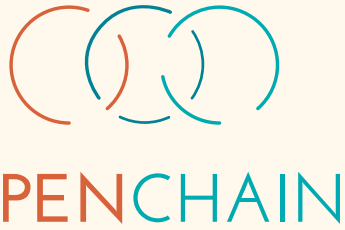

Three-Way Case Study:

The use of ISO/IEC 5230:2020 by a company providing mission-critical services to enterprise clients around the world

BlackBerry, OSS Consultants and OpenChain

Table of Contents

Introduction

The OpenChain Project maintains two ISO/IEC standards designed to help optimize business process management around open-source software. One of the standards, ISO/IEC 5230:2020, focuses on how to establish and run a quality open-source license compliance program. Another of the standards, ISO/IEC 18974:2023, focuses on how to establish and run a quality open-source security assurance program. Taken together, these standards provide a reliable, efficient and effective way to manage the open-source supply chain.

This case study will highlight the use of ISO/IEC 5230:2020 by a company providing mission-critical services to enterprise clients around the world.

Company Overview - BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company's software powers over 235M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.

Open-Source Management Overview

Although BlackBerry had made a significant investment in its open-source program, after acquiring several subsidiary companies it found itself with an assortment of tools, processes, technology, and subject matter expertise distributed throughout the company. BlackBerry identified a need to focus on standardization and wished to centralize a single source of truth and expertise by developing an Open-Source Programs Office (OSPO).

In partnership with OSS Consultants, an official OpenChain Partner, BlackBerry performed a full review of its catalog of software, tooling, build systems, processes, and capabilities within the open-source space. During this review, we found that we had effective processes, expertise, and scanning tools, but had an opportunity to improve coverage and reduce the cost of operating.

Company Overview - OSS Consultants

OSS Consultants is a full-service open-source consultancy, dedicated to helping organizations of all sizes, design, implement, and manage the most efficient, comprehensive and robust open-source program offices and policies.

With a rich history spanning decades in the software industry, OSS Consultants has a reputation for deep expertise and an unwavering commitment to simplifying management of open-source. We've partnered with a diverse range of clients, from nimble startups to global giants, crafting bespoke solutions for each. OSS Consultants is more than just a consultancy; we work as a strategic ally to help organizations realize their open-source goals with precision and foresight.

OSS Consultants – Your Trusted Partner in Open Source Management

For more information, visit ossconsultants.com and follow @OSSConsultants

Solution Overview

For BlackBerry's particular use-case, OSS Consultants recommended a centralized solution that enabled a single process to serve the business. This allowed BlackBerry to utilize our expertise to further develop in-house OSPO capabilities, reduce their tooling spend, and provide better holistic coverage based on a single strategy that included a single set of standards and principles.

Organization Overview - OpenChain

The OpenChain Project has an extensive global community of over 1,000 companies collaborating to make the supply chain quicker, more effective and more efficient. Our vision is a supply chain where open source is delivered with trusted and consistent process management information. Our mission is to make that happen. OpenChain is part of The Linux Foundation, a neutral, trusted hub for developers and organizations to code, manage, and scale open technology projects and ecosystems.

ISO 5230 - Overview

OpenChain ISO/IEC 5230:2020 defines the key requirements of a quality open source license compliance program. It helps organizations manage open-source licensing requirements for past, current and future products or services.

It identifies:

1. The key places to have license compliance processes
2. How to assign roles and responsibilities
3. And how to ensure sustainability of the processes

The OpenChain ISO/IEC 5230:2020 is lightweight, easy to read and is supported by a global community with free reference material and conformance resources.

OSPO Design

OSS Consultants started by understanding BlackBerry's needs in managing the use of open-source software. This helped inform not just the beginnings of what the future corporate open-source strategy would become, but also how OSS Consultants would conduct the assessment of the current state of open source management at BlackBerry.

Among the business units assessed, OSS Consultants identified parts of the business that had great open-source practices, and other parts that needed additional support in executing a holistic strategy. We worked with BlackBerry to come up with a new strategy for managing open-source software to achieve their operational goals.

Choice of Standard Rationale

- An Open Source Program Office (OSPO) was designed around OpenChain ISO/IEC 5230:2020, the industry standard for open source license compliance, to ensure a foundation following industry best practices.
- The implementation and execution of the OSPO was focused on having a clear vision, processes aligned with market norms, and consolidated tooling to ensure cost-effective and efficient operation.

