# Hardware Risk Analysis Report

## Contents

### Overview:

This document provides a risk analysis of the current hardware infrastructure based on the below mentioned inventory:

| System | Case (1U/2U) | OS | Host name | SerialNumber |
|---|---|---|---|---|
| SPCB-AUDLOG01 | 1u | Windows Server 2012 R2 Standard | SPCB-ALOGGER01 | CZJ5300FXZ |
| Storage | 2U | Windows Storage | SPCB-STORAGE01 | CZ26110366 |
| SPCB-AVSERVER01 | 1u | Windows Server 2012 R2 Standard | SPCB-AVSERVER01 | CZJ54104X2 |
| SPCB-AUDLOG02 | 1U | Windows Server 2012 R2 Standard | SPCB-ALOGGER02 | CZJ6100MVV |
| Storage | 2u | Windows Storage | SPCB-STORAGE02 | CZJ6110NKG |
| SPCB-VLOGGER04 | 2u | Windows Server 2012 R2 Standard | SPCB-VLOGGER04 | CZJ6110QJJ |
| SPCB-VLOGGER03 | 2u | Windows Server 2012 R2 Standard | SPCB-VLOGGER03 | CZJ6110QJK |
| SPCB-VLOGGER02 | 2u | Windows Server 2012 R2 Standard | SPCB-VLOGGER02 | CZJ6110QJH |
| SPCB-VLOGGER01 | 2u | Windows Server 2012 R2 Standard | SPCB-VLOGGER01 | CZJ6110QJL |
| SPCB-AUDIOAV | 2u | Windows Server 2012 R2 Standard |  | CZJ6110QJM |

All systems were purchased between late 2015 and early 2016. The organization intends to extend support for these systems until the end of 2027. Below is the detailed assessment and proposed mitigation plan.

## 1. Hardware Age & Reliability Risk:

- **Critical Hardware Aging**: All systems in use are 9–10 years old and would exceed 12 years of service by 2027—well beyond typical enterprise hardware lifecycles. This significantly increases the likelihood of component failure and service disruption.

- **End-of-Life (EOL) Status**: All major hardware components, including servers and storage units, will reach or have already reached EOL/EOS (End of Support) status. Continued operation beyond this point introduces unacceptable risks.

- **Reliability Concerns**: Aging power supplies, motherboards, and especially hard disk drives (HDDs), which are mechanical in nature, face sharply rising failure rates. These issues are difficult to predict and can result in prolonged unplanned outages.

- **No Replacement Parts Availability**: As manufacturers phase out legacy hardware, replacement parts are becoming increasingly rare or obsolete. This reduces the ability to recover quickly from failures and increases total downtime risk.

- **Operational Risk**: Maintaining systems beyond their designed lifespan places an unsustainable burden on IT support and introduces unacceptable risk to business operations and data integrity.

## 2. Storage Risks:

- **High Risk of Mechanical Failure**: The current storage infrastructure relies heavily on aging hard disk drives (HDDs), some supporting capacities up to 72 TB and 2x120 TB configurations. These drives are well past their optimal lifespan and increasingly prone to mechanical failure, posing a serious risk to data availability and integrity.

- **Lack of Redundancy and Modern Safeguards**: Older storage systems lack advanced fault tolerance and predictive failure technologies found in modern solutions. As a result, failures may go undetected until data loss or service interruption occurs.

- **End-of-Life Components**: Many of the storage subsystems are at or nearing EOL, making firmware updates, vendor support, and spare parts nearly impossible to obtain.

- **Increased Risk of Data Loss**: Without modern data protection features such as integrated snapshotting, deduplication, and encryption, the risk of data corruption or loss is significantly higher.

## 3. Support & Warranty:

- **Outdated Warranty Coverage**: All current systems are beyond their original manufacturer support periods, with OEM warranties fully expired. This leaves the organization dependent on third-party maintenance providers, which often offer limited coverage and slower response times.

- **Lack of Critical Updates**: With hardware reaching end-of-life status, there are no longer firmware or driver updates available from vendors. This prevents the resolution of emerging vulnerabilities and compatibility issues, increasing both security and operational risk.

- **Escalating Maintenance Costs**: The cost and complexity of maintaining legacy systems continue to rise, particularly as parts become scarce and specialized support more difficult to secure.

- **Increased Downtime Risk**: The absence of vendor-backed SLAs (Service Level Agreements) means any failure can result in extended outages and delayed recovery, especially when relying on refurbished components or unsupported configurations.

## 4. Security Risks:

**- Legacy Operating Systems Pose Critical Threats**: The infrastructure is built on Windows Server 2012 R2, which is no longer supported as of October 2023. Operating unsupported systems leaves the environment exposed to unpatched vulnerabilities and advanced persistent threats.

**- Lack of Modern Hardware Security Features**: The current hardware lacks essential security technologies such as Trusted Platform Module (TPM) 2.0, Secure Boot, and hardware-assisted virtualization protections. This makes it incompatible with current cybersecurity standards and regulatory requirements.

**- Increased Exposure to Targeted Attacks**: Legacy systems are frequent targets for exploitation due to widely known vulnerabilities and the absence of vendor security updates. Continuing to operate them significantly increases the risk of data breaches and ransomware incidents.

## 5. Recommendations:

- **Initiate Full Hardware Replacement by 2026**: Develop and execute a complete replacement plan for all legacy systems to eliminate exposure to hardware failures, unsupported components, and security vulnerabilities.

- **Transition to Modern OS Platforms**: Deploy systems with supported operating systems such as Windows Server 2019 or 2022 to ensure access to security updates, compliance features, and vendor support.

- **Upgrade to Secure, Scalable Infrastructure**: Invest in hardware that supports current security standards (e.g., TPM 2.0, Secure Boot, UEFI), virtualization capabilities, and future workload scalability.

- **Retire Legacy Systems and Software**: Decommission all systems running Windows Server 2012 R2 and other unsupported environments to remove systemic vulnerabilities.

- **Implement Robust Monitoring and Backup Solutions**: Modernize backup, redundancy, and disaster recovery strategies to align with new infrastructure and ensure business continuity.

## 6. Conclusion:

Given the advanced age of the current hardware infrastructure and the escalating risks associated with hardware failure, lack of support, and severe security vulnerabilities, it is no longer advisable to maintain these systems beyond 2025. The increasing likelihood of downtime, combined with unpatchable security exposures due to unsupported operating systems and obsolete firmware, presents a significant threat to operational continuity and data integrity.

We strongly recommend a complete replacement of all legacy hardware by 2026. This proactive approach will ensure compatibility with modern operating environments, restore vendor support, reduce operational risks, and significantly strengthen the organization’s cybersecurity posture. Delaying this transition could result in critical failures, extended outages, and potential data breaches/lost.