Information Security Control Requirements for CGA Licensed for CGA Licensees (B2C and B2B)

April 2026

Contents

Introduction

The Curaçao Gaming Authority (CGA) has developed these Information Security Guidelines to establish foundational cybersecurity requirements for **all CGA licensees** within its jurisdiction, **including both Business-to-Consumer (B2C) gaming operators and Business-to-Business (B2B) gaming technology providers.** Where this document refers to "licensees" or "operators," it applies equally to B2C and B2B entities unless a specific distinction is noted. Recognizing the diversity in operational scale, technological complexity, and cybersecurity maturity across the gaming sector, this document provides a **practical baseline** based on the **Center for Internet Security (CIS) Controls Implementation Group 1 (IG1)**.

IG1 represents the **starting point** of a broader cybersecurity roadmap designed to raise the security posture of all licensees while supporting regulatory compliance, data protection, and operational resilience.

These requirements are issued by the CGA to ensure the operator provides a safe and secure gaming environment to its players as required by the 'Landsverordening op de Kansspelen (LOK)' and Landsverordening Casinowezen Curacao (LCC)'.

1.1 Legal Basis and Authority

These Information Security Control Requirements are issued pursuant to the Landsverordening op de Kansspelen (LOK) and the Landsverordening Casinowezen Curaçao (LCC), including but not limited to the provisions relating to:

- the integrity, security, and reliability of gaming systems;
- the protection of player data and financial information;
- the prevention of fraud, manipulation, and unauthorized access; and
- the Curaçao Gaming Authority's supervisory and enforcement powers.

Compliance with these requirements constitutes a **mandatory condition of licensure** under the LOK.

1.2 Regulatory Interpretation

Unless explicitly stated otherwise, the terms *must*, *shall*, and *required* indicate **binding regulatory obligations** under the LOK.

The term *should* is used only where proportional or risk-based implementation is permitted by the Authority.

1.3 Cybersecurity Maturity Roadmap Approach

These guidelines form the **first phase** of a progressive cybersecurity maturity framework tailored to the risk and regulatory profile of the gaming industry:

- **IG1 – Foundation (This Document):**
  Designed as the mandatory baseline for small to medium-sized gaming operators. IG1 emphasizes essential security practices to defend against **common, non-targeted attacks** while supporting continuity of operations and regulatory obligations.
- **IG2 – Recommended Target (Future Guidance):**
  CGA strongly recommends that all licensed operators plan to achieve **IG2 maturity within 24 to 36 months**. IG2 is more appropriate for gaming environments due to their exposure to sensitive player data, financial systems, and increased threat vectors. It includes enhanced controls for **vulnerability management, centralized logging, and asset tracking**.
- **IG3 – Strategic Goal:**
  Intended for large gaming enterprises with mature IT operations and dedicated security personnel, IG3 provides advanced safeguards against **targeted, sophisticated threats** and enables operators to meet evolving regulatory expectations.

Note: While IG1 forms the enforceable baseline, CGA views IG2 as the **appropriate cybersecurity target** for most operators in the industry.

1.4 Alignment with ISO 27001 and Industry Standards

These guidelines are intentionally designed to align with internationally recognized cybersecurity and governance frameworks, supporting broader compliance efforts and industry best practices:

- **ISO/IEC 27001:2022:**
  Where CIS IG1 controls map to ISO 27001 Annex A controls, the mapping is noted throughout this document. This enables operators to integrate these controls directly into an **Information Security Management System (ISMS)** and work toward ISO certification if desired.
- **Recognized Gaming Security Frameworks:**
  Incorporates gaming-specific cybersecurity controls recognized by CGA-approved testing laboratories and audit firms.
- **IGSA Standards (Land-Based Operations):**
  Where applicable, aligns with the **International Gaming Standards Association**

protocols for secure system communications and device interoperability in land-based gaming environments.

Note on Unmapped Controls:
Some CIS IG1 controls do not have direct ISO 27001 equivalents but are included due to their **foundational importance** for risk reduction, particularly in smaller or hybrid environments.

1.5 Industry Alignment and Format

This guideline adopts a structure consistent with those issued by established international gaming regulators, ensuring clarity and operational familiarity for global operators.

- **Regulatory Best Practices:**
  Reflects the structure of cybersecurity guidance from established international gaming regulators.
- **Industry Audit Frameworks:**
  Aligned with **CGA-recognized gaming security audit frameworks**, supporting readiness for third-party assessments by approved testing laboratories.
- **International Harmonization:**
  Mirrors the format and control references of **ISO/IEC 27001:2022**, promoting cohesive compliance across jurisdictions and standards.

1.6 LOK Security Objectives

These requirements implement the LOK's core security objectives, namely to ensure that:

- gaming systems operate in a secure, controlled, and auditable manner;
- game outcomes, RNG processes, and transaction records are protected against manipulation;
- player data, payment data, and responsible gaming records are safeguarded;
- licensees maintain continuous operational control over outsourced or third-party systems; and
- the Authority can effectively supervise, investigate, and enforce compliance.

The CIS Controls Implementation Group 1 (IG1) framework is adopted as a *means* to achieve these statutory objectives, not as the *legal basis* for these requirements.

1.7 Scope

- These guidelines apply to **all holders of a CGA license**, regardless of whether they operate in a B2C or B2B capacity. B2B gaming technology providers are subject to these requirements **in their own right as CGA licensees**, not solely by virtue of being referenced in a B2C operator's compliance documentation. The requirements are applicable across the following categories:**Land-based gaming establishments**
- **Online gaming operators** (including B2C platforms)
- **Gaming technology providers** (B2B platforms)
- **Hybrid operators** offering both land-based and online services

Operating Model Considerations

The applicability of specific controls varies based on the licensee's operating model:

- **White-label and hosted B2C operators:** Where licensees operate on third-party platforms, the licensee remains fully responsible under the LOK for ensuring compliance. Technical controls implemented by the B2B provider must be verified through contractual assurances, due diligence assessments, and ongoing monitoring. The licensee must maintain documentation demonstrating how each applicable control is addressed.
- **Cloud-hosted operators:** For operators utilizing cloud infrastructure services (e.g., AWS, Azure, Google Cloud), hardware-specific controls are addressed through the shared responsibility model. Licensees must document which controls are managed by the cloud provider and maintain evidence of the provider's compliance certifications (e.g., SOC 2, ISO 27001). Licensees remain responsible for all controls within their sphere of responsibility.
- **Land-based specific controls:** Certain controls relating to physical hardware, IGSA protocols (e.g., G2S), and real-time monitoring systems apply specifically to land-based operations. These are identified as "Land-Based" where applicable.
- **Certified RGS and game content:** For online operators using certified Remote Gaming Servers and game content from licensed B2B providers, the following responsibility allocation applies:

- **B2B provider obligation:** The B2B provider, as a CGA licensee in its own right, bears direct regulatory responsibility for obtaining, maintaining, and renewing all required certifications for its gaming components, including RNG integrity, game logic, and RGS platform security. The B2B provider must proactively notify its B2C partners and the CGA of any changes to certification status, including lapses, withdrawals, scope changes, or pending renewals.
- **B2C operator obligation:** The B2C licensee is not responsible for the B2B provider's certification process but must exercise reasonable due diligence, including: (a) verifying the B2B provider's certification status at the point of onboarding and at defined intervals thereafter (at minimum annually); (b) including contractual provisions requiring the B2B provider to maintain valid certifications and to notify the B2C operator promptly of any changes; (c) promptly notifying the CGA if the B2C operator becomes aware that a B2B provider's certification has lapsed or been withdrawn; and (d) ceasing to offer game content from any B2B provider whose required certifications are no longer valid, until such certifications are restored.
- **CGA role:** The CGA maintains a register of certified B2B providers and their certification status. The CGA may notify B2C licensees directly of changes to a B2B provider's certification status and may require B2C operators to cease using affected components within a defined timeframe.

B2C and B2B Shared Responsibility Framework

The following table defines the allocation of information security responsibilities between B2C operators, B2B providers, and the CGA for key domains where gaming operations involve both license types. This framework recognises that B2C operators cannot exercise direct control over a B2B provider's internal systems or certification processes, and therefore focuses B2C obligations on due diligence, contractual assurance, and regulatory notification.

