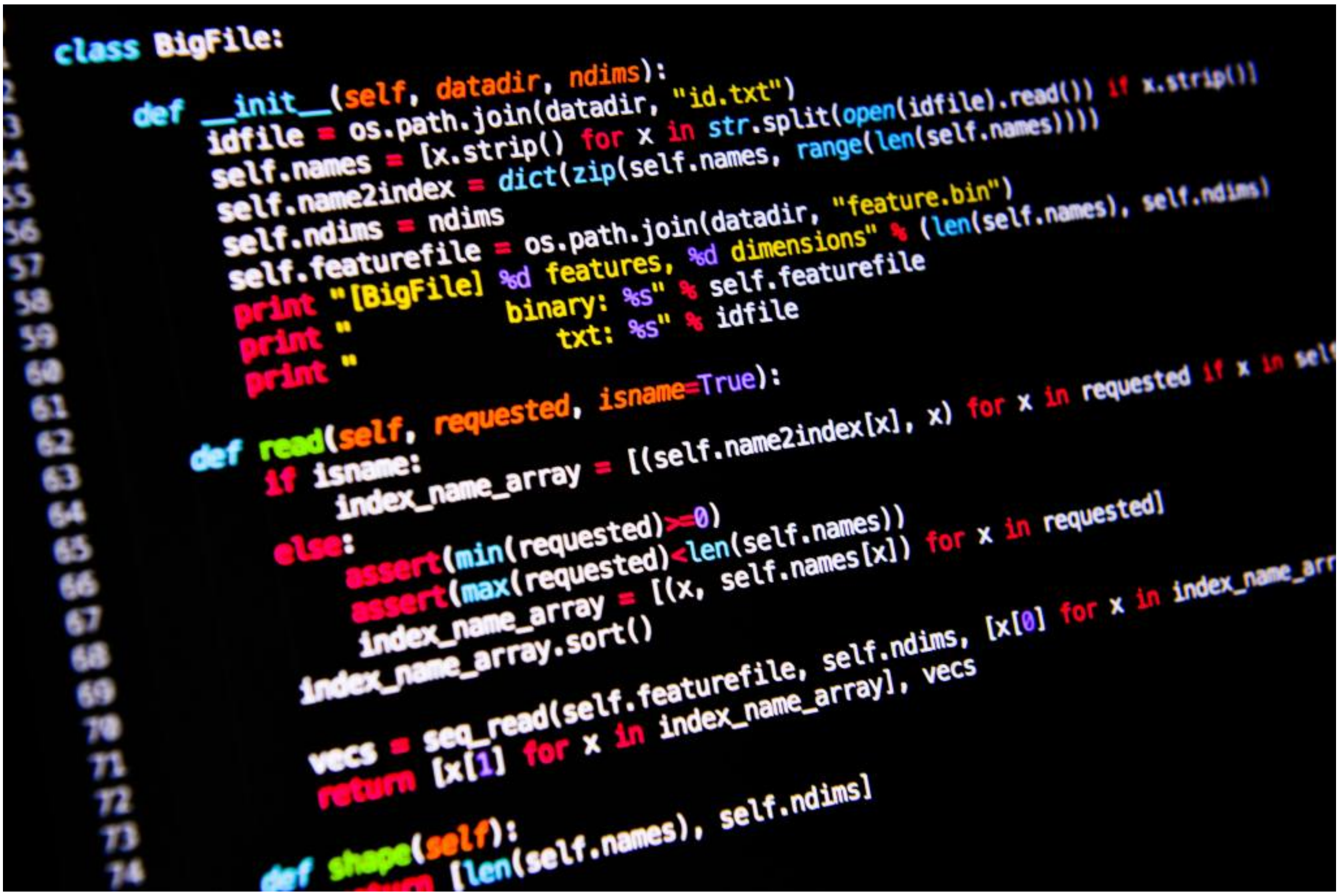


```
class BigFile:
    def __init__(self, datadir, ndims):
        idfile = os.path.join(datadir, "id.txt")
        self.names = [x.strip() for x in str.split(open(idfile).read()) if x.strip()]
        self.name2index = dict(zip(self.names, range(len(self.names))))
        self.ndims = ndims
        self.featurefile = os.path.join(datadir, "feature.bin")
        print "[BigFile] %d features, %d dimensions" % (len(self.names), self.ndims)
        print "          binary: %s" % self.featurefile
        print "          txt: %s" % idfile

    def read(self, requested, isname=True):
        if isname:
            index_name_array = [(self.name2index[x], x) for x in requested if x in sel
        else:
            assert(min(requested)>=0)
            assert(max(requested)<len(self.names))
            index_name_array = [(x, self.names[x]) for x in requested]
            index_name_array.sort()
        index_name_array.sort()

        vecs = seq_read(self.featurefile, self.ndims, [x[0] for x in index_name_arr
        return [x[1] for x in index_name_array], vecs

    def shape(self):
        return [len(self.names), self.ndims]
```

What is ISO 27000?

May 8, 2019 / Jason Miller / No Comments

Whether a business is relatively small or a huge global corporation, it's vital to follow standards to help ensure that the business runs smoothly and is free of any potential pitfalls that could bring the organization down. One of the most common issues that a business can face is when it suffers from a lack of information security. Whether it's stolen credit card details, mishandled personal information or even intellectual property that is entrusted to you by third parties, your business has an obligation to look after its data and prevent external and internal threats from accessing it.

To help companies keep their data and information assets secure from threats, it's important to understand security standards such as the ISO 27000 series. This will be important to protect financial information, customer data, employee details and also intellectual properties. In this article, we're going to explain what

ISO/IEC 27000 is, why you should use it as a standard and also discuss some of the advantages of achieving certification to those standards.

