

SUCCESS STORY:



JFE Shoji Power Canada Inc.

# Strategic IT Assessment and Recommendations for JFE Shoji Power Canada

A Case Study By Synchronworks Consulting

[synchronworks.net](http://synchronworks.net)  
[info@synchronworks.net](mailto:info@synchronworks.net)  
1.866.960.9409



 **SYNCHROWORKS**  
CONSULTING



## CONTENTS

<b>1</b>	Project Details	3
<b>2</b>	The Challenge	4
<b>3</b>	Opportunities & Solutions	5

# Project Details

## Location

Ontario, Canada

## Year

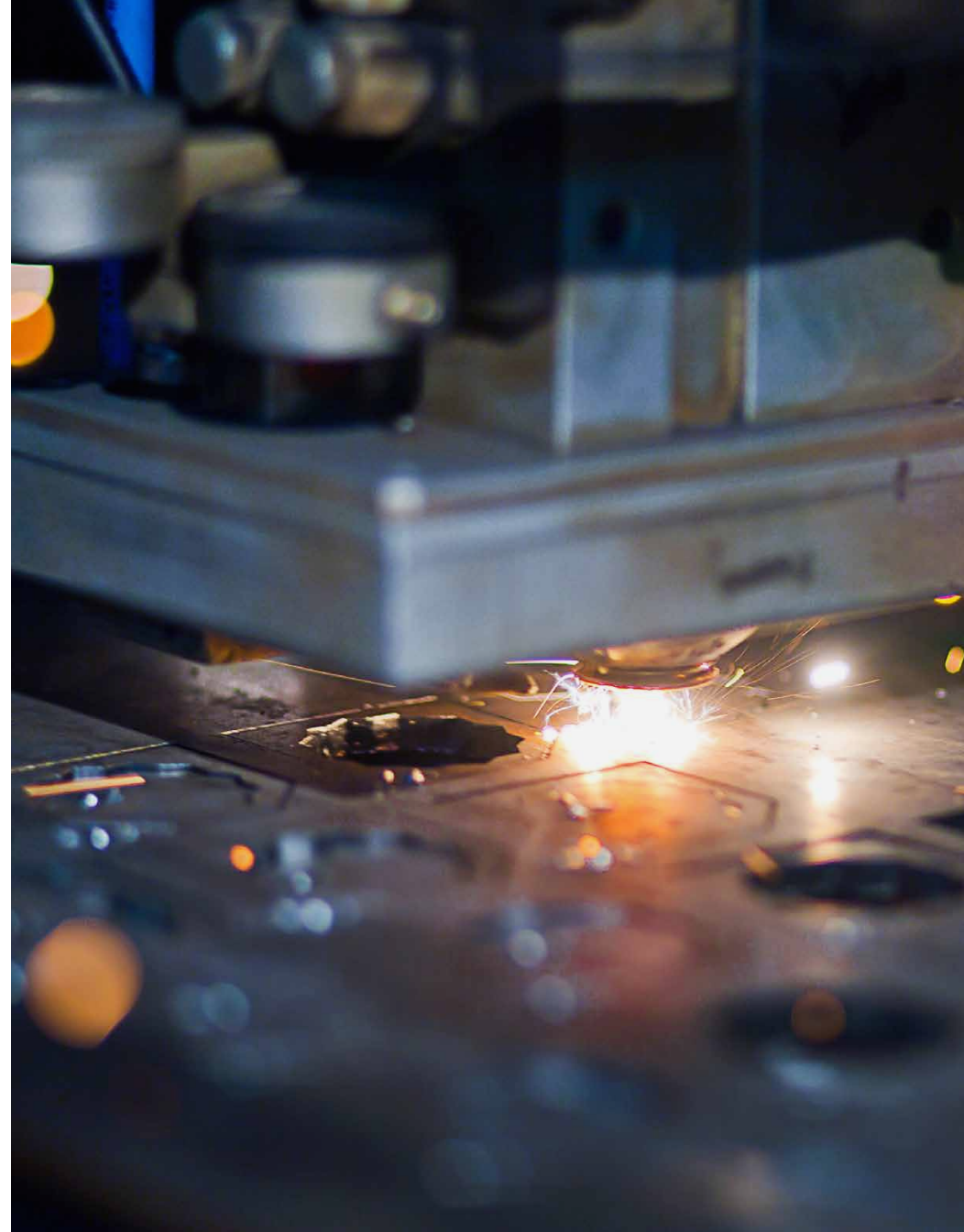
2024

## Industry

Manufacturing



JFE Shoji Power Canada Inc.