Game/RNG certification	Holds and maintains certification	Verifies status; contractual requirement	Registers and enforces
Game content integrity	Ensures integrity of supplied components	Monitors for anomalies; reports concerns	Audits and validates
Sports data feed integrity	Validates source authenticity and signing	Verifies feed integrity; contractual SLAs	Reviews controls
Platform security controls	Implements controls on own infrastructure	Implements controls on own infrastructure	Assesses both independently
Player data protection	Processes per B2C instructions and contract	Data controller obligations under LOK	Supervises compliance
Incident notification	Notifies B2C and CGA per contractual and regulatory obligation	Notifies CGA per LOK requirements	Receives, investigates, enforces
Certification lapse	Must remediate or cease supply	Must cease use of uncertified components; notify CGA	May suspend affected operations

Note: Contractual delegation of operational controls to a B2B provider does not relieve the B2C licensee of its regulatory accountability under the LOK. However, the nature of that accountability is one of due diligence, verification, and reporting—not direct operational control over the B2B provider's systems or processes.

1.8 Compliance Requirements

All licensed operators must implement the IG1 controls within **12 months** of license issuance or the date of publication of these guidelines.

While all IG1 controls are **mandatory**, CGA acknowledges that smaller operators may face constraints in staffing and technical resources. To support compliance, CGA will provide:

- A **Minimum Viable Implementation Checklist**
- Guidance on **low-cost and scalable solutions**, including open-source tools, automation, and managed service options

This ensures that compliance is not only **achievable and measurable**, but also aligned with real-world constraints while upholding the **baseline security expectations** for the gaming industry.

Operators must demonstrate compliance through:

- **Annual self-assessment reports**, using CGA-provided templates
- **Independent third-party security audits** (mandatory for online operators)
- **Incident reporting**, in accordance with CGA breach notification requirements
- **Ongoing compliance monitoring** by CGA through reviews, inspections, and technical validation

Foundational Security Controls Framework

This section outlines the baseline set of cybersecurity controls that all licensed operators under the Curaçao Gaming Authority (CGA) are required to implement. These controls are based on the Center for Internet Security (CIS) Controls Implementation Group 1 (IG1), which represents essential cyber hygiene practices for organizations with limited resources or technical staff. Each control includes a requirement, detailed implementation guidance, and specific considerations tailored for gaming environments. Where applicable, controls are mapped to ISO/IEC 27001:2022 clauses to support integrated compliance efforts.

1.9 Identify and Manage All Hardware and Software Assets

Establishing full visibility over enterprise assets is a critical first step in reducing cybersecurity risk. Operators must maintain an accurate inventory of both physical and digital assets used to support gaming operations and ensure unauthorized assets are identified and addressed promptly.

These controls align with **CIS Controls 1 and 2** and support **ISO/IEC 27001:2022 Annex A control A.5.9** (Inventory of Information and Other Associated Assets).

1.9.1 Maintain a Complete Inventory of Enterprise Devices

Operators are required to establish and maintain a complete and accurate inventory of all enterprise devices that interact with gaming data or systems.

Implementation Guidance:

- Document all enterprise hardware assets, including:
    - Gaming terminals and slot machines, in land based operations.
    - Application and infrastructure servers (gaming, financial, player management)
    - Networking hardware (routers, switches, firewalls)
    - End-user computing devices (desktops, laptops, tablets, smartphones)
    - Internet of Things (IoT) devices (e.g., surveillance cameras, sensors)
- Record key attributes for each device:
    - Static IP or MAC address

  - Hostname or device identifier
  - Asset owner or responsible business unit
  - Network approval or access status
- Perform a formal inventory review at least twice annually.
- **Gaming-specific consideration:** Include specialized gaming hardware such as electronic table management systems, loyalty tracking devices, and cashless wagering equipment.

This control maps to CIS 1.1 and supports ISO/IEC 27001:2022 control A.5.9.

1.9.2 Detect and Address Unauthorized Devices

Operators must proactively identify and respond to unauthorized assets that may appear within their networks or environments.

Implementation Guidance:

- Establish a documented weekly procedure to identify and respond to unauthorized devices.
- Use automated discovery tools or manual verification to detect rogue or unmanaged assets.
- Take appropriate mitigation actions such as:
  - Removing the device from the network
  - Blocking remote access
  - Placing the device in a quarantined zone
- Keep a log of incidents, actions taken, and justifications for any exceptions.
- **Gaming-specific consideration:** Give priority to identifying devices that could impact game fairness, manipulate outcomes, or introduce data protection risks.

This control maps to CIS 1.2. There is no direct ISO 27001 mapping, but it is considered a foundational security capability.

1.9.3 Maintain a Detailed Software Inventory

Operators must track all authorized software deployed within the organization to reduce risk from unauthorized, unsupported, or outdated applications.

Implementation Guidance:

- Maintain an inventory of all software used, including:
    - Gaming software platforms
    - Operating systems
    - Endpoint and server security tools
    - Reporting, management, and compliance applications
    - Jurisdiction ROM Version for Slot Machines for land based.
- Document for each game software entry, where applicable, according to industry specific requirements:
    - Title and game variant
    - Version and installation date
    - Purpose and associated business function
    - Number of licenses or installations
- Review and update the software inventory bi-annually. For land-based gaming environments using central management systems, software inventory shall be maintained in real time through automated tracking of all gaming machine software components.
- **Gaming-specific consideration:** Ensure tracking includes RNG software, game engines, and other components subject to regulatory oversight.

This control maps to CIS 2.1 and supports ISO/IEC 27001:2022 control A.5.9.

1.9.4 Verify Software Support Status and Address Unsupported Applications

Operators must verify that all installed software is currently supported by vendors and establish procedures to manage unsupported software.

Implementation Guidance:

- Conduct monthly checks to validate vendor support status for all approved software.
- Remove unsupported software or apply documented exceptions with mitigating controls.
- Define approval workflows for exceptions, and document:
    - Risk acceptance rationale
    - Compensating controls in place (e.g., network isolation, restricted access)
- **Gaming-specific consideration:** "**Land-based operators** shall coordinate closely with gaming software vendors to manage lifecycle dependencies for certified systems. Online B2C operators using certified Remote Gaming Servers and game content from licensed B2B providers are not responsible for game lifecycle management or the B2B provider's certification process. **The obligation to obtain and maintain valid certifications rests with the B2B provider as a CGA licensee.** The B2C operator must: (a) verify the B2B provider's certification status at onboarding and periodically thereafter; (b) contractually require the B2B provider to maintain certifications and provide timely notification of any status changes; and (c) notify the CGA if the B2C operator becomes aware of lapsed or withdrawn certifications affecting components in use.

This control maps to CIS 2.2 and 2.3. There is no direct ISO 27001 mapping, but it is considered essential to maintaining a secure baseline configuration.

1.10 Protect Sensitive and Regulated Data

Effective protection of sensitive data is critical in gaming environments due to the high volume of personal information, financial transactions, and regulated records involved. This section outlines the required practices for classifying, handling, storing, and disposing of sensitive data. Controls are aligned with **CIS Control 3** and support various clauses in **ISO/IEC 27001:2022**, including A.5.9, A.5.10, A.5.15, A.5.33, A.6.7, and A.8.1.

1.10.1 Establish a Documented Data Management Process

Operators must define and document how data is classified, handled, retained, and disposed of to ensure compliance and data protection.

Implementation Guidance:

- Classify all data types into sensitivity categories such as:
    - **Critical Gaming Data (e.g., game event outcomes, high-value transactions, jackpot triggers, sports data feeds and live odds, game results received from B2B providers or content aggregators, RNG output records, and aggregated content used to determine wager outcomes)Player Personal Data** (e.g., identity documents, payment details, behavioral data)
    - **Business Confidential Information** (e.g., internal financials, operational strategies)
    - **Public Data** (e.g., website content, marketing materials)
- Document handling procedures for each classification, including:
    - Access restrictions
    - Storage locations and protections
    - Sharing and transfer protocols
- Define minimum and maximum retention periods for each classification.
- Specify approved disposal procedures for data at end-of-life.
- **Review frequency:** Annually or upon significant system, regulatory, or process change.
- **Gaming-specific consideration:** Include specific procedures for safeguarding player protection data and storing regulatory gaming records.

This control maps to CIS 3.1 and supports ISO/IEC 27001:2022 controls A.5.9 and A.5.10.

1.10.2 Maintain a Central Inventory of Sensitive Data Locations

Operators must maintain an up-to-date record of all locations where sensitive data is stored, processed, or transmitted.

