Quantum

WHITE PAPER

QUANTUM STORNEXT SECURITY

Considerations for Customers Embarking on TISAX or Other Information Security Certification

CONTENTS

INTRODUCTION

Ensuring the security of sensitive and confidential information is critical. In many industries, individual companies exist within a tightly knit network of suppliers, customers, and service providers, where sensitive information is frequently shared across corporate boundaries. It is common in these environments for business partners to require demonstration of compliance with third-party information security standards. This ensures that information that is shared is still appropriately protected.

TISAX is one such standard, derived from ISO / IEC 2700, but adapted to the specific requirements of the German automotive industry. Many other information security standards exist, both public and private. One common feature of most information security standards is that they are holistic. That is, the certified entity is not a product, but an entire organization and its processes.

This document was created to provide IT and information security professionals with items to consider when implementing StorNext® in environments subject to TISAX certification. Most, if not all the information presented is also relevant to other information security standards and best practices.

In this document, we describe several tools required to augment StorNext to operate in a TISAX compliant environment, as well as stating our recommendations to be addressed by a StorNext customer aiming for a TISAX certification. Most of the recommendations are associated with security issues in the customer's organizational processes as they relate to a StorNext environment.

STORNEXT REFERENCE ARCHITECTURE

The diagram below represents a generic StorNext architecture as a reference. The diagram shows a StorNext 6 Cluster of nodes, along with direct-attached clients, proxy clients (aka Distributed LAN Clients), and NAS (NFS and/or SMB) clients. Clients may run Linux, MacOS, or Windows. The StorNext cluster nodes may consist of Quantum-supplied hardware appliances, or customer-supplied hardware. The cluster nodes are connected to the clients and the storage with a variety of network types, which carry data, metadata, or both. For a more detailed discussion of StorNext architecture, refer to the StorNext architecture white paper here.

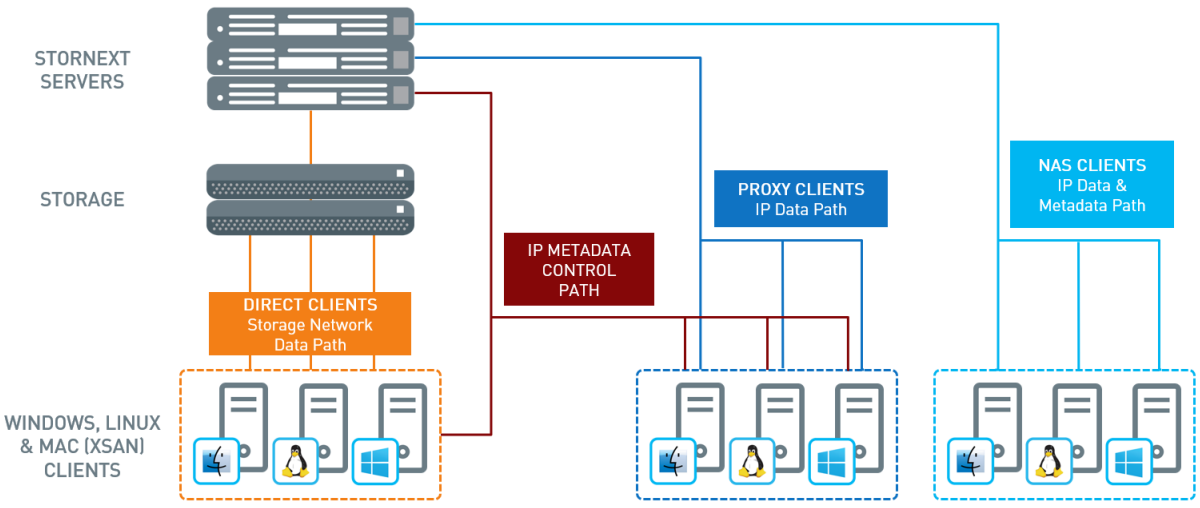

Figure 1 – General StorNext Architecture

ACCESS POINT PROTECTION

In a StorNext configuration as shown above there are several access points that need to be protected, using a layered approach:

a) StorNext direct clients
b) StorNext proxy clients
c) 3rd party NFS/SMB clients
d) Apple XSAN clients

The solution needs to protect all the above methods of access such that the user data is safe and intact. Further, there is a need to protect access to the project data folders on the system. Finally, there is a need to protect the actual user data on the disk sub-systems.

