Reduces risks** - ensuring that hazards are identified and that mechanisms to manage or mitigate them are in place.
- **Prevents sanctions** - guarantees that local requirements are followed, lowering the possibility of fines for data breaches.
- **Assists in company growth** - by providing standard guidelines across countries, making it easier to do business abroad and acquire access as a favored supplier.

Our Products And Services

We provide a one-of-a-kind combination of complementary goods and services, which are controlled by our three business streams: Compliance, Assurance, and Knowledge.

Compliance

To reap meaningful, long-term advantages, our customers must maintain continuous compliance with legislation, market requirement, or standard so that it becomes ingrained as a habit. We provide a variety of services and specialized management solutions to aid in this process.

Assurance

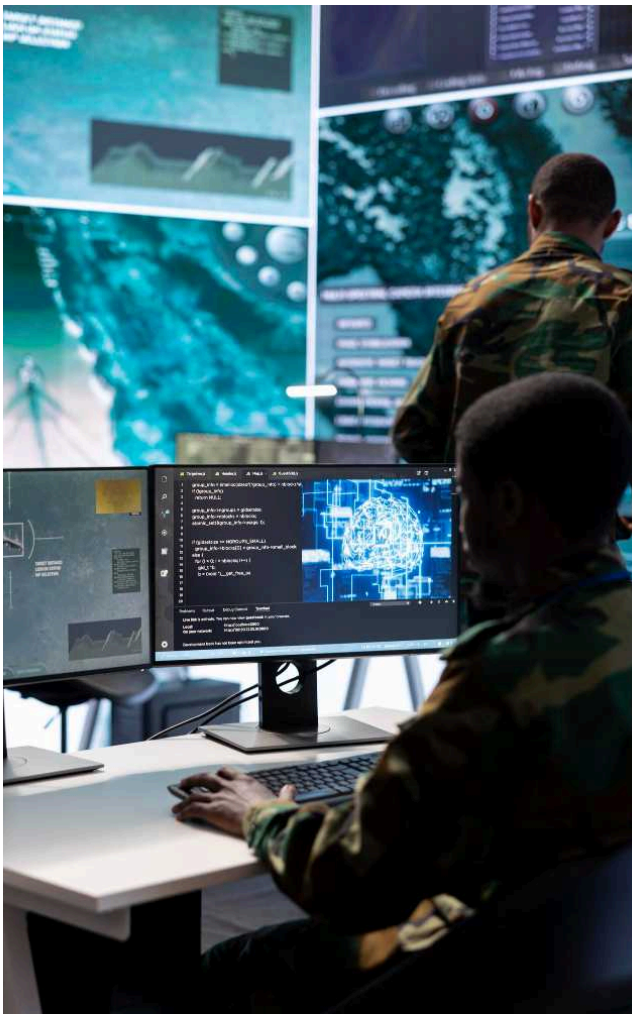
Independent evaluation of a process or product's conformance to a certain standard guarantees that our clients execute to a high degree of excellence. To guarantee that our clients get the most out of our standards, we train them in world-class implementation and auditing methodologies.

Knowledge

The information that we develop and share with our clients is at the heart of our company. We continue to expand our image as an expert body in the standards arena, bringing together industry leaders to establish standards at the local, regional, and worldwide levels.

About DTA

Delta Tech Africa Limited Is An ICT And Quality Consulting Organization Focused On Performance Management Across Business Verticals. Delta Means“ A Finite Increment”. We Help Organizations To Achieve This Increment Across Departments And Functions And To Improve The Overall Organizational Performance While Adding Value To The Stakeholders. Evolution Is A Constant Change. When The Pace Of Evolution Renders Societies Impatient, It Is A Technology That Accelerates Evolution Leading To The Transformation Of Societies. When That Evolution Happens, It Doesn’t Limit The Human Endeavors, To Get The Technology Evolution, It Has To Be Supported By Processes And Management Of The Best Quality. Hence, We At Delta Tech Africa Thought Of Bringing Both Technology And Quality Management Processes Together To Get The Best Organizational Performance And Value Across The Fast Growing Continent Of Africa.



Our Offices

Nigeria | PLOT 55B, Baderinwa Alabi Street, Central Lekki Residents' Association , Rahman Adeboyejo Street Lekki Phase 1, Lagos, Nigeria
Kenya | P.O.Box 39562-00623, Parklands, Nairobi, Kenya.
Ghana | Plot 3, Dade Link, Off Dade Street, Labone, Accra, Ghana.
South Africa | 1 Waterhouse Place Century City Cape Town 7441

Our Phone Numbers

+27 63 933 1982, +27 10 594 5356

Our Email

info@dtafrica.com

Our Website

https://www.dtafrica.com

DELTA TECH AFRICA LIMITED

info@dtafrica.com | www.dtafrica.com