Recertification as part of quality management and continuous improvement

- The concept of "kaizen" or continual improvement was applied to use milestones such as ISO/IEC 5230 recertification as an opportunity for refinement and quality management.
- In practice, this focused on identifying what aspects of operational processes were working at high efficiency and what areas could be improved on without disrupting workflows.
- The recertification process was also a signifier for customers to underline a commitment to a secure supply chain led by an entity responsive to market evolution.

Key Lesson Learned

The ISO/IEC 5230 recertification process provided an excellent opportunity to assess lessons learned and consider these not only from the company perspective, but also with respect to larger supply chain optimization.

Working across a broad and diverse set of development teams

It isn't easy to find a one-size-fits-all approach to scanning, inventorying, and analyzing products made up of such a diverse set of technologies and by an even more diverse group of developers. Make sure your approach is flexible and agile to meet the needs of your stakeholders.

Software Bill of Materials (SBOM)

Having a properly inventoried open-source footprint has never been more important. To effectively fulfill requirements around SBOM, it's critical to understand your open-source footprint, your patching and vulnerability risk posture, and your compliance with the licenses of those libraries.

Staffing a dedicated team

Open Source is a field with growing demand, especially due to Software Bill of Materials requirements. Talent in this space has never been more sought after, and we need to drastically increase the talent pool in the industry to meet current and future demand. It is important to look not only internally for talent with an interest in open source but also to survey the pool of development talent out there who might be interested in focusing on an open-source role.

Implementing Recognized Standards

"It was important to BlackBerry to implement a process that would be recognized as an industry standard. This makes it easier to communicate with our customers regarding how we work to protect them and maintain a high-quality, industry-recognized process. OpenChain provides us with the blueprint that helps us do that" – Christine Gadsby, Vice President of Product Security at BlackBerry.

"OSS Consultants prides itself as the first OpenChain Partner to lead an organization through the process of attaining whole-entity conformance with OpenChain ISO 5230:2020 from beginning to end. We are grateful for the longstanding partnership between OSS Consultants and BlackBerry. This partnership is not just a collaboration; it's a strategic alliance that exemplifies our joint commitment to delivering unparalleled value to clients and staying at the forefront of technological advancements, ensuring that our combined efforts continue to set new a new bar for quality in the industry." - Russ Eling, CEO at OSS Consultants

"BlackBerry has one of the deepest industry pedigrees in bringing increased peace of mind to enterprise and governmental organizations. Certifying their open source software management underlines their commitment to excellence and serves as a beacon for other companies to follow. Their contribution to securing the open source supply chain is significant, as is their thought-leadership in inspiring others to follow." – Shane Coughlan, General Manager at the OpenChain Project

Conclusion

Businesses face an ongoing tension between seeking excellence and the pressures of bringing products to market. Mechanisms such as a solid policy, clear processes, and good training help to ensure this tension is addressed as effectively as possible.

The use of standards is a simple way to package all of the key requirements for excellence in a manner that is known to work and which aligns with other industry stakeholders. It also provides a clear signal to the supply chain and to customers of company intent and execution.

OpenChain ISO/IEC 5230 and OpenChain ISO/IEC 18974 represent landmark standards that define solutions to open-source license compliance and security assurance. Aligning with the processes they identify ensures an unequivocal level of quality in the respective open-source programs.

As this three-way case study between BlackBerry, OSS Consultants, and OpenChain has shown, adoption of these standards in a running business with deployed products is a beneficial choice for companies, including those in critical industries. Further, collaborating with an official OpenChain Partner often allows internal teams to minimize some of the pressures of implementing a conformant open-source program by minimizing disruptions, while enabling the organization to continue focusing on its core objectives. Companies of all sizes in all industries are invited to obtain similar benefits, and to engage with the OpenChain community at www.openchainproject.org to get started.

About OpenChain Project

The OpenChain Project is building a supply chain where open source is delivered with trusted and consistent process management information. It maintains OpenChain ISO/IEC 5230:2020, the international standard for open source license compliance, and ISO/IEC 18974:2023, the international standard for open source security assurance.

There is an extensive global community of over 1,000 companies collaborating around the OpenChain Project to make the supply chain quicker, more effective and more efficient.

https://www.openchainproject.org/

About The Linux Foundation

The Linux Foundation is dedicated to building sustainable ecosystems around open source projects to accelerate technology development and industry adoption.

Founded in 2000, The Linux Foundation provides unparalleled support for open source communities through financial and intellectual resources, infrastructure, services, events, and training. Working together, The Linux Foundation and its projects form the most ambitious and successful investment in the creation of shared technology.

https://www.linuxfoundation.org/