ISO 27001 certification

An imperative for industries dealing with IoT

White paper

Executive Summary

Security breaches are common in today's world, especially in industries that services critical infrastructure and machines such as public utilities, emergency systems, building environmental controls and industrial equipment. Data or information assets are prone to constant outside attacks as well as theft and internal breaches at the supplier's end, which is a reality of today's world.

Choosing the right supplier for providing cloud services and devices in public utilities and critical equipment segment is important and one of the primary parameters are its security controls and practices. Any laxity can lead to financial loss, loss of sensitive and critical information, loss of reputation and even possible threat to lives, when emergency systems and public utilities are involved. ISO/IEC 27001 is an information security standard that ensures the business has undertaken key steps to secure its assets, which can include customer data, employee details, financial information or intellectual property.

ISO27001: Quality Standard for Security of Data

VPN (virtual private network) and tunneling are techniques that allow, among other benefits, to encrypt data links between yourself and another computer. This computer might belong to your organization, a trusted person or organization, or a commercial VPN service. Tunneling encapsulates a specific stream of data within an encrypted protocol, making everything that travels through the tunnel unreadable to anyone along the transmission path. Using a VPN or other form of tunneling to encrypt data is one of the best way to ensure that it will not be seen by anyone other than you and people you trust. Another major benefit of this technique is the authentication of remote parties.

ISO 27001
CERTIFIED
VINÇOTTE

Problem Definition

Security breaches range from stolen password to complicated targeted attack for which preparedness would have been impossible. No organization is safe from data and security breaches is a bold statement, because even government departments like the Internal Revenue System in US have been victims of such attacks exposing information of more than 700,000 individuals in 2016. Government or organizations in foreign countries with malicious intent can benefit from such information, which can used for criminal fraud. From social media sites like LinkedIn and Facebook to retailers like Whole Foods, have been victims of data breaches and attacks.

What happens to the data, once it is breached? It can be misused for various illegal purposes. It can reach underground cyber forums, where individuals and groups aim to make huge profits from reselling contact information such as names, addresses, titles, email addresses, dates of birth and credit card information. One of the biggest cyber-attacks in 2014 was a data breach at JP Morgan Chase with information of 76 million households was compromised. Verizon Enterprise Solutions, one of the leading providers of cloud security solutions in the world, has been a victim of a data breach that have affected more than a million of its enterprise customers. This could have had wide-ranging implications on telecom and cloud security solutions.

Safety is primary – who would you rely on for the safety of you and your customer's data? Today, hacking and outright attacks are common.

HMS Connecting Devices
ISO 27001 CERTIFIED
Talk2M
STAR CERTIFIED OSSTMM 3.0 SECURITY TEST AUDIT REPORT

High-Level Solution

The solution is that businesses need to be more proactive at protecting their infrastructure and data. They can only do that with measures like deploying security tools and practices to protect data and make continuous efforts to manage risks.
An international certification like ISO27001 ensures commitment to quality & security. Minimizing and managing security risk is the responsibility of the service provider. A security certification gives a stamp of reliability on the required security measures undertaken by an organization.

What the organizations stand to gain?

- Customer-friendly security standards are adhered to
- When companies evaluate their own information security risks within their own environment, besides those
- providing cloud services and infrastructure, they invest more in the growth of their business and that of their customers in a way.
- Certification ensures full assessment and validation of end-to-end security systems
- Responsiveness to security incidents increases with heightened awareness and robust security measures
- Following recognised information security best practice gives peace of mind for customers and the business too.
- Adhering to standards also allows interoperation between systems
- It guarantees efficient management and protection from potential threats
- Helps achieve business continuity and operational excellence goals

What the customers stand to gain?

- It ensures accountability on part of the service provider
- Helps customers to make an informed decision when choosing a supplier that follows highest possible industry standards around security
- Guarantees the organization's standard and quality of its products, as security and quality aspects are taken care of
- Builds credibility in the minds of the customer, as expectations of service and specific requirements are met

What is ISO 27001 certification?