Implementation Guidance:

- Identify and document all physical and logical storage locations, including:
    - On-premise databases and application servers
    - File systems and shared drives
    - Cloud-based storage platforms and backup repositories
- Clearly label each data store by data type and classification.
- Prioritize accurate mapping of locations holding gaming-critical and personal player data.
- **Update frequency:** At least once annually or during significant changes to infrastructure.

This control maps to CIS 3.2 and supports ISO/IEC 27001:2022 control A.5.9.

1.10.3 Restrict Data Access Based on Role and Necessity

Access to sensitive data must be limited using role-based access controls and the principle of least privilege.

Implementation Guidance:

- Establish access policies that enforce "need-to-know" restrictions.
- Use role-based access control (RBAC) to manage permissions.
- Review access settings regularly for the following systems:
    - Gaming databases (e.g., game event outcomes, jackpot logs)
    - Player personal information account data and loyalty systems
    - Financial transaction records and bonusing schemes systems
    - Security and audit systems
- **Gaming-specific consideration:** Clearly distinguish access privileges for gaming floor personnel, administrative users, and third-party vendors.

This control maps to CIS 3.3 and supports ISO/IEC 27001:2022 controls A.5.15 and A.8.3.

1.10.4 Define Data Retention Periods and Ensure Secure Disposal

Operators must define and enforce retention policies and ensure that data is disposed of securely when no longer required.

Implementation Guidance:

- Establish retention schedules for all data categories, in line with:
    - Regulatory requirements
    - Business and operational needs
- Implement secure data disposal processes, including:
    - Cryptographic erasure
    - Overwriting or degaussing
    - Physical destruction of media
- **Gaming-specific consideration:** Ensure retention schedules comply with local laws or license conditions (e.g., retain gaming transaction records for 5years).

This control maps to CIS 3.4 and 3.5 and supports ISO/IEC 27001:2022 controls A.5.33 and A.5.10.

1.10.5 Encrypt Sensitive Data on End-User Devices

Operators must encrypt all sensitive data stored on user-accessible devices to prevent exposure in case of loss or theft.

Implementation Guidance:

- Apply full-disk encryption (FDE) on laptops, tablets, and mobile devices that store or process regulated data.
- Use industry-standard encryption tools and protocols appropriate for the operating system in use (such as full-disk encryption solutions for Windows, macOS, and Linux environments).
- Ensure encryption keys are managed securely.

- **Gaming-specific consideration:** Verify that encryption solutions are compatible with gaming applications and do not disrupt system performance.

This control maps to CIS 3.6 and supports ISO/IEC 27001:2022 controls A.6.7 and A.8.1.

1.11 Apply Secure Configuration to All Systems and Devices

Improperly configured systems are a common target for exploitation. All CGA-licensed operators must apply secure configurations across enterprise systems, including servers, endpoints, gaming terminals, and networking equipment. These controls align with **CIS Control 4** and support **ISO/IEC 27001:2022** controls A.8.5, A.8.9, A.6.7, and A.8.1.

1.11.1 Define and Maintain Secure Configuration Standards

Operators must develop and maintain documented secure configuration standards for all technology systems used in the gaming environment.

Implementation Guidance:

- Develop system hardening guides for the following asset categories:
    - Gaming terminals and floor equipment
    - Physical and virtual servers
    - Security appliances (e.g., intrusion detection systems, firewalls)
    - User endpoints (e.g., laptops, desktops)
    - Network infrastructure (e.g., routers, switches)
- Use vendor-recommended hardening templates or recognized industry baselines (e.g., CIS Benchmarks).
- Review and update configuration standards annually, or when deploying new technologies.
- **Gaming-specific consideration:** Ensure that performance requirements for gaming systems are preserved when applying hardening standards.

This control maps to CIS 4.1 and 4.2 and supports ISO/IEC 27001:2022 control A.8.9.

1.11.2 Implement Automatic Session Locking on User Devices

To reduce the risk of unauthorized access, all user systems must be configured to lock automatically after a defined period of inactivity.

Implementation Guidance:

- Set lockout timers as follows:
    - General systems: 15 minutes maximum

    - Mobile devices: 2 minutes maximum

- Apply settings through centralized configuration management tools or group policy.
- **Gaming-specific consideration:** Adjustments may be required for gaming terminals actively engaged in player sessions; ensure changes are documented and risk-assessed.

This control maps to CIS 4.3 and supports ISO/IEC 27001:2022 controls A.8.5 and A.8.9.

1.11.3 Deploy and Manage Firewalls on Enterprise Devices

Operators must implement firewall controls to manage incoming and outgoing traffic and reduce unauthorized network exposure.

Implementation Guidance:

- Install and configure host-based firewalls on all supported servers.
- Enforce endpoint firewalls with default-deny rules and allow-listing policies.
- Use operating system firewalls or third-party firewall agents.
- Review, approve, and document all rule changes, including exceptions.
- **Gaming-specific consideration:** Firewall rules must support authorized gaming traffic while preventing exposure to unnecessary services or external threats.

This control maps to CIS 4.4 and 4.5 and supports ISO/IEC 27001:2022 controls A.6.7 and A.8.1.

1.11.4 Use Secure Management Protocols for System Administration

Administrative interfaces must be protected using encrypted and authenticated protocols to prevent interception and misuse.

Implementation Guidance:

- Require the use of secure protocols such as SSH, SFTP, and HTTPS for all administrative and configuration activities.
- Disable insecure protocols such as Telnet, HTTP, and FTP unless explicitly required and risk-justified.
- Where possible, manage configurations using version-controlled scripts and infrastructure-as-code (IaC) methods.
- **Gaming-specific consideration:** Collaborate with vendors of gaming-specific hardware to ensure remote management interfaces are securely configured and monitored.

This control maps to CIS 4.6. There is no direct ISO/IEC 27001 mapping, but it is considered foundational for secure systems management.

1.11.5 Disable or Secure Default Accounts on All Systems

Default accounts present a significant security risk if left unchanged. Operators must ensure that such accounts are either secured or removed entirely.

Implementation Guidance:

- Disable or rename default accounts on all systems, applications, and devices.
- Change all default passwords upon deployment.
- Maintain a list of default accounts and document justifications for any retained accounts, including compensating controls.
- **Gaming-specific consideration:** Work closely with vendors to securely manage embedded default accounts in proprietary gaming devices and platforms.

This control maps to CIS 4.7 and supports ISO/IEC 27001:2022 controls A.8.2 and A.8.9.

1.12 Manage User, Administrator, and Privileged Accounts

Effective account management reduces the risk of unauthorized access, privilege misuse, and insider threats. Operators must maintain strict control over account lifecycle, enforce strong password practices, and apply separation of duties. These controls align with **CIS Control 5** and support **ISO/IEC 27001:2022** controls A.5.15, A.5.16, A.5.17, and A.8.2.

1.12.1 Maintain an Inventory of All Accounts

Operators must maintain a complete and up-to-date inventory of all user, service, and administrative accounts across their environment.

Implementation Guidance:

- Document and track:
    - Standard user accounts
    - Privileged administrative accounts
    - System/service accounts used for automation and integrations
- For each account, record:
    - Full name and department
    - Username
    - Account creation and deactivation dates
- Conduct quarterly reviews to ensure all active accounts are valid, assigned to current staff, and necessary.
- **Gaming-specific consideration:** Include role-specific account types such as cage operators, surveillance users, and gaming floor supervisors.

This control maps to CIS 5.1 and supports ISO/IEC 27001:2022 control A.5.16.

1.12.2 Enforce Strong and Unique Passwords

All accounts must use passwords that meet defined strength criteria, and shared or default passwords must be strictly prohibited.

Implementation Guidance:

- Set password complexity based on authentication method:
    - 8-character minimum for accounts protected by multi-factor authentication (MFA)
    - 14-character minimum for accounts without MFA
- Require passwords to be unique across all systems and accounts.
- Encourage or require password managers to support unique credential storage.
- **Gaming-specific consideration:** Evaluate the operational impact of frequent logins for gaming floor staff; apply risk-adjusted controls if needed (e.g., session timeouts instead of short password expirations).

This control maps to CIS 5.2 and supports ISO/IEC 27001:2022 control A.5.17.

1.12.3 Disable Dormant Accounts

Inactive accounts represent a significant risk if left unmonitored. Operators must have a policy to identify and deactivate dormant accounts promptly.

Implementation Guidance:

- Implement automated inactivity monitoring where technically feasible.
- Disable accounts after 45 days of non-use.
- Retain audit logs and document procedures for reactivating accounts when necessary.
- **Gaming-specific consideration:** Consider extended retention or alternative handling for seasonal staff accounts with limited, recurring assignments.

This control maps to CIS 5.3. There is no direct ISO/IEC 27001 mapping, but it is a core element of good account lifecycle management.

1.12.4 Manage Privileged Accounts Separately

Privileged access must be restricted to dedicated administrative accounts and used only for elevated functions.

Implementation Guidance:

- Separate administrative accounts from users' standard business accounts.
- Prevent privileged accounts from accessing non-administrative resources (e.g., web browsing, email).
- Require general activities (e.g., email, document editing) to be performed on non-privileged accounts.
- **Gaming-specific consideration:** Apply strict role separation for administrative access to gaming software and system configurations, ensuring audit logging and access control reviews.

This control maps to CIS 5.4 and supports ISO/IEC 27001:2022 controls A.5.15 and A.8.2.

1.13 Control and Monitor User Access to Systems and Data

Controlling who can access systems and data—and under what conditions—is a core principle of cybersecurity. Operators must enforce access governance policies that support accountability, reduce insider risk, and comply with gaming regulations. These controls align with **CIS Control 6** and support **ISO/IEC 27001:2022** controls A.5.15, A.5.16, A.5.18, A.6.5, A.6.7, and A.8.2.

1.13.1 Define a Formal Access Granting Process

Operators must implement a documented and auditable process for provisioning user access to enterprise systems.

Implementation Guidance:

- Use automated provisioning systems wherever technically feasible.
- Require written or system-based manager approval for all access requests.
- Maintain documentation for access assignments linked to:
    - Employee onboarding
    - Internal role changes
    - Temporary assignments or third-party engagements
- Clearly define access roles based on job functions.
- **Gaming-specific consideration:** Incorporate employee gaming license status into the access provisioning workflow to ensure regulatory compliance.

This control maps to CIS 6.1 and supports ISO/IEC 27001:2022 controls A.5.15, A.5.16, and A.5.18.

1.13.2 Revoke Access Promptly Upon Role Change or Termination

Operators must ensure user access is revoked immediately following employee departure, contract completion, or job function change.

Implementation Guidance:

- Trigger automatic account disablement upon HR-initiated termination or transfer.
- Send notifications to IT or system administrators when offboarding actions occur.

- Retain audit logs by disabling accounts instead of deleting them.
- Ensure processes are enforced consistently across on-premise and cloud-based systems.
- **Gaming-specific consideration:** Align account revocation with license status changes and other regulatory requirements.

This control maps to CIS 6.2 and supports ISO/IEC 27001:2022 controls A.5.16, A.5.18, and A.6.5.

1.13.3 Enforce Multi-Factor Authentication (MFA)

Multi-factor authentication must be used to strengthen identity verification for sensitive systems, remote access, and administrative functions.

Implementation Guidance:

- Require MFA for:
  - All internet-facing or externally accessible applications and portals
  - Remote VPN, RDP, or similar access methods
  - Administrative access to core gaming systems and infrastructure
- Acceptable authentication methods include:
  - Time-based one-time password (TOTP) authenticator applications
  - Hardware security tokens (FIDO2/WebAuthn compliant)
  - Biometric identifiers (e.g., facial recognition, fingerprint scanning)
- **Gaming-specific consideration:** Select MFA solutions that do not interfere with emergency response procedures or operational uptime of critical systems.

This control maps to CIS 6.3, 6.4, and 6.5 and supports ISO/IEC 27001:2022 controls A.5.15, A.6.7, and A.8.2.

1.14 Identify, Remediate, and Patch Vulnerabilities

Unpatched vulnerabilities are among the most common attack vectors in cyber incidents. CGA-licensed operators must implement vulnerability and patch management processes that reduce exposure to known threats. These controls align with **CIS Control 7** and support **ISO/IEC 27001:2022** control A.8.8 (Management of Technical Vulnerabilities).

1.14.1 Establish a Vulnerability Management Program

Operators must maintain a documented, risk-based approach to identifying, prioritizing, and remediating vulnerabilities across enterprise assets.

Implementation Guidance:

- Develop a formal vulnerability management policy that includes:
    - Asset discovery and classification
    - Vulnerability scanning schedules
    - Risk evaluation criteria
    - Time-bound remediation guidelines
- Conduct vulnerability scans at least monthly, or more frequently for critical systems.
- Use automated vulnerability scanning tools to detect issues across:
    - Operating systems
    - Network infrastructure
    - Web applications
    - Third-party software
- Integrate threat intelligence and vendor advisories to adjust prioritization.
- Perform an annual review of the program or following major environmental changes.
- **Gaming-specific consideration:** Include sources specific to gaming environments, such as vendor notifications for slot systems, player tracking platforms, and RNG firmware.

This control maps to CIS 7.1 and 7.2 and supports ISO/IEC 27001:2022 control A.8.8.

1.14.2 Implement a Structured Patch Management Process

Operators must maintain an automated and repeatable process for applying patches and updates to enterprise systems.

Implementation Guidance:

- Apply patches for operating systems, software, and firmware at least monthly.
- Test updates in a staging or non-production environment before deployment.
- Automate patch deployment where feasible using endpoint or systems management tools.
- Maintain documentation of patch approvals, deployment results, and exceptions.
- Coordinate with vendors to understand compatibility impacts on critical gaming systems.
- Schedule updates to avoid peak operating hours or service disruptions.
- **Gaming-specific consideration:** Plan patch cycles around gaming floor operations and regulatory audit periods to avoid system downtime or player impact.

This control maps to CIS 7.3 and 7.4 and supports ISO/IEC 27001:2022 control A.8.8.

1.15 Monitor and Safeguard System Activity Through Logging

Comprehensive logging is essential for detecting incidents, tracing unauthorized actions, and supporting compliance. Operators must ensure that audit logs are generated, collected, stored securely, and reviewed regularly. These controls align with **CIS Control 8** and support **ISO/IEC 27001:2022** controls A.8.15 and A.8.6.

1.15.1 Establish an Audit Log Management Process

Operators must define, implement, and maintain a documented process for managing audit logs across all critical systems.

Implementation Guidance:

- Identify and document logging requirements by system type and business function.
- Define minimum retention periods based on regulatory or business requirements.
- Include procedures for:
    - Centralized log collection
    - Periodic log reviews for anomalies
    - Log archival and secure storage
- Ensure audit log access is restricted to authorized personnel.
- **Review frequency:** Annually, or when significant changes to systems or operations occur.
- **Gaming-specific consideration:** Include logging of critical events such as player activity, transaction records, payout validation, and surveillance integrations.

This control maps to CIS 8.1 and supports ISO/IEC 27001:2022 control A.8.15.

1.15.2 Enable and Secure Audit Log Collection and Storage

Operators must ensure audit logs are consistently generated and stored in a manner that preserves integrity and availability.

Implementation Guidance:

- Enable audit logging on all enterprise assets, including endpoints, servers, applications, and security tools.
- Configure systems to forward logs to centralized, tamper-resistant storage (e.g., SIEM platforms).
- Ensure log storage meets defined retention and access control requirements.
- Monitor log integrity using cryptographic hashing or write-once storage mechanisms.
- **Gaming-specific consideration:** Critical gaming logs must include:
    - Gameplay and betting transactions
    - Jackpot wins and high-value events
    - Cash and credit movement logs
    - Administrative access and system configuration changes

This control maps to CIS 8.2 and 8.3 and supports ISO/IEC 27001:2022 controls A.8.15 and A.8.6.

1.16 Protect Users from Web and Email Threats

Internet browsers and email systems are frequent delivery methods for malware and phishing. Operators must reduce risk by restricting usage to supported software and filtering known threats. These controls align with **CIS Control 9** and support **ISO/IEC 27001:2022** controls A.8.1 and A.8.23.

1.16.1 Use Supported Browsers and Email Clients

Operators must ensure that only fully supported and up-to-date browsers and email clients are deployed on enterprise systems.

Implementation Guidance:

- Maintain only current versions of browsers and email applications.
- Apply automatic updates to address emerging security vulnerabilities.
- Remove unsupported software promptly.
- **Gaming-specific consideration:** Verify that updates remain compatible with web-based gaming platforms and system administration portals.

This control maps to CIS 9.1 and supports ISO/IEC 27001:2022 control A.8.1.

1.16.2 Apply DNS Filtering to Block Malicious Domains

DNS filtering must be used to block access to known malicious or unauthorized domains.

Implementation Guidance:

- Deploy DNS filtering agents across all endpoints—both on-premises and remote.
- Integrate threat intelligence feeds to maintain updated blocklists.
- Monitor DNS activity for anomalies.
- **Gaming-specific consideration:** Ensure DNS filtering does not interfere with connectivity to legitimate gaming services, systems, or cloud environments.

This control maps to CIS 9.2 and supports ISO/IEC 27001:2022 control A.8.23.

1.17 Defend Against Malware and Unauthorized Removable Media

Operators must deploy and maintain appropriate anti-malware defenses and limit the risk posed by removable storage devices. These controls align with **CIS Control 10** and support **ISO/IEC 27001:2022** controls A.8.1 and A.8.7.

1.17.1 Deploy Anti-Malware Tools Across All Systems

Operators must ensure that all systems are protected by up-to-date, centrally managed anti-malware tools.

Implementation Guidance:

- Install anti-malware software on all supported endpoints and servers.
- Configure for automatic signature and engine updates.
- Enforce regular scanning of devices and file activity.
- **Gaming-specific consideration:** Verify vendor compatibility with gaming systems and platforms, and confirm that protection tools do not introduce performance degradation.

This control maps to CIS 10.1 and 10.2 and supports ISO/IEC 27001:2022 controls A.8.1 and A.8.7.

1.17.2 Disable Auto-Execution from Removable Media

Where removable media is used in the gaming environment, licensees shall implement controls to to prevent the automatic execution of potentially harmful content.

Implementation Guidance:

- Disable autorun and autoplay functionality for USB and other removable devices.
- Define procedures and technical controls for authorizing removable media usage.
- Require scanning or validation before data transfer from external storage.
- **Gaming-specific consideration:** Give particular attention to exposed ports on gaming kiosks, terminals, and administrative workstations.

This control maps to CIS 10.3. While it has no direct ISO/IEC 27001 mapping, it is considered a critical baseline safeguard.

1.18 Ensure Recoverability of Critical Data and Systems

Operators must be prepared to recover data and restore systems in the event of a cyber incident, hardware failure, or data corruption. A structured backup and recovery strategy is vital to business continuity and regulatory compliance. These controls align with **CIS Control 11** and support **ISO/IEC 27001:2022** control A.8.13.

1.18.1 Document the Data Recovery Strategy

Operators must define a comprehensive data recovery process, including backup planning, priority systems, and data integrity assurance.

Implementation Guidance:

- Identify which data types and systems require backup, with emphasis on critical gaming operations.
- Document the procedures for data backup, storage, and recovery testing.
- Include recovery point objectives (RPOs) and recovery time objectives (RTOs).
- Define security measures for backup data, including access restrictions and encryption.
- **Review frequency:** Annually or when major systems or regulations change.
- **Gaming-specific consideration:** Ensure that gaming transaction data, configuration files, and player activity logs are included and protected in backups.

This control maps to CIS 11.1 and supports ISO/IEC 27001:2022 control A.8.13.

1.18.2 Automate Backups and Enforce Isolation and Protection

Operators must perform automated backups and ensure that backup data is adequately protected, isolated from production systems, and readily restorable.

Implementation Guidance:

- Automate backups for systems handling sensitive or regulated data.
- Perform backups at a minimum weekly frequency; increase frequency for high-risk or high-volume systems.
- Use offline, off-site, or immutable storage where feasible to prevent tampering or ransomware-related corruption.

- Apply the same access controls and security protections to backup data as to the original production data.
- **Gaming-specific consideration:** Gaming transaction logs and financial data may require daily or real-time backups to meet regulatory retention requirements and avoid data loss.

This control maps to CIS 11.2, 11.3, and 11.4 and supports ISO/IEC 27001:2022 control A.8.13.

1.19 Keep Network Infrastructure Secure and Updated

Operators must ensure all network devices are operating on current, supported firmware and software to maintain a strong security baseline. This control aligns with **CIS Control 12**.

1.19.1 Regularly Update Network Infrastructure

Implementation Guidance:

- Maintain an inventory of network infrastructure (e.g., routers, switches, firewalls).
- Review firmware and software version status at least monthly.
- Apply updates or patches based on vendor advisories and risk impact.
- Use supported versions and avoid end-of-life products in live environments.
- **Gaming-specific consideration:** Coordinate updates with gaming system maintenance windows and ensure support continuity with third-party vendors.

This control maps to CIS 12.1. There is no direct ISO/IEC 27001 mapping, but this is a foundational IT security practice.

1.20 Educate Employees and Stakeholders on Cybersecurity

Security awareness among staff is essential for preventing social engineering attacks and ensuring secure practices are followed throughout operations. These controls align with **CIS Control 14** and support **ISO/IEC 27001:2022** control A.6.3.

1.20.1 Conduct a Security Awareness Program

Operators must deliver security awareness training to all personnel to promote safe behaviors and understanding of their responsibilities.

Implementation Guidance:

- Provide baseline cybersecurity training to all employees during onboarding.
- Repeat training annually or in response to policy or threat changes.
- Training should cover:
    - Secure system and asset use
    - Regulatory obligations and compliance expectations
    - Gaming-specific threats and use cases
- **Gaming-specific consideration:** Include modules on gaming fraud, data privacy, and social engineering techniques targeting casinos and online operators.

This control maps to CIS 14.1 and supports ISO/IEC 27001:2022 control A.6.3.

1.20.2 Deliver Specialized Role-Based Security Training

Operators must provide additional training targeted to specific roles and responsibilities that pose elevated risk.

Implementation Guidance:

- Offer training in the following areas:
    - **Social engineering defense (CIS 14.2):** Recognize phishing, business email compromise (BEC), and pretexting
    - **Authentication practices (CIS 14.3):** Password hygiene, MFA use, credential protection
    - **Data handling (CIS 14.4):** Secure storage, transfer, archival, and destruction

- **Unintentional exposure (CIS 14.5):** Preventing accidental data loss or misdelivery
- **Incident awareness (CIS 14.6):** How to detect and report potential incidents
- **Security updates (CIS 14.7):** Reporting missing or failed software patches
- **Network safety (CIS 14.8):** Risks of using insecure networks, especially remote access

- **Gaming-specific consideration:** Training should include simulated exercises involving gaming-specific threats and compliance-driven procedures.

These controls map to CIS 14.2–14.8. Most align indirectly with ISO/IEC 27001:2022 A.6.3, except CIS 14.3 (authentication practices), which is foundational but not directly mapped.

1.21 Track and Manage Third-Party Service Providers

Operators rely on various external vendors and service providers that may introduce cybersecurity and regulatory risks. Effective oversight is essential. This control aligns with **CIS Control 15** and supports **ISO/IEC 27001:2022** control A.5.19.

Where a licensee relies on third-party platforms, hosting providers, game suppliers, or managed security services, the licensee remains **fully responsible under the LOK** for compliance with these requirements. Contractual delegation does not transfer regulatory accountability.

Gaming-specific consideration: Operators must specifically identify and manage the following categories of third-party providers as part of their service provider inventory:

- **Game content aggregators** that supply or distribute game titles from multiple B2B studios
- **Sports data feed providers** that supply live results, odds, event data, or statistics used in determining wager outcomes
- **B2B platform providers** that supply Remote Gaming Servers, game engines, or player management systems

For each such provider, the operator must document: the nature and scope of data exchanged, contractual security and integrity obligations, certification or audit status, and procedures for detecting and responding to feed manipulation, data integrity failures, or service disruptions.

1.21.1 Maintain a Service Provider Inventory

Operators must maintain a complete, current record of all service providers and vendors involved in delivering technical or operational support.

Implementation Guidance:

- List all active service providers, including:
    - Gaming software vendors
    - Cloud hosting and infrastructure providers
    - Payment processors
    - Security monitoring and support services
- For each provider, document:
    - Contract type and scope of services
    - Internal contact/owner
    - Classification of data or systems accessed

- **Review frequency:** Annually or when changes to providers or services occur.

This control maps to CIS 15.1 and supports ISO/IEC 27001:2022 control A.5.19.

