At-a-Glance Risk Summary	Assessment Determination .
☐ 5 – CRITICAL *(Should not proceed)* ☒ 4 – High *(Executive Approval Needed)* ☐ 3 – Medium *(Policy Exception Required)* ☐ 2 – Low *(Acceptable Risk)* ☐ 1 – Informational	☐ 🟩 **RECOMMENDED** *(No further review is required)* ☒ 🟨 **Recommended with Discrepancies** *(Noted in Summary)* ☐ 🟥 **Not Recommended for Advancement** *(Noted in Summary)*

Prepared by	Drew Blandford-Williams
Date	**11/03/2022**

1. Project Overview

Box Office Service Request #
PRJ0001522

Senior Leadership Sponsor:
Mark G.

Business Process Owner:
Dustin K.

Business Process Area:
Eagle Mountain Case Ready

IT Project Lead:
John D.

Risk Assessment Analyst:
Akan G.

Date: 11/03/2022

BUSINESS / PROJECT SUMMARY

The Solutions Provided by Customer Vendor/Supplier is to enable the safety and operational data capture via network connectivity for alerting, training, and management of safety events with these saws and analytic information for performance and efficiency. Provides alerts on saw safety events, cutting run times, number of cuts, efficiency measurements for each operator and provide video capture of safety events to be used in operator training. It also provides setup to remote diagnosis of Bandsaws

Currently they are implemented at 5 Fresh Meat plants and will be implemented at 18 in the future. There will be 22 devices implemented at Eagle Mountain, currently bringing 9 online for startup.

Kando Innovations has existing relationship with “Client” which is the parent of Customer Vendor/Supplier.

2. Summary, Scope & Identified RIsks

SUMMARY:

The purpose of the risk assessment was to identify threats and vulnerabilities related to the use, deployment, and integration of Guardian Band Saws into the "Client" business environment. The risk assessment will be used to identify risk mitigation plans related to this business association. Through this assessment, Guardian Band Saws has been identified as a potential high-risk system in relation to how it is planning to interact within the "Client" environment, which are referenced in this assessment report.

1. Scope of this assessment

Customer Vendor/Supplier hosts data on their Guardian servers in New Zealand data center & accessible from outside the "Client" network using any web browser access to Guardian Portal. The Guardian portal provides a web-based portal for viewing safety and performance data from the Customer Vendor/Supplier. The portal allows plant management to update and maintain the users for each of their bandsaws. The Customer Vendor/Supplier can only be operated by users, who need to login to the bandsaw using the on-screen interface.

The scope of this assessment includes all the components described above as well as a review of the TeamViewer software, which is used to provide remote support for the Customer Vendor/Supplier. This software allows for Customer Vendor/Supplier technicians to remotely view the on-screen user interface of the bandsaw, allowing them to assist on-site staff with any fault diagnosis, or perform periodic software updates. Overall, the risk behind this setup is exploitation of the Bandsaws' physical control. For an event like this to be safeguarded, multiple security controls should be implemented within the technology, thereby reducing the overall risk to potential data compromise within the "Client" environment.

2. Identified Risks

The assessment team used a modified version of the self-assessment questionnaire in NIST 800 / SP-26 "Security Self-Assessment Guide for Information Technology Systems." This questionnaire assisted the team in identifying risks

- **User Credentials & Authentication**
  Multi-factor authentication feature in accordance with Client Identity & Access Management policies is not available with vendor. Integeration with "Client" IDAM is not supported.
- **Data Integrity Compromise**
  Data Data could be inappropriately extracted/modified from "Client" database by entering SQL commands into input fields. Data (at rest), is not stored with encryption of AES 256 or stronger encryption. The potential for threat actors to bypass stated controls becomes higher, because as they gain access within the infrastructure (or move laterally once inside), the data, despite the encryption,

can be accessed in clear text. This fundamental gap is one of the main reasons that data breaches are announced almost daily and continue unhindered.

- **Potential for Denial of Service**
  A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Anti-DDOS measures are not in place for Guardian Band Saw integration.
- **Unauthorized Access**
  The system does not perform sufficient integrity checks on data input into the system. As currently demonstrated in its present state, this vendor cannot restrict access to trusted "Client" IP space if desired.
- **No SOC2 Compliance**
  SOC2 compliance is an essential component of information security for many businesses and organizations. SOC 2 audits and reports help service providers show that the privacy, confidentiality and integrity of the data they handle (i.e., protecting "Client" data is a priority for this potential partner, which has been verified through a SOC2 audit). This cendor does not have a SOC2 audit on record.