Developed by the International Organization for Standardization (ISO), ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards, but specific to information security management system (ISMS). ISMS is a systematic approach to managing sensitive company information. It includes people, processes and IT systems by applying a risk management process.

The security standard relates to the storage, monitoring and maintenance of data. Businesses are not obliged to obtain the certification as it would be sufficient for them to just follow the recommended security best practices. However, the organization achieves assuredness when it gets the certificate and continuously adheres to the standards following a systematic approach. The certification can be obtained from an accredited certification body, which gives credibility and confidence.

How is the certification obtained?

After an initial meeting with the accredited body, the ISMS scope is defined. Then a series of other steps must be taken that includes awareness training, GAP assessment, identifying and determining assets within scope, performing the risk assessment, creating the statement of applicability, developing the risk treatment plan, implementing the chosen controls, determining improvement plan in areas which lack adequate control, delivering the operational ISMS training, performing the internal assessment, followed by an assessment visit and formal certification audit itself. Reassessment under ISMS happens every 12 months.

What the assessment covers?

The internal checklist includes everything from information security policies, organisation of information security with defined roles and responsibilities, HR (prior, during employment and termination of employment), mobile device and teleworking policy, asset management and control, information classification, removable media handling, disposal and transfer, cryptography, physical and environmental security, operations, communications (network security management and information transfer), system acquisition, development and maintenance, information security in supplier relationships, information security incident management, and compliance with legal and contractual requirements.
An important aspect of information security is business continuity management. This determines whether the business has planned, documented, implemented and maintained processes that ensure the continuity of service if an adverse situation comes about. This also needs to be validated and verified at regular intervals.

Solution Details

What measures are undertaken to ensure adherence to security standards, specific to this industry? How do you select the right product provider?

When working with remote connections to industrial control systems, network security, integrity and reliability of the cloud infrastructure and its customers' networks are paramount. Creating the best-in-class remote access solution also means developing a managed, hybrid, layered cyber security approach to protect the devices, network and most importantly, customer's industrial systems.

With strong security processes and security controls laid out, the business can identify the areas which have strong security controls and areas which require improvements.

All these measures ensure that system is adept to keep pace with changes, identify vulnerabilities, predict security threats and is able to limit business impact in case of a security breach.

Business benefits

Business and market growth are dependent on whether or not organizations meet regulatory and compliance standards. In-built in the ISO27001 management system are security practices to continuously improve, so it ensures security all throughout. The certification also includes internal education efforts, so employees of the business and suppliers are educated and empowered to protect the information.

With high risks of data vulnerability, protecting, storing and managing data needs to be based on proven practices and systematic approaches. With enhanced internal control over business assets, customers can be assured that there is a rigorously managed and documented approach to daily operations. Sometimes, ISO is the minimum requirement to garner business in the first place, so it gives a great competitive advantage because protecting reputation of your own business and that of the client, gives one a head start.

How do you choose?

Which supplier would you rely on for the products that are on the cloud, remotely accessed and monitored and has a direct bearing on your organization's brand and reputation? The one which has an internationally accepted certification.

The certification itself is not easy to come by. Scrutinized and assessed by an accredited leading international certification body, long reviews and in-depth compliance audits and follow up audits makes it not only reliable but instils confidence in customers as they see that their provider has invested in information security efforts.

Summary

HMS Industrial Networks has obtained ISO 27001 Certification for eWON Talk2M, its award-winning cloud connectivity platform, ensuring that security measures were taken across infrastructure, data centers and services. With the certification, HMS joins the ranks of organizations that follow highest international standards and operate in accordance with industry leading best practices such as Cisco services organization (for its networking, data centers, communications and collaboration products and solutions) or Amazon web services (AWS).

The certification offers convenience to customers who know that their data is secure in the most secure environment of such businesses, owing to the processes followed. Data security is essential when dealing with Internet of Things (IoT). Not only the staff needs to dedicatedly work towards continuous prevention and monitor security threats through systems, tools and processes, but ensure third-party suppliers also comply to the practices.

