BeyondTrust

>>> Get the full picture of your organization's security standing

Cybersecurity Control Checklist

Step-by-Step Security Controls Evaluation

The first step in making cybersecurity and data security improvements is cataloging what control processes are already in place.

Getting the full picture of your organization's *actual* security standing?

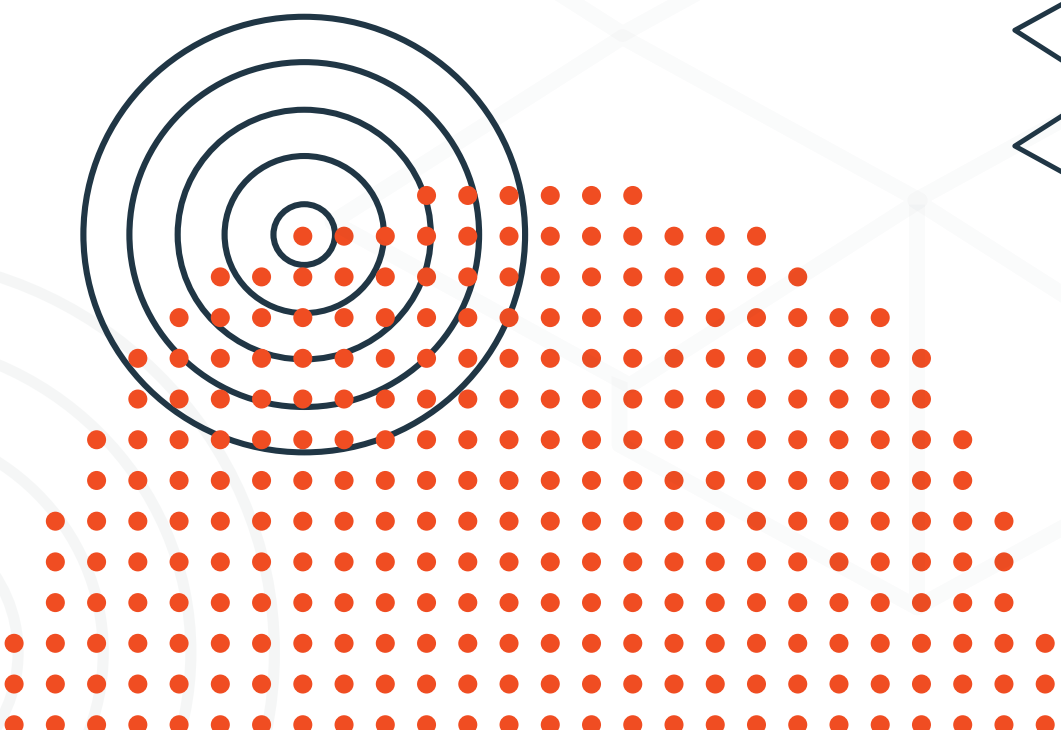
Easier said than done.

That's where this checklist is designed to help.

Examine security controls piece-by-piece—from password policies to solution-specific compliance requirements—to evaluate the realities of your existing security conditions.

Use this sample security assessment questionnaire to evaluate your organization's current security controls – and any weak points that need to be addressed.

These questions span the basic requirements for organizations seeking to host solutions in the cloud or on-premises, including personnel, network, IT application, vulnerability, physical security, and cyber insurance control measures.



	Cybersecurity and Personnel Security Controls	Response (Yes, No, N/A)	Additional Notes
1	Is there a dedicated information security organization, team, or department responsible for security program management?		
2	Is there an information security program in place approved by management and distributed across the organization?		
3	Are information security policies reviewed annually, at a minimum?		
4	Is a background screening performed prior to allowing employees and contractors access to systems and resources?		
5	Has the organization established and documented data governance frameworks with multiple sensitivity tiers?		
6	Is there an acceptable use policy in place, outlining authorized use of equipment?		
7	Are there non-disclosure agreements (NDA) and/or confidentiality agreements in place to outline permissible data use?		
8	Are all employees and contractors required to sign an NDA or confidentiality agreement prior to being granted access to customer data?		
9	Are self-assessments of internal security controls being performed for purposes of verifying compliance with information security policies, as well as with any legal, regulatory, or industry requirements?		
10	Are independent audits being performed at a regular cadence to ensure compliance with regulatory requirements?		
11	Are there independent assessments of security controls performed annually, at a minimum?		

Network Security Controls		Response (Yes, No, N/A)	Additional Notes
1	Are there asset management policies or programs in place that includes both hardware and software?		
2	Are formally documented hardening guides for all deployed assets available (on-premises and cloud)?		
3	Are firewalls used for all internal connections?		
4	Are firewalls used for all external connections?		
5	Are firewalls used to segment internal networks?		
6	Is there a web application firewall (WAF) in use?		
7	Are network DMZ segments being used to segment devices initiating outbound traffic?		
8	Are network and production systems limiting communications with known malicious IP addresses (block lists) or limiting access to trusted sites only (allow lists)?		
9	Is remote access to systems and networks containing customer data permitted?		
10	Is multi-factor authentication (MFA) required for remote access?		
11	Are there network monitoring or a network access control devices (NAC) to detect unauthorized connections to the network?		

Data Protection and Recovery Controls		Response (Yes, No, N/A)	Additional Notes
1	Is there a Data Loss Prevention solution in place to monitor and control the flow of data within the network?		
2	Is scoped data sent or received electronically?		
3	Is scoped data sent or received via physical media or paper?		
4	Is there an appropriate transport security layer in place for scoped data?		
5	Are data layer encryptions in place for in-scope data?		
6	Is collected customer data obtained and securely sent back to the customer?		
7	Is customer data permitted on endpoint devices, such as laptops or other workstations?		
8	Has hard drive encryption software been pushed to laptops and workstation devices?		
9	Has hard drive encryption software been pushed to mobile devices?		
10	Is customer data ever copied to mobile media (USB drives, CDs, DVDs, external drives, etc.)?		
11	Are there documented policies for business continuity and disaster recovery?		
Physical Security Controls		**Response (Yes, No, N/A)**	**Additional Notes**
1	Are there physical security policies covering scoped systems and data?		
2	Is there a Service Organization Controls report that covers physical and environmental security controls of data centers?		

User Access and Authentication Controls		Response (Yes, No, N/A)	Additional Notes
1	Is there a formally documented access control policy covering adding, changing, and removing users from systems and networks?		
2	Are there dynamic calls/API calls in place to eliminate embedded or hard-coded credentials?		
3	Are unique user access IDs assigned to all employees, contractors, and machine-based identities?		
4	Are passwords, SSH keys, and other secrets automatically rotated according to a defined schedule, or after each use?		
5	Are there single sign-on (SSO) protocols in place?		
6	Are password management policies enforced across all privileged access points?		
7	Are user access rights reviewed annually, at a minimum?		
8	Are there formally documented password policies dictating length, strength, history, and account lockouts for corporate resources?		

Vulnerability Management Controls		Response (Yes, No, N/A)	Additional Notes
1	Are all systems and applications patched according to service- level agreements?		
2	Are vulnerability scans performed on systems and data at a regular cadence?		
3	Are external penetration tests performed on systems and data annually, at a minimum?		
4	Are there operational change management and change control policies in place?		

IT Monitoring and Response Controls		Response (Yes, No, N/A)	Additional Notes
1	Are there established programs, standards, or strategies for logging and monitoring suspicious activity?		
2	Are there intrusion detection (IDS) or intrusion prevention (IPS) systems in place?		
3	Are security event data and logs captured for all applications and solutions provided to the customer?		
4	Are all collected logs sent to a centralized logging or Security Information and Event Management (SIEM) solution?		
5	Are there documented policies for incident management that are readily available to the organization?		
Vendor and Third-Party Management Controls		**Response (Yes, No, N/A)**	**Additional Notes**
1	Do external parties (vendors, subcontractors, etc.) have access to systems and applicable data within scope?		
2	Are there contractual controls to ensure personal information shared with third parties is closely constrained to defined parameters?		
3	Are there documented management processes in place for the selection and oversight of third-party access?		
IT Application Controls		**Response (Yes, No, N/A)**	**Additional Notes**
1	Are there formal Software Development Life Cycle (SDLC) processes documented?		
2	Is source code frequently reviewed to ensure adherence to the programming standards, cleansing of dead code, or checking of critical algorithms?		
3	Is open source software permitted?		
4	Are there automated secure source code reviews for all code, prior to production?		
5	Are mobile applications developed and used for in-scope data?		
6	Do mobile application development workflows follow the same secure coding procedures as software?		

	Solution-Specific Security Controls	Response (Yes, No, N/A)	Additional Notes
1	Are all customer users provisioned to systems based on job function or role, including administrator access?		
2	Are there formally documented termination procedures in place for customer stakeholders?		
3	Are access reviews performed at a regular cadence for the solution provided to the customer?		
4	Is there collaboration with the customer to review user accounts?		
5	Are single-sign-on (SSO) options available for the application provided to the customer?		
6	Do inactive customer sessions timeout after a designated period?		
7	Do systems used by customers have password policies that meet the below requirements? • *Minimum 12 characters* • *3 character types required for complexity* • *Previous 12 passwords cannot be reused* • *Accounts lock after more than 5 attempts in 24 hours*		
8	Are self-resets allowed for passwords, when locked or forgotten?		
9	Are user passwords encrypted at rest?		
10	Are multi-factor authentication (MFA) features a solution option or are they required?		
11	Are application penetration tests performed at least annually on any in scope applications?		
	Cyber Insurance Controls	**Response (Yes, No, N/A)**	**Additional Notes**
1	Does the organization possess insurance coverage for a cyber-related incident or attack?		
2	What is the total amount of coverage provided by cyber insurance?		

Noticing gaps in security coverage? BeyondTrust can help.

Privileged accounts pose one of the biggest threats to your organization's security. You need to know identities and access pathways are secure.

The BeyondTrust platform enables identity and access security that is monitored, managed, secured, and just-in-time. BeyondTrust's Privileged Access Management (PAM) solutions are built to quickly get your organization aligned with identity and access security best practices. Reliably address gaps around privileges, identities, access controls, remote access, monitoring, and auditing with BeyondTrust.

BeyondTrust PAM is comprised of:

Privileged Password Management
Discover, manage, audit, and monitor privileged accounts and credentials.

Secure Remote Access
Centrally manage remote access for service desks, vendors, and operators.

Endpoint Privilege Management
Enforce least privilege across Windows, Mac, Linux, and Unix endpoints.

Cloud Security Management
Automate the management of identities and assets across your multicloud footprint.

Learn more about BeyondTrust | **Contact our experts for recommendations**

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network.

beyondtrust.com