3. Actionable Details (at a glance)

Requirement	Impact / Result	Analyst Summary	Action Taken
Data Elements	○ Public Data ○ Internal Data ○ Confidential Data ● Restricted Confidential Data ○ Unspecified	Plant conditions, outage start/end time, user credentials, name, email address, telephone numbers.	● Executed ○ Informed Risk (No PolEx) ○ Actionable Risk (PolEx/Wvr)
Data in Transit	● Meets Requirements ○ May Meet Requirements ○ Does Not Comply	Data in transit encrypted using a secure SSL/TLS protocol (TLS 1.2) with 2048-bit or larger key length	● Executed ○ Informed Risk (No PolEx) ○ Actionable Risk (PolEx/Wvr)
Data at Rest	○ Meets Requirements ○ May Meet Requirements ● Does Not Comply	Data at rest is not stored with encryption of AES 256 or stronger encryption at Vendor side.	○ Executed ○ Informed Risk (No PolEx) ● Actionable Risk (PolEx/Wvr)
Access Control	○ Meets Requirements ○ May Meet Requirements ● Does Not Comply	Bandsaw users are managed by the vendor portal, not integrated with ARS.	○ Executed ○ Informed Risk (No PolEx) ● Actionable Risk (PolEx/Wvr)

Authentication / Authorization	○ Meets Requirements (Ty Mgd Auth/Auth) ○ May Meet Requirements (NON-Tyson Auth) ● Does Not Comply (NON-Tyson Auth)	No “Client” IDAM at use.	○ Executed ○ Informed Risk (No PolEx) ● Actionable Risk (PolEx/Wvr)

3. ACTIONABLE FINDINGS

Based on the information shared in this assessment and the sensitivity of data this application will have access, the security risk associated with this project is determined to be **High** level. Further investigation and executive approval for the PERs is needed prior to advancement of this project.

Potential Indicators of Compromise	Recommended Course of Action
“Client” IDAM not utilized	The authrority of user management having control over the physical Bandsaws are managed by Vendor portal, although the control will be provided to “Client”, “Client” IDAM with SSO and MFA to be utilized for secured process.
Data at rest is not stored with encryption of AES 256 or stronger encryption at Vendor side	Ensure AES 256 or higher to be placed for security of Data-at-Rest.
Vendor does not have a documented tenant key management policy/process.	Tenant key management policy/process enablement with proper confidentiality, integrity, and availability, unique for all tenants. Vendor has to provide feature for “Client”’s key management.
Encryption keys are not stored in a secure location that is separated from encrypted data	Encryption keys to be placed in a secure storage, separate from encrypted data, and protected from- Generation until no longer needed.
The system can not enforce password expiration standards	Strict password policy shall be in place including length/complexity/expiration/aging and lockout enablement.
Anti-DDOS measures are not in place for this solution.	DDOS protection measures and relevant incident response plan in place to be available for proper Availability.
Vendor’s system cannot automatically deliver a user access report on a scheduled basis.	Users access to be monitored and shared with “Client” on a periodic basis. “Client” IDAM provides this, but an added control over the usage of Bandsaws to be shared periodicaly.

An insurance policy is not in place to provide compensation to a customer in the event of a loss or breach of customer data.	Insurance policy in place to provide compensation to customer in the event of a loss or breach of customer data and to be included in the contract.
High availability measures are not in-place.	High Availability with minimum down-time and sorted recovery issues with adequate subscriptions (whichever applicable) to be in place.

4. ASSESSMENT ARTIFACTS

NARRATIVE:

The Customer Vendor/Supplier uses EtherCAT for fieldbus communication to all I/O modules and devices. This includes standard I/O terminals, as well as the variable speed drive (VSD) for controlling the bandsaw motor and a valve island for the onboard pneumatics.

Each saw is equipped with 4 cameras that allow for configuration of the safety zone, any violation of the safety zone stops the saw and transmits video and saw statistics to the Guardian server in New Zealand. Each saw will also send periodic saw statistics to the Guardian server.

Customer Vendor/Supplier hosts data on their Guardian servers in New Zealand data center providing a portal to be used by management to setup and maintain the list of operators for each bandsaw. This includes creating new operator logins, editing existing logins and changing user passwords.

Transmitted Data to Vendor:

1. When a safety activation occurs, the following data is transferred:

- Machine specific information (company, location, machine name)
- The current user logged into the bandsaw
- The reason for the safety activation (e.g., "Vision Not Safe", "E-Stop Pressed", "Door Opened")
- A short video of the safety activation. This video is approximately 10 seconds in duration and is a slow-motion capture from the 4 bandsaw cameras showing 1.2 seconds before and 0.8 seconds after the safety activation.