JFE Shoji Power Canada (JFE) gained a clear roadmap to address critical vulnerabilities, enhance operational efficiency, and align their IT infrastructure and cybersecurity practices with industry standards.

# The Challenge

JFE faced significant challenges in its IT operations, creating vulnerabilities that impeded its ability to meet business objectives securely and efficiently. Key issues included:

- **IT Team Structure:** A misaligned IT team lacked specialized roles, formalized responsibilities, and adequate training, leading to operational inefficiencies and gaps in governance.
- **Network Infrastructure:** An outdated, flat network structure lacked segmentation and enterprise-grade hardware, increasing security risks.
- **Cybersecurity Operations:** The absence of multi-factor authentication (MFA), mobile device management (MDM), and proactive threat monitoring left the organization exposed to potential breaches.
- **Backup and Disaster Recovery:** No formal disaster recovery plans or tested backup procedures existed, putting critical data and operations at risk.
- **Vendor Management and Governance:** Insufficient vendor oversight and an absence of formal IT governance policies limited the organization's ability to mitigate third-party risks and align IT with strategic goals.

These gaps heightened the risk of security breaches, data loss, and compliance failures, necessitating immediate and strategic interventions.

Our task was to conduct a comprehensive IT assessment to identify these weaknesses and provide actionable recommendations for improvement, with a focus on aligning their IT operations with industry best practices, improving security, and optimizing overall performance.

# Opportunities & Solutions

To address JFE's IT challenges, our team conducted a detailed assessment guided by industry standards, including CIS, SOC 2 Type 2, and ISO 27001.

Through a detailed evaluation of JFE's IT systems, infrastructure, cybersecurity measures, and organizational structure, we identified several key areas that presented significant opportunities for improvement. Based on the findings, we provided a set of recommendations designed to address these gaps and enhance the organization's IT capabilities. The recommendations focused on the following areas:

## 1 IT Team Structure and Resourcing

- Expand the IT team to include specialized roles to address current deficiencies and support scalability.
- Formalize roles and responsibilities, particularly around governance, cybersecurity, and vendor management.
- Develop a comprehensive training program to upskill IT staff in line with evolving standards and technologies.



## 2 Network Infrastructure

- Implement a layered network architecture to enhance security and support advanced protocols.
- Upgrade network hardware to enterprise-grade components.
- Increase network segmentation and enforce strict access controls to improve security and performance.

## 3 Cybersecurity and Cloud Operations

- Conduct regular penetration testing to identify vulnerabilities and mitigate risks.
- Implement multi-factor authentication (MFA) and mobile device management (MDM) for secure remote access.
- Establish a comprehensive cybersecurity strategy with proactive monitoring and threat detection.

## 4 Backup and Disaster Recovery

- Formalize and document backup and disaster recovery plans for critical systems like IT, OT, and ERP.
- Conduct regular testing and restoration exercises to ensure data integrity and business continuity.



## 5 Vendor Management

- Formalize vendor management processes, including risk assessments and controls over third-party access.
- Develop a vendor risk management program to reduce potential exposure from external relationships.

## 6 Governance and Compliance

- Establish a formal governance framework for IT operations to ensure compliance with industry standards and regulatory requirements.
- Integrate IT into strategic planning processes to better align technology initiatives with business goals.



# Deployment Timeline

To ensure the successful implementation of these recommendations, we proposed the following phased deployment timeline, structured over 3, 6, 12, and 24 months:

## 3-Month Goals

### Immediate Security Enhancements

- Conduct internal and external penetration tests.
- Deploy multi-factor authentication (MFA) across all critical systems.
- Implement mobile device management (MDM) for secure remote access.
- Formalize IT policies and governance frameworks.
- Clarify IT team roles and responsibilities.
- Deploy web filtering, anti-virus, and anti-phishing software.