What Is ISO/IEC 27000?

Also known as the ISO 27000 Family of Standards, it's a series of information security standards that provide a global framework for information security management practices. They're published and developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 27000:2018 focuses on information technology, security techniques and information security management systems. This particular standard involves an overview and vocabulary used by the ISO 27000 series standards and serves as a general introduction to the more common ISO/IEC 27001:2013, also known as ISO 27001.

What Is ISO/IEC 27001?

The ISO 27001 standard explains the requirements for an organization's information security management system (ISMS). It enables organizations to prove that they meet regulatory requirements that are related to information security and it demonstrates that the company is committed to protecting sensitive and confidential data.

The ISO 27001 standard provides a framework for organizations to use when protecting information. This is often done through the use of different technologies, auditing practices and tests. It also helps to improve staff awareness on ISO 27001 so that internal incidents have a low risk of breaking ISO 27001 standards due to uninformed or untrained staff.

In most cases, an organization will have a number of different security controls that it uses to regulate the flow of information in and out of the business. However, these controls are often disjointed without an ISMS governing them. This is because security controls are often implemented as point solutions to specific areas of the business for convenience but cannot be monitored or controlled from a central area. An ISMS seeks to simplify these security controls in order to make data security easier to manage. It's a systematic approach that helps to manage sensitive company data in order to secure it and it can be applied to virtually any business that uses technology regardless of its size.

The ISO 27001 standard requires that your data management staff are capable of systematically examining the organization's information security risks. This means taking into consideration all vulnerable points in your system, the threats that could be posed to these weaknesses and also the impact it could have on your overall data management solution. It also requires that you design and implement a comprehensive suite of information security controls that can address risks that would be deemed as dangerous or risky. Lastly, it also requires that your management staff adopt a management process that ensures that all of your information security controls meet the information security needs of the organization.

Why Use the ISO 27000-Series Standards?

The ISO 27000-series standards are designed to assist companies in managing cyber attack risks and internal data security threats. As an organization grows, it becomes more complex and the technological solutions are open to more vulnerabilities that aren't immediately obvious. Cyber criminals pose a constant threat to all industries that make use of networked technologies and it can become incredibly difficult to protect your data.

In addition, the ISO 27000-series standards focus on helping companies implement effective and affordable solutions that can assist in protecting personal data, corporate data and intellectual properties. Among the standards, ISO-27001 is arguably the most popular because it's currently the only standard that can provide a company with an audited certification. However, ISO-27001 isn't the only standard that can provide an organization with assistance in how they protect their business. For instance, ISO-27005 provides guidance on conducting risk assessments for your information security and ISO 27032 provides general guidance on the best practices to enforce cyber security measures.

What Are the Advantages of Following ISO-27000 Series Standards?

There are a number of useful advantages to following the ISO-27000 series standards. For starters, it allows an organization to protect business-critical data and also helps to safeguard employee and customer details. This can help give your customers and employees more faith in your processes, drastically improving your reputation and potentially avoiding any hits to how trustworthy you are in the eyes of your audience.

Data breaches can also come with expensive fines especially if you breach standards such as the General Data Protection Regulation. These expensive fines can be incredibly damaging to not just your financial situation but also your reputation. Penalties may also halt your business which can be devastating, often enough to completely ruin your business. Lastly, following the ISO-27001 series standards and receiving certification for ISO-27001 mean that you'll improve customer confidence and show that your company is capable of abiding by the strongest and most trusted security practices.

It's important to remember that while the ISO-27000 series of standards is already well-defined, it's a constantly evolving standard that will continue to be updated as new technologies and threats appear. By adopting these new standards and always ensuring that you're up-to-date with ISO-27000 regardless of your chosen industry, you'll always be able to protect your organization's most sensitive data and build trust with both employees and customers.

Search …

Recent Posts

Trends in Cybercrime Today: Protect Your Business

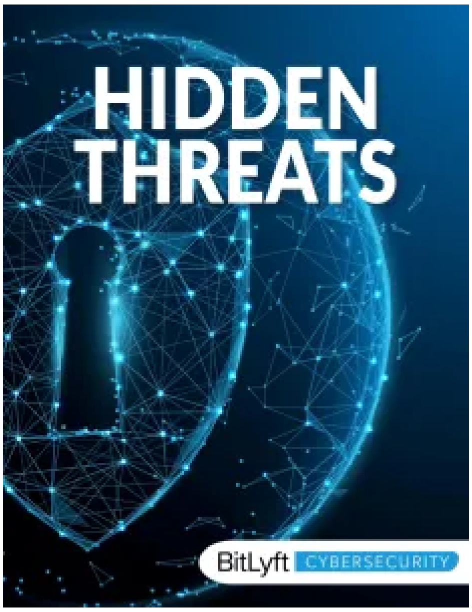
What is Threat Remediation in Cyber Security?

Popular Types of Cyber Attacks In Manufacturing

What is the Difference Between IDS and IPS?

What is Computer Network Defense (CND)?

Stop The Hidden Threats Before They Start



About the Author

Jason Miller

Jason is a Chief Executive Officer of BitLyft Cyber Security. He has spent the last 19 years of his career focusing on network, system administration, and cloud technologies. He is passionate about helping businesses embrace the next generation of technology including cloud adoption and high performance scaling software.

Start a Conversation

We are ready to help assess your cybersecurity concerns and partner with you in your cybersecurity needs.

START A CONVERSATION

Leave a Comment

Your email address will not be published. Required fields are marked *

Type here..

Name*

Email*

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment »