Security Audit: Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document. (sent on a separate email).

Controls assessment checklist

Yes	No	Control
□	☑	Least Privilege
□	☑	Disaster recovery plans
□	☑	Password policies
□	☑	Separation of duties
☑	□	Firewall
□	☑	Intrusion detection system (IDS)
□	☑	Backups
☑	□	Antivirus software
□	☑	Manual monitoring, maintenance, and intervention for legacy systems
□	☑	Encryption
□	☑	Password management system
☑	□	Locks (offices, storefront, warehouse)
☑	□	Closed-circuit television (CCTV) surveillance

☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
□	☑	Only authorized users have access to customers’ credit card information.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
□	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
□	☑	E.U. customers’ data is kept private/secured.
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☑	□	Ensure data is properly classified and inventoried.

☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
□	☑	User access policies are established.
□	☑	Sensitive data (PII/SPII) is confidential/private.
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
□	☑	Data is available to individuals authorized to access it.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional):

Dear IT Manager and Stakeholders,

Outside of the previously exposed checklist, here are my personal conclusions and suggestions.

There is a lot missing from what we could call a secure IT Infrastructure: Network, Data, Assets infrastructure here, and I believe you guys are lucky no government auditor has been summoned here.
I will proceed to outline my recommendations, with the priorities at the top:

1- We cannot have Personal Identifiable Information and Sensitive Personal Identifiable Information stored in non-encrypted databases. Encryption mechanisms should be in place for these tables, also take into consideration hardware requirements for dealing with encrypted data in terms of computing power.

Make this a priority, since law infringement fines are severe if we were to fail in this area.

2- Someone from I.T., should have no access to accounting database information or payroll informational data. Only the I.T. lead and its DBA (Database Admin) should have access to these. We saw many users members of a lot of groups in Active Directory, granting them permissions to tools they don't really use or need.
If their access is compromised, all of those tools will be affected as well.

3- The majority of users are using weak passwords; the company has password policies, yes, but they are outdated. Make sure your Domain Controller's Active Directory enforces strong password policies and longevity.
Here is a good one:

- -Password must be at least 12 characters long
- -Must contain at least one capital letter
- -Must contain at least one number
- -Must contain at least one special character
- -It should not contain any logical or calendar sequence
- -Password expires every 4 months, users are forced to change to a new password that wasn't used before.

4- I understand this might be troublesome for some users, consider acquiring Business Password Managers for your users. (LastPass and BitWarden are the ones I like).

5- We currently have no way to determine if we are under attack by black hat hackers or threat actors, with the lack of Intrusion Prevention and Intrusion Detection Systems, we are sitting ducks in the cybersecurity world.
Consider acquiring IDS and IPS systems, like Palo Alto or Security Onion, there are a lot of good options out there, feel free to visit:
[Top 10 Intrusion Detection and Prevention Systems - ClearNetwork, Inc]

6- No security system is perfect, and we must be ready for Worst Case Scenarios.

We need backup solutions for our Workstations, Servers, and Network equipment config files, as currently, a successful ransomware attack will leave us with two options:

A. Start from Scratch and lose all Data, (all of it).
B. Pay the ransom

7- Employees working from home (or from Starbucks), are allowed to connect to Insecure\Public Wifi networks.

Please Implement a GPO Policy (from your Domain Controller) to the company's workstations, where connections to WPA2 SSIDs is a must.

8- The good feedback is in regards to your physical controls; those are up to date and top notch, we need to take both Technical Controls and Administrative Controls to the same level.

Let's circle back about this in a week.

Regards
Raul A. Pinedo Z.
Enterprise IT Systems Senior Advisor

raul@pinedo.xyz