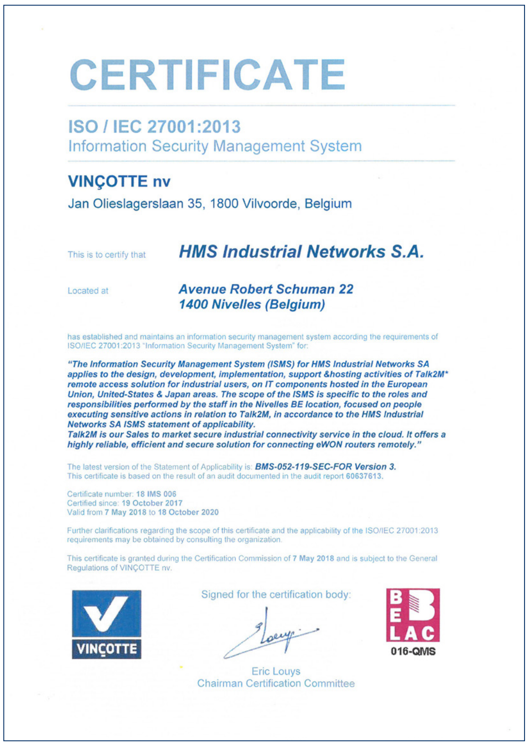
Security - Part of the decision process

Choosing an organization that follows a global standard for information security management is the first set of criteria that a company or firm needs to consider before awarding business. Confidentiality and constant availability of data are the hallmarks of good security practices and controls. How the information security risks are managed can affect the integrity and reputation of the company and its customers' information. This white paper shows why ISO 27001 certification is an essential step in this direction.

HMS is a provider of quality gateways/routers that takes away the burden of on-premise monitoring and control when it can be done remotely, saving cost and time. The success of this solution depends on whether the data flow is well monitored and kept completely secure, something which HMS is able to do, owing to its compliance to ISO 27001 standards.

Visit eWON website (www.ewon.biz/security) to learn more about our services and how we follow and maintain global security standards.

https://www.crn.com/news/security/300080151/telecom-partners-say-cloud-security-is-top-of-mind-in-wake-of-verizon-breach.htm?itc=refresh
https://www.iso.org/isoiec-27001-information-security.html



CERTIFICATE

ISO / IEC 27001:2013
Information Security Management System

VINÇOTTE nv
Jan Olieslagerslaan 35, 1800 Vilvoorde, Belgium

This is to certify that **HMS Industrial Networks S.A.**

Located at **Avenue Robert Schuman 22**
1400 Nivelles (Belgium)

has established and maintains an information security management system according the requirements of ISO/IEC 27001:2013 "Information Security Management System" for:

"The Information Security Management System (ISMS) for HMS Industrial Networks SA applies to the design, development, implementation, support &hosting activities of Talk2M* remote access solution for industrial users, on IT components hosted in the European Union, United-States & Japan areas. The scope of the ISMS is specific to the roles and responsibilities performed by the staff in the Nivelles BE location, focused on people executing sensitive actions in relation to Talk2M, in accordance to the HMS Industrial Networks SA ISMS statement of applicability.
Talk2M is our Sales to market secure industrial connectivity service in the cloud. It offers a highly reliable, efficient and secure solution for connecting eWON routers remotely."

The latest version of the Statement of Applicability is: ***BMS-052-119-SEC-FOR Version 3.***
This certificate is based on the result of an audit documented in the audit report **60637613.**

Certificate number: **18 IMS 006**
Certified since: **19 October 2017**
Valid from **7 May 2018** to **18 October 2020**

Further clarifications regarding the scope of this certificate and the applicability of the ISO/IEC 27001:2013 requirements may be obtained by consulting the organization.

This certificate is granted during the Certification Commission of **7 May 2018** and is subject to the General Regulations of VINÇOTTE nv.

VINÇOTTE

Signed for the certification body:

Eric Louys
Chairman Certification Committee

BELAC
016-QMS