NEXT PERIMETER

INFORMATION SYSTEMS

AUDIT CHECKLIST

NextPerimeter.com // 888-286-4816

INTERNAL AND EXTERNAL AUDIT	✓	✗
1. Internal audit program and/or policy		
2. Information relative to the qualifications and experience of the company's internal auditor		
3. Copies of internal IS audit reports for the past two years		
4. Copies of most recent IS audits performed by regulatory agencies or other outside auditors		
5. All IT's responses to IS audits or regulatory examinations		
6. Minutes of audit committee minutes		

MANAGEMENT	✓	✗
1. Organizational chart listing individuals responsible for IS along with job titles		
2. Any available biographical or certification data for key IS personnel		
3. Any available job descriptions		
4. Minutes of the board of directors meetings for the past twelve months		
5. Information about IS governance committees often called steering committees or technology committees as well as minutes of meetings for the past twelve months		
6. Copies of all policies governing IS activity		
7. Copies of current IS insurance policies including coverage on: equipment and facilities, media reconstruction, items in transit, employee fraud, third-party fraud, business interruption, and errors and omissions		
8. Copies of information systems/ information technology strategic plans		

VENDOR MANAGEMENT	✓	✗
1. Schedule of all applications processed in-house including the name of the software vendor and/or support vendor		
2. Schedule of all applications processed by a service bureau		
3. Any agreements with software, hardware, or network service providers used by the company		
4. Service providers' audited financial statements and annual reports		
5. Any third-party reviews of service providers' controls over information technology and related processes such as SAS 70 reports		
6. Any information about the disaster recovery program and the testing of same for key service providers		
7. Any evidence documenting due diligence concerning the management of vendors such as the way primary outsourced vendor invoices are reviewed for accuracy		
8. Information about the company's involvement in user groups		
9. Procedures for implementing core software vendor release updates		

DEVELOPMENT AND ACQUISITION	✓	✗
1. Procedures, policies, or standards governing the acquisition of technology equipment or software systems and programs		
2. Information about any major development or acquisition projects (A) recently completed, (B) currently underway, or (C) planned for the future		
3. Information about any custom software which the company has developed internally or which it has commissioned a company or person to develop		
4. Information about the development and use of query or data mining reports used by the company		
5. Information about the management, organization, and storage of software licenses for software being utilized by the enterprise		

INFORMATION SECURITY	✓	✗
1. Any information relative to a formal information security program		
2. Any information relative to a formal risk assessment program		
3. Any external reports, studies, or assessments of risks relative to information security		
4. Diagrams or schematics of local and wide area networks		
5. Information about network access controls including firewalls, application access controls, remote access controls, etc.		
6. Information relative to the management, configuration, and monitoring of the network firewalls		
7. Lists and samples of any firewall-generated reports, logs or alerts		
8. Information relative to intrusion protection		
9. Authentication controls including password standards for the network as well as the host processor		

INFORMATION SECURITY	✓	✗
10. Lists and samples of any system-generated reports or logs or any special software used to automatically monitor and report system activity relative to either the network, or any ancillary systems		
11. Vulnerability assessments and/or penetration tests		
12. Information relative to security education of employees		
13. Non-disclosure agreements with vendors		
14. Any information about the use of virus protection software		
15. Information about physical security including locks, fire extinguishers, sprinklers, etc.		
16. Employee handbooks, standards, or policies		
17. Information about any disclosures or contracts signed by employees relative to information systems		

OPERATIONS	✓	✗
1. Schedule of all significant computer equipment including manufacturer, model, operating system if applicable, and as many other identifying characteristics as possible		
2. Operator checklists, user instructions, run books, or other documentation of this type		
3. Procedures designed to facilitate separation of operational duties		
4. Procedures relative to master file changes such as changes of address, due dates, etc.		
5. Procedures or policies relative to the handling of negotiable items		
6. Samples of any manual logs maintained to track IS-related events or problems		

BUSINESS CONTINUITY	✓	✗
1. Information regarding internet banking, telephone banking, and other electronic banking activities engaged in by the company		

BUSINESS CONTINUITY	✓	✗
1. Business continuity plan		
2. Emergency preparedness plans		
3. Inventory of offsite storage facilities		
4. Contracts with business continuity providers		
5. Schedule of equipment and other resources at the designated alternate processing site		
6. Reciprocal agreements with other businesses		
7. Reports of recent business continuity tests		
8. Documentation of vendor assurances relative to business continuity		
9. Procedures, and/or schedules relative to the media backup of all data on all servers including standalone PCs, networked PCs, core processing system, and all ancillary systems		

BUSINESS CONTINUITY	✓	✗
2. Procedures relative to customer user-profiles and passwords		
3. Daily procedures carried out by employees relative to electronic banking		
4. Copies of policies and procedures governing electronic banking activities		
5. Copies of contracts with electronic finance vendors		
6. Network schematic to identify the location of major components		
7. Information relative to the number of customers who use the various electronic banking applications		
8. Information relative to risk assessment of electronic financial activities		
9. Information relative to the design and maintenance of the company's website		
10. Information relative to the flow of information between the company's electronic banking applications and the company's core processing system		

FEDLINE & RETAIL PAYMENT SYSTEMS	✓	✗
1. Business continuity plan		
2. Documentation relative to Fedline or finance related procedures		
3. Documentation relative to ATM administration		
4. Documentation relative to the issuance of ATM/debit cards		
5. Vendor contracts for ATM/ debit card services		
6. Procedures governing PIN administration		
7. Procedures relative to captured and returned cards		
8. Information relative to intrusion protection		
9. ACH policy		
10. ACH origination agreements with customers		
11. Recent NACHA or GACHA audits		
12. Any information relative to funds transfer administration		

WHAT SETS US APART?

It All Starts in the Cloud

Your .com is what ties your business to the web, allowing you to get your email and collaborate online. Whether you're using Google Workspace or Microsoft 365, **Next Perimeter** has you covered. Your team can leverage our certified experts for matters concerning your email deliverability, DNS records, licensing concierge, and more.

Your Team and Workstations are Fully Covered

When your team logs into your corporate environment today, what types of protections exist? **Next Perimeter**, by default, deploys endpoint security and hardware monitoring to every workstation that we manage, ensuring productivity is at an all-time high. Your team will enjoy unlimited round-the-clock support for everyday issues ranging from authentication to hiccups with their equipment.

Battle-Tested SOPs

Whether we will handle all of your IT, or collaborate with an internal team, our procedures have been perfected against millions of business scenarios. Our system has been trained to adapt to each customer as their organizations evolve.

Future-Proofed for Compliance

We know you want your cybersecurity to be reliable, predictable, functional, and cost-effective - that's why we've simplified cyber so it's back-of-mind. By signing up for Essentials, you've created a predictable path toward future compliance needs as our agents can fulfill virtually all requirements they might ask for with simple per-user/device pricing.

NEXT PERIMETER

Let's Work Together

Phone
888-286-4816

Mail
sales@nextperimeter.com

Website
NextPerimeter.com

About Us

As a leader in cloud-first cybersecurity and IT support, Next Perimeter protects businesses from modern threats, whether in the office or remote. Our Zero Trust architecture and SaaS posture management deliver a secure, optimized endpoint experience without the need for servers or office space.

Our SASE network as a service replaces traditional VPNs with an always-on, secure connection, ensuring high-speed, reliable network security across the globe. Specializing in holistic threat detection and response, we safeguard your digital assets with cutting-edge AI-powered solutions.