1.21.2 Integrity of Externally Supplied Game Content and Data Feeds

Where operators rely on third-party providers for game content, sports data feeds, or aggregated results that influence wager outcomes, the following controls must be implemented:

- **Source authentication:** All data feeds must be received over authenticated and encrypted channels. API connections must use mutual TLS or equivalent authentication mechanisms.
- **Data integrity validation:** Operators must implement integrity checks on received data, such as cryptographic signatures, hash verification, or message authentication codes, to detect tampering or corruption in transit.
- **Feed monitoring and anomaly detection:** Operators must monitor feed availability, latency, and data consistency. Procedures must be in place to detect and respond to unexpected feed interruptions, result discrepancies, or anomalous data patterns.
- **Failover and suspension procedures:** Operators must define and document procedures for suspending affected wagering markets or game offerings when feed integrity cannot be assured, and for resuming operations only after integrity is re-established.
- **Contractual assurances:** Agreements with feed providers and aggregators must include requirements for security controls, incident notification, data integrity guarantees, and the right to audit or request evidence of compliance.

Gaming-specific consideration: Sports betting operators must pay particular attention to the integrity of live event data feeds, as manipulation of this data can directly affect wager outcomes. Operators must ensure their feed providers can demonstrate adequate controls against data manipulation at source.

B2B certification monitoring: For B2C operators relying on licensed B2B providers, the third-party management programme must include: periodic verification of the B2B provider's certification status (at minimum annually), contractual right-to-audit or right-to-request-evidence provisions, contractual requirements for the B2B provider to notify the B2C operator of certification lapses or scope changes, and documented escalation procedures in the event of a certification lapse, including suspension of affected game content and notification to the CGA.

1.22 Prepare for and Respond to Security Incidents

Operators must develop and maintain the capacity to detect, report, and respond to cybersecurity incidents quickly and effectively. These controls align with **CIS Control 17** and support **ISO/IEC 27001:2022** controls A.5.5, A.5.6, A.5.24, and A.6.8.

1.22.1 Assign Incident Response Roles and Responsibilities

Operators must formally designate personnel responsible for coordinating incident detection, response, and communication.

Implementation Guidance:

- Appoint a primary and backup incident response manager.
- Define roles for IT, security, compliance, legal, and public relations.
- Use internal staff or contracted incident response services—but maintain internal oversight.
- **Review frequency:** Annually or during significant organizational or threat landscape changes.
- **Gaming-specific consideration:** Include roles for handling gaming-specific scenarios such as payout manipulation or integrity violations.

This control maps to CIS 17.1 and supports ISO/IEC 27001:2022 control A.5.24.

1.22.2 Maintain an Up-to-Date Incident Contact Directory

Operators must maintain and review contact lists for reporting and escalating incidents internally and externally.

Implementation Guidance:

- Include internal stakeholders, law enforcement, regulatory bodies, and insurance providers.
- Update contact details regularly.
- Incident response plans should specify:
    - Notification timelines (e.g., 24–72 hours)
    - Required information for reporting
    - Coordination with forensics and legal counsel

- **Gaming-specific consideration:** Ensure inclusion of gaming regulators, financial intelligence units, and vendors responsible for critical infrastructure.

This control maps to CIS 17.2 and supports ISO/IEC 27001:2022 controls A.5.5, A.5.6, and A.5.24.

1.22.3 Define and Document an Incident Reporting Process

Operators must have a well-documented process for internal and external incident reporting.

Implementation Guidance:

- Define what constitutes a reportable incident.
- Specify escalation criteria and reporting channels.
- Make policies available to all employees and service providers.
- Maintain templates or forms to streamline reporting.
- **Gaming-specific consideration:** Clearly define CGA-required reporting timeframes (e.g., 24 hours for serious incidents) and supporting documentation needed.

Mandatory CGA Notification (pursuant to LOK Article 5): Licensees shall notify the Curaçao Gaming Authority **without undue delay**, and in any event within 24 hours, of any security incident that:

- compromises gaming integrity;
- affects player funds or personal data; or
- may impact regulatory reporting, system availability, or game fairness.

Failure to notify constitutes a breach of license conditions under the LOK.

This control maps to CIS 17.3 and supports ISO/IEC 27001:2022 control A.6.8.

1.23 Physical Security Controls for Gaming Environments

Operators must implement physical and environmental controls to protect gaming infrastructure, sensitive areas, and equipment from unauthorized access, tampering, and environmental threats.

Implementation Guidance:

- Restrict physical access to secure areas (e.g., server rooms, vaults, surveillance control rooms) using access cards, biometric scanners, or guards.
- Maintain entry logs and conduct periodic reviews.
- Deploy surveillance systems (e.g., CCTV) and ensure coverage of critical locations.
- Install environmental safeguards including climate controls, smoke detectors, and UPS systems.
- Enforce clean desk/clear screen policies.
- Secure equipment stored or used off-premises.

Gaming-specific consideration: Physical security must include protections for slot machines, payout systems, surveillance infrastructure, and regulated storage areas.

This control supports ISO/IEC 27001:2022 controls A.7.1–A.7.14.

1.24 Human Resource Security Controls

Operators must manage security responsibilities throughout the employment lifecycle to reduce personnel-related risks.

Implementation Guidance:

- Conduct background checks for new hires in critical or sensitive roles.
- Include confidentiality obligations in employment agreements.
- Require employees to acknowledge security responsibilities during onboarding.
- Enforce disciplinary action for non-compliance.
- Reclaim company assets and disable accounts promptly during offboarding.

Gaming-specific consideration: Enhanced screening should be applied to employees managing financial systems, player data, or gaming system oversight.

This control supports ISO/IEC 27001:2022 controls A.5.11, A.6.1–A.6.6.

1.25 Legal and Regulatory Compliance Measures

Operators must identify and comply with all legal, regulatory, and contractual information security obligations.

Implementation Guidance:

- Maintain a register of applicable laws and obligations (e.g., privacy, AML/CFT, licensing).
- Assign responsibility for tracking legal and regulatory changes.
- Implement controls to safeguard personal data and intellectual property.
- Align data retention and disposal procedures with legal requirements.

Gaming-specific consideration: Must support CGA reporting requirements, data retention laws, and demonstrate compliance during inspections.

This control supports ISO/IEC 27001:2022 controls A.5.31–A.5.34.

1.26 Business Continuity and Operational Assurance

Operators must ensure that information security is maintained during disruptions and that critical systems remain available.

Implementation Guidance:

- Integrate information security into business continuity and disaster recovery plans.
- Test and review continuity plans annually or when significant changes occur.
- Implement failover and redundancy for mission-critical gaming systems.
- Include change management risk assessments.
- Use data masking and controlled access during audits and test activities.

Gaming-specific consideration: Transaction processing systems, real-time reporting tools, and regulatory interfaces must have defined fallback procedures.

This control supports ISO/IEC 27001:2022 controls A.5.29, A.8.14, A.8.32–A.8.34.

1.27 Security Governance and Oversight

Operators must establish governance structures and procedures to ensure the information security program remains effective, compliant, and continuously improving.

Implementation Guidance:

- Assign executive responsibility for information security oversight.
- Conduct independent reviews of policy compliance and control effectiveness.
- Maintain documented operational procedures for key activities (e.g., backups, user access, audits).
- Monitor implementation of corrective actions.
- Review and approve policies and standards on a recurring schedule.

Gaming-specific consideration: Must ensure game audit data and compliance logs are governed with defined ownership and oversight.

This control supports ISO/IEC 27001:2022 controls A.5.4, A.5.35–A.5.37.

1.28 Cryptographic Controls and Data Masking

Operators must use cryptographic protections and data masking to safeguard sensitive gaming, player, and financial data.

Implementation Guidance:

- Encrypt sensitive data at rest and in transit using secure, industry-standard protocols.
- Apply data masking techniques in development, QA, or analytics environments.
- Establish a key management program covering key generation, storage, use, and retirement.
- Maintain a register of cryptographic controls and any approved exceptions.

Gaming-specific consideration: RNG data, player credentials, and jackpot triggers must be encrypted and masked appropriately.

This control supports ISO/IEC 27001:2022 controls A.8.11, A.8.24.

Relationship to International Standards

The Curaçao Gaming Authority (CGA) has based these security guidelines on the **Center for Internet Security (CIS) Controls Implementation Group 1 (IG1)**. These controls offer a prioritized, risk-based cybersecurity baseline for organizations with limited security resources. However, due to the sensitive nature of gaming operations, CGA recommends that operators **progress toward Implementation Group 2 (IG2)** within 24–36 months.

This section outlines how the CIS-based framework aligns with global information security standards and industry-specific regulatory models to support both **local compliance** and **international recognition**.

1.29 ISO/IEC 27001:2022 Alignment

These guidelines are structured to help gaming operators **align with ISO/IEC 27001:2022**, the globally recognized standard for information security management.

