Breach Prevention Audit

Alpine Security's data Breach Prevention Audit (BPA) is a tool we developed, based on decades of experience with penetration testing, incident response, audits, and working with clients on cybersecurity strategy. We leverage this experience to bring you an audit tool that pinpoints and ranks your weak areas that could be leveraged by an attacker to compromise your environment and data.

Our BPA covers 31 security concepts based on the NIST framework of Identify, Protect, Detect, Respond, and Recover. These security concepts are scored based on the following control groups:

Management

- Cybersecurity controls that focus on the management of risk and the management of information system security.

Operational

- Cybersecurity controls that are primarily implemented and executed by people (as opposed to systems).

Technical

- Cybersecurity controls that are primarily implemented and executed by systems through hardware, software, or firmware.

*The purpose of Alpine Security's data Breach Prevention Audit is to provide organizations with a **quantifiable overview of their cybersecurity landscape** based on management, operational, and technical control groupings. The Breach Prevention Audit report includes a list of top weaknesses along with a prioritized Top 10 list including individual recommendations.*

Our data Breach Prevention Audit is designed to quantifiably measure your risk of a data breach.

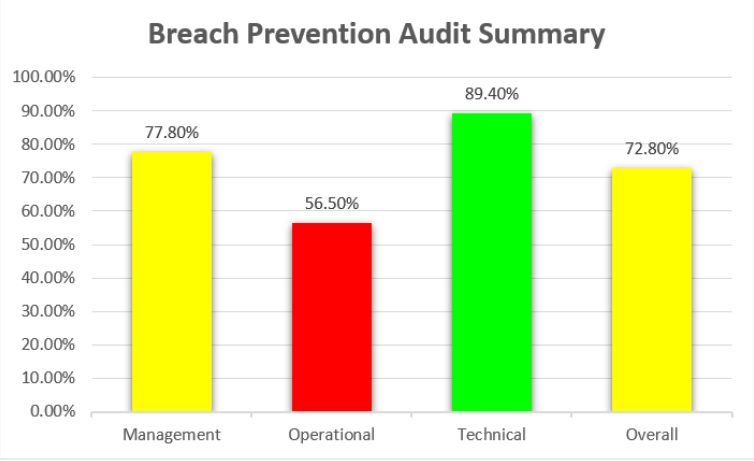
www.alpinesecurity.com
844-925-7463
info@alpinesecurity.com

BPA Report

Our BPA Report includes the following:

- Graph depicting a score for each control group (management, operation, and technical) and an overall breach prevention risk score
- Top weaknesses per category
- Top 10 findings and recommendations
- Report review session to discuss weaknesses and recommendations

	Category	Weakness	Recommendation
1	Operational	No risk assessment	Have a detailed risk assessment performed on organization systems
2	Management	Incident response plan training	Practice the organizations incident response plan, learn from the drill and update the plan accordingly, schedule a future training event
3	Operational	No asset management	Follow organization policy and track devices that are added / removed from the network
4	Technical	Backups are not secured	Protect backup data the same as any other organization data
5	Operational	Shoulder surfing	Implement a password management tool and enforce a clean desk policy to negate shoulder surfing



Contact IMEC to learn more about or schedule your Breach Prevention Audit:

- Emily Lee, Program & Partner Relations Coordinator
- elee@imec.org

www.alpinesecurity.com
844-925-7463
info@alpinesecurity.com