2. When the bandsaw is stopped normally (i.e., by the operator pressing the STOP button) the following data is transferred:

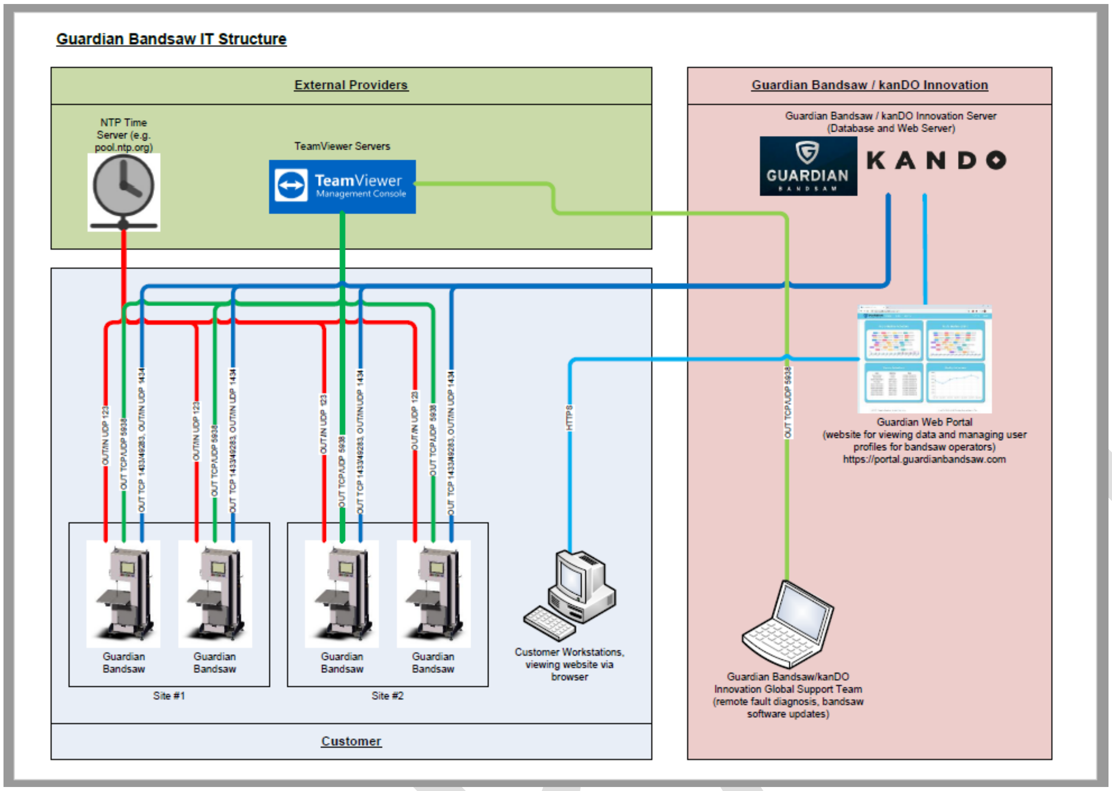
- Machine specific information (company, location, machine name)
- The current user logged into the bandsaw
- The start and end date/time for the preceding run
- The number of cuts recorded by the bandsaw during this run
- The average power (in kilowatts) used by the bandsaw motor during the run
- The total power consumption (in kilowatt-hours) during the run

Technical:

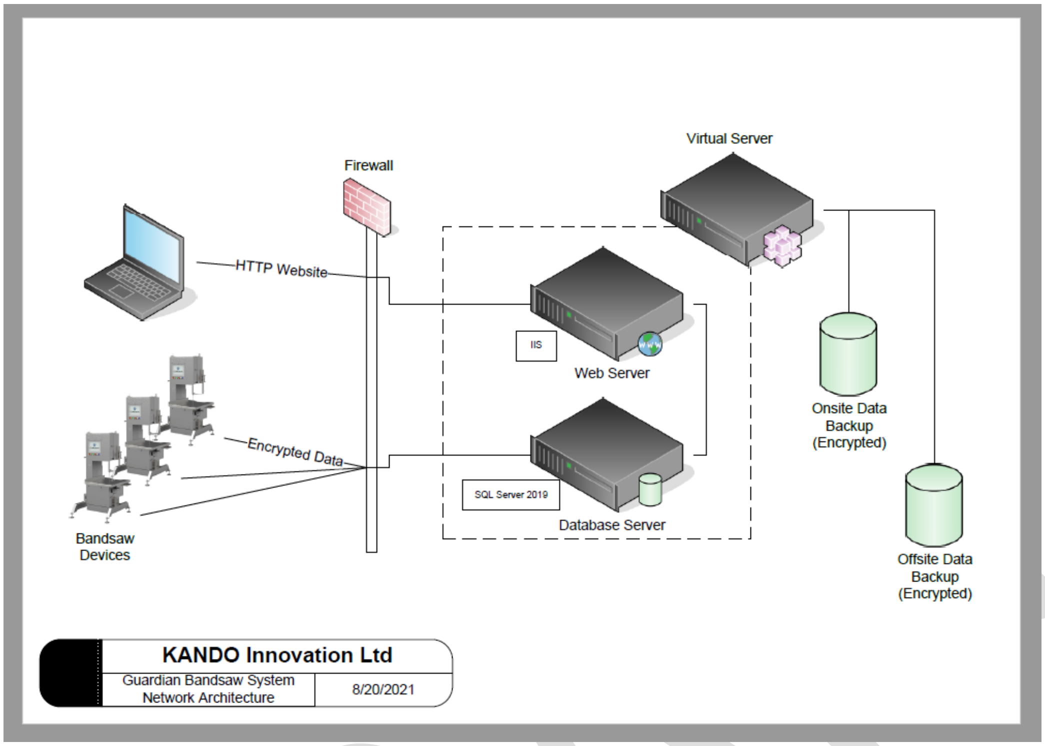
- SOC2 Type II and ISO 27001 Certification is not currently held by Customer Vendor/Supplier.
- System cannot provide admin audit logs, user audit logs, and data access logs.
- Vendor doesn't have an information security team to handle security concerns.
- Vendor doesn't conduct external audits regularly as prescribed by industry best practices and guidance.
- Website penetration testing was performed by 3rd party on 20-08-2021. During this assessment, 34 issues were found in total, 8 low and 26 informational severity issues. Of the 34 issues, XXX were reported to be tied to **[[a former release / open source bug reported / design flaw / authentication tie-in, etc]]**
- Network Vulnerability Scan was performed by 3rd party on 21-08-2021. During this assessment, 86 issues were noted in total, 2 High, 9 Medium, 64 low and 11 informational issues. **[[Again, explain why this is relevant and which issues should be considered as being called out for reference]]**
- The system cannot restrict access to trusted "Client" IP space if desired, especially for administrators and highly privileged users.
- Anti-DDOS measures are not in place for this solution. **[[Why is this important and what does an "anti-DDoS solution" look like?]]**
- Vendor does not have a documented tenant key management policy/process.
- Vendor does not have the ability to physically or logically segment customer data from the data of other tenants.
- Do not have a capability to continuously monitor and report the compliance of infrastructure against established information security baselines.
- Any third-party vendors and remote workers of Customer Vendor/Supplier are not utilizing multi-factor authentication when accessing company resources remotely.
- Periodic employee awareness is not evident

NETWORK DIAGRAM:

1. The Business team has shared this diagram:


Guardian Bandsaw IT Structure
External Providers
NTP Time Server (e.g. pool.ntp.org)
TeamViewer Servers
TeamViewer Management Console
Guardian Bandsaw / kanDO Innovation
Guardian Bandsaw / kanDO Innovation Server (Database and Web Server)
GUARDIAN BANDSAW
KANDO
OUT/IN UDP 123
OUT TCP/UDP 5938
OUT TCP 1433/49283, OUT/IN UDP 1434
OUT/IN UDP 123
OUT TCP/UDP 5938
OUT TCP 1433/49283, OUT/IN UDP 1434
OUT/IN UDP 123
OUT TCP/UDP 5938
OUT TCP 1433/49283, OUT/IN UDP 1434
OUT/IN UDP 123
OUT TCP/UDP 5938
OUT TCP 1433/49283, OUT/IN UDP 1434
HTTPS
OUT TCP/UDP 5938
Guardian Web Portal (website for viewing data and managing user profiles for bandsaw operators) https://portal.guardianbandsaw.com
Guardian Bandsaw
Guardian Bandsaw
Guardian Bandsaw
Guardian Bandsaw
Site #1
Site #2
Customer Workstations, viewing website via browser
Guardian Bandsaw/kanDO Innovation Global Support Team (remote fault diagnosis, bandsaw software updates)
Customer

2. The architecture diagram shared by vendor:


Firewall
Virtual Server
HTTP Website
IIS
Web Server
Onsite Data Backup (Encrypted)
Encrypted Data
SQL Server 2019
Database Server
Bandsaw Devices
Offsite Data Backup (Encrypted)
KANDO Innovation Ltd
Guardian Bandsaw System Network Architecture
8/20/2021