- **Mapped Controls:**
  Where a CIS IG1 control aligns with an ISO 27001 Annex A control, this relationship is clearly indicated. This helps operators understand how implementing technical controls also contributes to broader governance and certification objectives.

- **Unmapped Controls:**
  Some CIS controls do not map directly to ISO 27001. These are marked as **[No ISO 27001 Mapping]**, but are retained due to their value in building a strong foundational security posture. Examples include weekly unauthorized asset review or DNS filtering.

- **Management System Integration:**
  All controls in this guideline can be incorporated into an ISO 27001 Information Security Management System (ISMS). Operators pursuing ISO certification can use this document as a **practical implementation guide** to meet both technical and management system requirements.

In addition, certain ISO/IEC 27001 requirements—particularly in areas such as physical security, legal compliance, human resource screening, and business continuity—are not addressed by CIS Controls but are essential for comprehensive coverage in a regulated industry like gaming. These include:

- **Physical and Environmental Security** (e.g., facility access, equipment protection, off-premises security)

- **Legal and Regulatory Compliance** (e.g., protection of personal data, contract compliance, licensing obligations)

- **Human Resource Security** (e.g., background checks, NDAs, disciplinary measures)
- **Operational Resilience** (e.g., security during disruption, change management)

These ISO requirements will be included as part of the CGA baseline and must be addressed by all CGA licensees to ensure full sectoral coverage and alignment with the minimum security expectations.

1.30 CIS Controls and Gaming-Specific Risk Posture

While IG1 provides the **minimum security requirements**, gaming operators handle sensitive player data, financial transactions, and face elevated regulatory scrutiny. These characteristics more closely match the threat model for **CIS Implementation Group 2 (IG2)**.

CGA Recommendation:
All CGA licensees are encouraged to **adopt IG2 controls as a strategic objective**. IG2 introduces additional safeguards such as centralized logging, automated asset tracking, and stronger data protection practices—making it more suitable for both online and land-based operations.

CGA will provide future guidance on IG2 expectations and phased progression planning to help operators elevate their cybersecurity maturity.

1.31 Gaming Industry Standards Integration

To ensure relevance within the gaming sector, this framework is aligned with **industry-specific security and regulatory models**, enabling smoother compliance across jurisdictions and audit scenarios.

- **Gaming Security Framework Compatibility:**
  These guidelines complement **CGA-recognized gaming security frameworks**, which is widely used for independent gaming system audits and covers integrity, traceability, and system access controls.
- **IGSA Standards Alignment (Land-Based Operations):**
  Where applicable, the controls support technical alignment with the **International Gaming Standards Association (IGSA)**, particularly in areas of secure device management, communication protocols, and system interoperability.

Additional Considerations for Gaming Operations

The successful implementation of cybersecurity controls in the gaming industry requires consideration of operational realities, technical compatibility, and regulatory obligations. This section outlines key factors that must be taken into account to ensure that security enhancements are both effective and sustainable across diverse operator environments.

1.32 Performance Impact Considerations

Cybersecurity measures must be implemented in a manner that safeguards operations without compromising the core functions of gaming systems. Operators must ensure that controls are applied in a way that **preserves system integrity, responsiveness, and compliance capabilities**.

Specifically, security controls must not adversely affect:

- The **performance and availability** of gaming platforms and infrastructure
- The **player experience**, including game fairness, reliability, and uptime
- **Real-time processing** of transactions, wagers, or gameplay outcomes
- **Timely regulatory reporting**, data collection, and audit functions

Note: Where technical safeguards may introduce latency or operational overhead, compensating controls or alternate configurations should be considered to maintain continuity of gaming services.

1.33 Integration with Gaming Industry Standards

These guidelines are designed to complement existing **gaming industry standards and regulatory requirements**, and should not be implemented in isolation. Operators must ensure that their security controls are also aligned with:

- The **CGA-recognized gaming security frameworks**
- Applicable **International Gaming Standards Association (IGSA)** specifications
- **Vendor-specific security requirements** for gaming platforms, devices, and software
- Other relevant **jurisdictional regulations** and technical compliance mandates

Integration with these standards enhances audit readiness, promotes consistency across technical environments, and supports multi-jurisdictional compliance efforts.

1.34 Scalability Across Operator Types

The framework is intentionally designed to be **scalable and adaptable** across the full spectrum of CGA licensees, regardless of size, structure, or delivery model. The control expectations and implementation guidance apply equally to:

- **Small-scale, single-site land-based operations**
- **Large, multi-site gaming enterprises** with complex infrastructures
- **Online-only operators**, including B2C and B2B platforms
- **Hybrid operators** combining both land-based and online services

Enforcement and Penalties

The Curaçao Gaming Authority (CGA) maintains the right and responsibility to enforce these guidelines to ensure the integrity, security, and trustworthiness of CGA licensees. Operators must treat these requirements as binding conditions of licensure.

Enforcement actions described in this section are exercised under the CGA's statutory powers pursuant to the LOK and may be applied **independently or cumulatively** with other regulatory measures.

1.35 Compliance Monitoring

CGA will actively monitor operator compliance using a combination of assessments, tools, and validation methods designed to ensure transparency and accountability.

Compliance oversight will include:

- **Scheduled system reviews**, utilizing standardized assessment frameworks aligned with CIS Controls and CGA policies
- **Incident analysis and trend monitoring**, to identify systemic weaknesses or emerging threats across operators
- **Independent third-party audits**, conducted by CGA-approved assessors with domain-specific expertise
- **Annual self-assessment submissions**, validated by CGA through spot-checks, document sampling, and configuration testing

CGA monitoring tools and capabilities may include:

- **Remote Security Assessments** – Use of network scanning tools (e.g., Nmap, Nessus) to evaluate external attack surfaces and verify patch status
- **Automated Compliance Verification** – Execution of scripts and configurations checks to validate asset inventory, password settings, MFA enforcement, and other basic requirements
- **Incident Pattern Analysis** – Centralized correlation of incident reports to detect recurring security issues, supply chain vulnerabilities, or process failures across multiple licensees

- **Policy and Document Review** – Use of standardized review checklists to evaluate operator policies, procedures, and incident response plans for completeness and applicability
- **On-Site Inspections** – Physical verification of implemented controls, particularly for land-based operations or in response to high-risk indicators or reported deficiencies

Note: CGA reserves the right to conduct **unannounced assessments** or request immediate remediation where urgent security gaps or data protection violations are identified.

1.36 Consequences of Non-Compliance

Failure to comply with these guidelines may result in **regulatory action** in accordance with CGA's enforcement authority (based on LOK and LCC) and applicable licensing conditions.

Depending on the nature and severity of the non-compliance, the following penalties may apply:

- **Formal written warnings**, with a required corrective action timeline
- **Issuance of compliance orders** mandating remediation of specific deficiencies
- **Administrative financial penalties**, scaled to the risk level and scope of violation
- **Temporary or permanent suspension of license** in cases of severe or repeated violations
- **Imposition of enhanced security obligations**, including additional audits, external security oversight, or infrastructure upgrades

Operators are expected to cooperate fully with CGA investigations and remediation timelines. Failure to do so may result in escalation of enforcement measures.

Appendix A: Definitions and Glossary

A.1 Gaming-Specific Terms

Anti-Money Laundering (AML): Policies, procedures, and controls designed to prevent the use of gaming operations to disguise the origins of illegally obtained funds.

Cage Operations: The financial center of a gaming establishment responsible for currency exchange, credit transactions, and cash handling procedures.

Cashless Gaming System: Technology that allows players to conduct gaming transactions without physical currency, typically using cards, mobile devices, or digital wallets.

Data Feed Integrity: The assurance that data received from an external source has not been altered, corrupted, or manipulated during transmission or processing, and accurately reflects the data as sent by the originating source.

CGA Licensee: Any entity holding a valid license issued by the Curaçao Gaming Authority under the LOK or LCC, including Business-to-Consumer (B2C) gaming operators, Business-to-Business (B2B) gaming technology providers, land-based gaming establishments, and hybrid operators. Where this document refers to "licensees" or "operators," it applies to all such entities unless a specific distinction is stated.

Game Content Aggregator: A third-party entity that integrates, distributes, or provides access to game content from multiple B2B providers through a unified platform or API, enabling B2C operators to offer a wider range of games without direct integration with each game studio.

Gaming Device: Any electronic, electromechanical, or mechanical contrivance designed for gaming purposes, including but not limited to slot machines, electronic table games, and lottery terminals.

