convergent

GZ Media Group

MPA 5.1

Evaluation Date: 25-Mar-2024

Report Issued: 13-Apr-2024

Evaluator: Alex Vaughan

STRICTLY PRIVATE & CONFIDENTIAL

Disclaimer

This Report has been commissioned directly by GZ Media - Lodenice, Czech Republic ("the Owner"). It is intended to provide GZ Media - Lodenice, Czech Republic ("Company") with a view of the security of its management systems, physical and digital environments. Convergent Risks Inc ("Convergent", "we", "us" or "our") has prepared this report (including any enclosures and attachments) for the exclusive use and benefit of the Company and solely for the purpose for which it is provided. Unless we provide express prior written consent, no part of this report should be reproduced, distributed, quoted, or communicated in any way to any third party. We do not accept any liability if this report is used for an alternative purpose from which it is intended, nor to any third party in respect of the findings of this report.

The purpose of this report is to provide an opinion, based on our assessment, about the security of the Company's physical and digital measures, organizational processes, and systems in accordance with the MPA's Content Security Best Practices (version 5.1) framework controls. Whilst we endeavor to provide recommendations which minimize the likelihood of content loss and/or theft occurring, Convergent makes no representations or warranties of any kind, express or implied, about the suitability, application, or implementation of the assessment and/or recommendations detailed within this report to an individual vendor. Any reliance you place on the use of such assessment and/or recommendations, as well as any results yielded, is therefore strictly at your own risk. Information contained in this report is current as of the date of this report and may not reflect any event or circumstances which occur after the date of this report.

Document Control

Version	Date	Name	Action
1.0	4/11/2024 4:01:34 PM	SanctumHUB	Document generated from system data

Table of Contents

1 Executive Summary

GZ Media Group, a leading vinyl record manufacturer with a global footprint, boasts 8 production plants worldwide and over 2,700 employees. Established in 1951, the company has continuously expanded its vinyl products and services while also offering premium print services, warehousing, and distribution. Holding ISO certifications for quality, environmental management, and supply chain security, GZ is committed to excellence across all facets of its operations.

In addition to vinyl production, GZ Media plays a significant role in digital content distribution, adhering to stringent security protocols. Leveraging its expertise and advanced technologies, GZ provides a diverse range of vinyl records and packaging to support artists and labels in their creative marketing endeavors.

The vendor's campus spans approximately 80,000 square meters, meticulously secured with a 24/7 security presence, electronic access controls, CCTV monitoring, and comprehensive access management. Rigorous security measures, including perimeter fencing, access control, and security checks, are in place to safeguard the facility. Employee security is paramount, with strict enforcement of non-disclosure agreements and thorough screening processes for all personnel.

GZ Media Group successfully underwent a Content Owner Protection Security assessment, achieving a high level of compliance with the MPA Content Security Best Practices version 5.1.

Physical asset handling workflow:

GZ Media Loděnice specializes in customized physical processes for vinyl production, including mastering, pressing, packaging, and shipping. Upon delivery, assets like stampers are securely stored and tracked in the IFS system. Palletized content undergoes visual inspections before being loaded onto courier vehicles. Alias use ensures privacy, and detailed shipping logs comply with regulations. Shipments are restricted to the Production department, with strict access controls and thorough product confirmations. Additionally, robust security measures ensure the secure handling of high-security assets, including custom management tools and adherence to stringent content security standards.

Digital content handling workflow:

Periodically, GZ receives client content via secure transfer servers like Aspera or Signiant client servers, ensuring both physical and digital restrictions within the data I/O environment. Symantec antivirus scans all content for viruses and malware before it's transferred into the isolated production network. Work is executed in accordance with industry standards and client requirements within this environment.

Upon completion, the necessary deliverables, including client-specified Masters, undergo rigorous testing and packaging processes. These are then entrusted to client-specific couriers for physical delivery, as there is no digital delivery of assets. After project completion, source files and master stampers are retained for future order fulfillment needs.