## 6-Month Goals

### Infrastructure and Access Control

- Transition to user-based access control and implement the Principle of Least Privilege (PoLP).
- Establish a formal change management process.
- Upgrade network hardware and implement a layered network architecture.
- Standardize updates and maintenance schedules.

## 12-Month Goals

### Resiliency and Vendor Management

- Conduct tabletop exercises for incident response and disaster recovery.
- Formalize and test backup and disaster recovery plans for IT, OT, and ERP systems.
- Document vendor management processes and develop a vendor risk management program.

## 24-Month Goals

### Strategic Integration and Efficiency

- Integrate IT into strategic project planning.
- Improve inter-departmental communication.
- Implement an asset management system and secure disposal processes.
- Establish formal onboarding/offboarding procedures.
- Regularly review and update policies to adapt to new technologies and threats.

# The Result

The IT assessment provided JFE with a comprehensive set of recommendations designed to enhance security, streamline operations, and improve overall IT governance. These recommendations offer clear guidance for addressing the company's existing vulnerabilities and positioning them for future growth.

The key outcomes include:

## 1 Enhanced Security Posture

- Proactive security measures, including the implementation of multi-factor authentication (MFA) and mobile device management (MDM), to secure critical systems and remote access.
- Identified the need for regular internal and external penetration testing to identify and address vulnerabilities before they can be exploited.
- Recommendations to establish robust cybersecurity practices, including web filtering and anti-phishing measures, to protect against common threats.

## 2 Optimized IT Infrastructure

- Clear guidance on upgrading network hardware to enterprise-grade components and improving network architecture with layered security, enhancing both performance and protection against breaches.
- Network segmentation and access control measures to reduce attack surfaces and enforce stricter security protocols.
- Recommendations to standardize IT system updates and maintenance schedules to ensure consistency and reduce the risk of outdated systems.

## 3 IT Governance and Operational Efficiency

- A proposed framework for formalizing IT team roles and responsibilities, which will help align IT staff with organizational goals and ensure governance and accountability.
- Creation of formal IT policies and procedures to establish a clear governance framework, ensuring that IT operations are aligned with industry standards such as ISO 27001 and NIST.
- Implementation of the Principle of Least Privilege (PoLP) and user-based access control to enhance security and simplify IT management.

## 4 Improved Disaster Recovery and Continuity

- Development of formal disaster recovery and backup strategies for critical systems, ensuring that JFE can quickly restore operations in the event of a cyberattack or technical failure.
- Recommendations for regular testing and validation of backup and recovery processes, ensuring data integrity and business continuity.

## 6 Scalable IT Framework

- Recommendations that support scalability, including IT team expansion, role specialization, and the establishment of on-call structures to ensure timely responses to IT issues as the company grows.
- Clear guidance for integrating IT into strategic business projects, ensuring that technology initiatives align with and support JFE's long-term business goals.

In summary, the IT assessment provided JFE with a solid foundation for strengthening its IT infrastructure, enhancing security, and aligning technology with strategic business objectives. With these recommendations in hand, JFE is well-equipped to address existing vulnerabilities, improve operational efficiency, and scale effectively for the future.

## 5 Vendor Risk Management

- A comprehensive vendor management strategy, including risk assessment processes and third-party access controls, to mitigate potential risks associated with external partnerships.
- Formalization of vendor management practices, including regular reviews, to ensure that all third-party services meet the company's security and operational standards.

## 7 Clear Actionable Roadmap

- A detailed, prioritized set of recommendations, providing a roadmap for the organization's IT improvements, with a focus on security, infrastructure upgrades, and IT team development.





# Interested in working together?

Let's talk about how we can help you transform your goals into achievements.

---

[synchronworks.net](https://synchronworks.net)  
[info@synchronworks.net](mailto:info@synchronworks.net)  
1.866.960.9409