Gaming Floor: The designated area within a gaming establishment where gaming activities are conducted and players engage with gaming devices or table games.

Gaming Management System: The central computer system that monitors, controls, and reports on gaming device operations and player activity.

Gaming System: The complete technological infrastructure supporting gaming operations, including gaming devices, management systems, player tracking, and associated networks.

Gaming Transaction: Any electronic or recorded exchange involving gaming credits, cash, or player accounts, including wagers, payouts, deposits, and withdrawals.

Know Your Customer (KYC): Procedures to verify the identity of players and assess their suitability for gaming services, including age verification and risk assessment.

Player Account: An electronic record maintaining a player's gaming history, credits, personal information, and transaction records.

Player Data: Any information relating to an identified or identifiable player, including personal details, gaming behavior, financial transactions, and preferences.

Player Management System: Technology platform that tracks player activity, manages player accounts, and supports customer relationship management and responsible gaming programs.

Player Tracking System: Technology that monitors and records individual player gaming activity across multiple gaming devices and sessions.

Random Number Generator (RNG): Hardware or software algorithm that produces sequences of numbers or symbols that cannot be reasonably predicted better than by random chance.

Responsible Gaming: Policies and practices designed to promote safe gaming behaviors and provide assistance to players who may be experiencing gaming-related problems.

Sports Data Feed: A real-time or near-real-time electronic data service providing sports event information, results, odds, statistics, or other data used by operators to determine the outcome of sports-related wagers.

Table Management System: Electronic system that monitors and records activity at gaming tables, including player tracking, bet monitoring, and dealer performance.

A.2 Technical Security Terms

Access Control List (ACL): A list of permissions attached to an object that specifies which users or system processes are granted access and what operations are allowed.

Administrative Account: A user account with elevated privileges that allow system configuration, user management, and other administrative functions.

Anti-Malware Software: Programs designed to detect, prevent, and remove malicious software including viruses, worms, trojans, and other threats.

Asset Inventory: A comprehensive list of all enterprise assets including hardware, software, and data that require protection and management.

Audit Log: A chronological record of system activities and events that provides an audit trail for security monitoring and compliance purposes.

Authentication: The process of verifying the identity of a user, device, or system before granting access to resources.

Authorization: The process of granting authenticated users permission to access specific resources or perform certain actions.

Backup: A copy of data stored separately from the original to enable recovery in case of data loss, corruption, or system failure.

Configuration Management: The process of maintaining computer systems, servers, and software in a desired, consistent state.

Data Classification: The process of organizing data into categories based on sensitivity, value, and criticality to the organization.

Data Encryption: The process of converting readable data into an encoded format that can only be accessed with the proper decryption key.

Data Loss Prevention (DLP): Technologies and processes designed to detect potential data breaches and prevent sensitive data from leaving the organization.

DNS Filtering: A cybersecurity technique that blocks access to malicious websites by filtering DNS queries.

Dormant Account: A user account that has not been accessed or used for a specified period, typically 45 days or more.

Enterprise Asset: Any hardware, software, or data owned or managed by the organization that supports business operations.

Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Incident Response: The organized approach to addressing and managing the aftermath of a security breach or cyberattack.

Multi-Factor Authentication (MFA): An authentication method that requires two or more verification factors to gain access to a resource.

Network Segmentation: The practice of dividing a computer network into smaller segments to improve security and performance.

Patch Management: The process of managing updates for software applications and technologies.

Penetration Testing: A simulated cyberattack against a computer system to evaluate its security.

Privileged Access: Administrative rights that allow users to perform system-level functions and access sensitive resources.

Risk Assessment: The process of identifying, analyzing, and evaluating cybersecurity risks to organizational assets.

Security Awareness Training: Educational programs designed to help users recognize and respond to cybersecurity threats.

Service Provider: External organizations that provide technology services, support, or resources to the gaming operation.

Software Inventory: A comprehensive list of all software applications installed and licensed within the organization.

Vulnerability: A weakness in a system, application, or network that could be exploited by threats to gain unauthorized access or cause harm.

Vulnerability Management: The cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.

A.3 Regulatory and Compliance Terms

Business Continuity: The capability of an organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Compliance: Adherence to laws, regulations, guidelines, and specifications relevant to gaming operations.

Data Controller: The entity that determines the purposes and means of processing personal data.

Data Processor: The entity that processes personal data on behalf of the data controller.

Data Protection Officer (DPO): An individual responsible for monitoring compliance with data protection regulations and serving as a contact point for data protection authorities.

Data Retention: The policies and procedures governing how long different types of data must be kept and when they can be securely disposed of.

Data Subject: An individual whose personal data is being collected, held, or processed.

Financial Intelligence Unit (FIU): A national center for receiving, analyzing, and disseminating financial intelligence and suspicious transaction reports.

Gaming License: Legal authorization granted by a gaming authority to operate gaming activities within a specific jurisdiction.

Gaming Regulator: Government agency responsible for overseeing and regulating gaming activities within a jurisdiction.

Information Security Management System (ISMS): A systematic approach to managing sensitive company information including people, processes, and IT systems.

Personal Data: Any information relating to an identified or identifiable natural person.

Privacy Impact Assessment (PIA): An evaluation of how a project, system, or program collects, uses, shares, and maintains personally identifiable information.

Regulatory Reporting: The submission of required information to gaming regulators according to specified formats and timeframes.

Regulated Data: Information subject to specific protection requirements under the LOK, LCC, or other applicable legislation within the supervisory remit of the CGA, for the purposes set out therein, including without limitation player personal and financial data, game event outcomes and transaction records, responsible gaming intervention

data, anti-money laundering records, and system audit logs required for regulatory oversight.

Sensitive Data: Information that must be protected from unauthorized access due to regulatory, business, or privacy requirements.

A.4 Abbreviations and Acronyms

AML - Anti-Money Laundering
API - Application Programming Interface
CGA - Curaçao Gaming Authority
CIS - Center for Internet Security
DNS - Domain Name System
DLP - Data Loss Prevention
GDPR - General Data Protection Regulation
GLI - Gaming Laboratories International
GSF - Gaming Security Framework
HTTP/HTTPS - Hypertext Transfer Protocol/Secure
ISMS - Information Security Management System
IoT - Internet of Things
IP - Internet Protocol
ISO - International Organization for Standardization
IT - Information Technology
KYC - Know Your Customer
MFA - Multi-Factor Authentication
NIST - National Institute of Standards and Technology
PCI DSS - Payment Card Industry Data Security Standard
RNG - Random Number Generator
SIEM - Security Information and Event Management
SSH - Secure Shell
SSL/TLS - Secure Sockets Layer/Transport Layer Security
VPN - Virtual Private Network

Appendix B: LOK and LCC Alignment Summary

This annex provides a summary of how the Information Security Control Requirements align with the core security obligations under the Landsverordening op de Kansspelen (LOK) and Landsverordening Casinowezen Curaçao (LCC).

Integrity, security, and reliability of gaming systems

Relevant Sections: 2.1 (Asset Management), 2.3 (Secure Configuration), 2.6 (Vulnerability Management), 2.7 (Logging), 2.10 (Data Recovery), 2.11 (Network Security), 2.18 (Business Continuity), 2.20 (Cryptographic Controls)
Enforcement: Non-compliance may result in license suspension or revocation.

Protection of player data and financial information

Relevant Sections: 2.2 (Data Protection), 2.4 (Account Management), 2.5 (Access Control), 2.17 (Legal Compliance), 2.20 (Cryptographic Controls)
Enforcement: Breaches trigger mandatory reporting; subject to administrative penalties.

Prevention of fraud, manipulation, and unauthorised access

Relevant Sections: 2.4 (Account Management), 2.5 (Access Control), 2.8 (Web/Email Security), 2.9 (Malware Defence), 2.15 (Physical Security), 2.16 (HR Security)
Enforcement: Failures may result in immediate compliance orders and enhanced oversight.

Licensee accountability for third-party systems

Relevant Sections: 2.13 (Third-Party Management), 2.19 (Security Governance)
Enforcement: Contractual delegation does not transfer regulatory accountability under the LOK.

CGA supervisory and enforcement powers

Relevant Sections: 2.14 (Incident Response), Section 5 (Enforcement and Penalties), 1.5 (Compliance Requirements)
Enforcement: Full range of administrative measures including warnings, compliance orders, financial penalties, and license suspension/revocation.