**Email Templates – adjust and fill in as required:**

**Security Assessments for Storage**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} {!how granular?>infrastructure security and compliance.|IT security and compliance.|storage security and compliance.}

We’re seeing growing interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint.

StorageGuard ensures that the storage is hardened, meets security best practices and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Should we meet to review this topic together?

**Security Assessments for Storage (SEC Risk drop)**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} infrastructure security and compliance.

We’re seeing growing interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint.

Given the [SEC Risk Alert](https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf), many began storage security initiatives.

StorageGuard ensures that the storage is hardened, meets security best practices, and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Should we meet to review this topic together?

For this email, please make 2 templates - one for each subject line [1,2]:

1.**Storage Security Audit**

2.**Would {!company} pass a Storage Security Audit?**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} {!how granular?>infrastructure security and compliance.|IT security and compliance.|storage security and compliance.}

We’re seeing significant interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint. For that reason, many began storage security initiatives.

StorageGuard ensures that the storage is hardened, meets security best practices and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Interested in learning more?

**Qualys/Nessus Blind Spot**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} {!how granular?>infrastructure security and compliance.|IT security and compliance.|storage security and compliance.}

We’re seeing growing interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint.

StorageGuard ensures that the storage is hardened, meets security best practices and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Should I arrange a meeting?

**Qualys/Nessus Blind Spot: Enterprise storage**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} {!how granular?>infrastructure security and compliance.|IT security and compliance.|storage security and compliance.}

We’re seeing growing interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint.

StorageGuard ensures that the storage is hardened, meets security best practices and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Should I arrange a meeting?

**Will {!company} pass the next Infrastructure Security Audit?**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} {!how granular?>infrastructure security and compliance.|IT security and compliance.|storage security and compliance.}

We’re seeing significant interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint. For that reason, many began storage security initiatives.

StorageGuard ensures that the storage is hardened, meets security best practices and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Interested in learning more?

**Does {!(company)} run storage security assessments?**

Hi {!name}, I understand you {!how are they involved> are involved with|are responsible for|hold accountability over} securing the enterprise storage at {!(company)}.

We’re seeing growing interest from many in the {!industry>banking|insurance|financial services|communications} industry concerning storage security. They typically turn to us as they successfully secure the OS, servers, and databases, but cannot assess the storage infrastructure. We provide a solution - “Data Security Advisor”.

StorageGuard ensures that the storage is hardened, meets security best practices, and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the storage estate.

Should we meet to review this topic together?

**Is Storage Security a low priority for {!company}?**

Hi {!name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} {!how granular?>infrastructure security and compliance.|IT security and compliance.|storage security and compliance.}

We’re seeing significant interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint. For that reason, many began storage security initiatives.

StorageGuard ensures that the storage is hardened, meets security best practices, and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Interested in learning more?

**Security Assessments for Storage**

Hi {!first name}, I understand that you {!involvement>are involved with|are responsible for|hold accountability over} infrastructure security and compliance.

We’re seeing growing interest from other {!financials/banks>leading banks|insurance leaders|communications leaders|financial services leaders} who successfully secure the OS, servers and databases, but don't have visibility of the enterprise storage from a security/compliance standpoint.

StorageGuard ensures that the storage is hardened, meets security best practices, and complies with standards (NIST, CIS, ISO, SNIA) - across all areas of the enterprise storage.

Should we meet to review this topic together?

**Short templates:**

(1)

We’re helping local & worldwide banks to assess the security of the Storage environment.

Recently banks identified storage as an unacceptable blind spot.

Hacking a storage system =

1. Equivalent of hacking into hundreds of DB servers
2. Ability to delete production data volumes AND replicas/snapshots = make recovery (from ransomware) impossible

(2)

My focus is assisting too-big-to-fail banks assess the security of the storage & backup systems; an area that is gaining more traction due to the enormous amount of data kept and the concern of losing both production and backup data when the storage is hacked.

(3)

I wanted to share the final and approved SP800-209 (Storage Security Guide), co-authored by NIST and our CS team -

<https://csrc.nist.gov/publications/detail/sp/800-209/final>

With the increase in ransomware attacks on enterprises, storage/backup security is naturally gaining more traction (being the final line of defense).

(4)

Our company assists banks such BofA and BNP to assess the security of the enterprise storage estate.

Many security teams feel that they have poor control over the storage environment (non-standard OS, networking, CLI, etc.) - even though this is where all the data is kept.

A breach to a storage system is the equivalent of breach in hundreds of database servers.

(5)

I invite you to check the Storage Security Guide we co-authored with NIST: [csrc.nist.gov/publications/detail/sp/800-209/final](https://csrc.nist.gov/publications/detail/sp/800-209/final)

With the increase in ransomware attacks, storage/backup security is gaining more traction, being the final line of defense.

**Message bodies – can add your opening and closing greetings + call to action:**

1. For example, Bank of America is using our StorageGuard solution to scan thousands of storage devices ensuring that security baselines and regulatory requirements are met.

StorageGuard can also be used for a one-time comprehensive storage security and risk assessment.

I invite you to check the [Storage Security Guide](https://csrc.nist.gov/publications/detail/sp/800-209/final) we co-authored with NIST.

With the increase in ransomware attacks, storage/backup security is gaining more traction, being the final line of defense.

1. A brief reminder of how we protect critical storage systems, StorageGuard ensures that the storage is hardened, ransomware attacks are prevented, meets security best practices and complies with standards ([NIST](https://www.nist.gov/publications/security-guidelines-storage-infrastructure), CIS, [ISO](https://www.iso.org/standard/44404.html)) - on an ongoing basis, across all areas of the storage estate.

You might find this blog interesting [Security baselines for enterprise storage systems: Is yours being followed?](https://www.continuitysoftware.com/blog/baseline-security/security-baselines-for-enterprise-storage-systems-is-yours-being-followed/)

1. While large organizations successfully secure their OS, network, and databases, the vast majority do not have adequate visibility on the security of their **storage systems**.

Our StorageGuard ensures that the storage is hardened, meets security best practices, and complies with standards ([NIST](https://l.shitrk.com/r/e/jovLvsGGzBQH910b7?r=https://www.nist.gov/publications/security-guidelines-storage-infrastructure), CIS, [ISO](https://l.shitrk.com/r/e/e4eReuXXxl6iQ5wVK?r=https://www.iso.org/standard/44404.html)) - on an ongoing basis, across all areas of the storage estate.

StorageGuard can also be leveraged for a one-time storage vulnerability scan, producing a comprehensive storage security report of findings.

1. While large organizations successfully secure their OS, network, and databases, the vast majority do not have adequate visibility on the security of their **storage systems**.

With StorageGuard your customers will be able to automatically check:

1. Security best-practices from the storage vendors.
2. Compliance with standards (NIST, ISO, CIS, SNIA, etc.) as applied to storage.
3. Vulnerabilities (CVEs) for the storage environment.
4. Commonly used security baselines.

StorageGuard can also be leveraged for a one-time storage vulnerability scan, producing a comprehensive storage security report of findings.

1. We are helping local & worldwide banks to assess the security of the Storage environment.

Recently banks identified storage as an unacceptable blind spot.

Hacking a storage system =

1. Equivalent of hacking into hundreds of DB servers
2. Ability to delete production data volumes AND replicas/snapshots = make recovery (from ransomware) impossible

Our StorageGuard solution can also be leveraged for a one-time storage vulnerability scan, producing a comprehensive storage security report of findings.