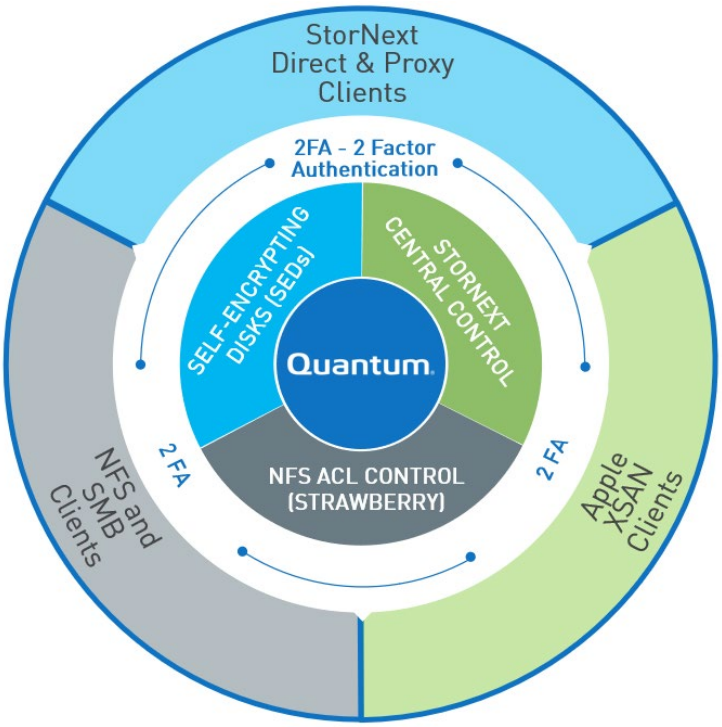

Figure 2 – Protection Layers

The following tools and methods may be employed to accomplish the items called out above:

a) A two-factor authentication (2FA) tool such as SAASPASS to control access to any desktop connected to a StorNext environment
b) The use of StorNext Central Control to secure node access to a StorNext file system
c) A NFSv4 ACL control package such as Strawberry to control user access to a given set of folders
d) Self-encrypting disk drives (SEDs) to secure the data on disk should any disk be stolen

These tools and methods protect a StorNext system against the following threats:

1) A rogue user manages to steal the password from a legitimate user and has physical access to a normal client.
   - Access is blocked by 2FA, the rogue user can't log in.
2) A rogue user manages to steal a password and unlocked 2FA device and has physical access to a normal client.
   - The rogue user can log into the system, but they cannot access any files because the project is closed. ACLs prevent access and the rogue user doesn't have a Strawberry account password to modify ACLs.
3) A rogue user has reverse-engineered StorNext and has their own client version of StorNext that doesn't do any security checking on their own rogue client.
   - Access is blocked by StorNext Central Control since the rogue client's IP address is not on the authorized list.
4) A rogue user steals hard drives.
   - Even if they have access to StorNext, the rogue user would not be able to access the data on the hard drives, because they are encrypted.

DETAILED RECOMMENDATIONS

This chapter contains detailed recommendations cross-referenced to the applicable TISAX requirements. In Quantum's opinion, the TISAX requirements as defined within the TISAX Information Security Assessment (ISA) questionnaire for the following chapters do not apply to StorNext:

- Chapter 1: General Aspects
- Chapter 5: Information Security Policy
- Chapter 6: Organization of Information Security
- Chapter 7: Human Resource Security
- Chapter 15: Supplier Relationships
- Chapter 18: Compliance

However, these requirements are still applicable for Quantum customers pursuing TISAX certification. Note that chapter numbering in the TISAX ISA questionnaire skips from chapter 1 to chapter 5. There are no chapters 2, 3, or 4.

The TISAX ISA questionnaire used in the preparation of this document was v4.1.1.

The remainder of this document lists all TISAX requirements Quantum believes apply to StorNext, organized by ISA questionnaire chapter and reference number. For each requirement number and text there is a short description explaining why the requirement is relevant to StorNext, and the recommended actions customers should take to address the requirement in the context of a StorNext environment.

TISAX ISA requirements are worded in the form of "to what extent..." questions. The answer is stated in terms of one of six maturity levels, from Level 0 (Incomplete) to Level 5 (Optimizing). Refer to the ISA questionnaire document for a detailed explanation of the levels and summary of the typical assessment process.

TISAX CHAPTER 8 - ASSET MANAGEMENT

TISAX ISA Requirements

#	Question
8.1	To what extent are inventories existent for objects (assets) that contain information in different versions?
8.2	To what extent is information classified according to its protection needs and are there regulations in place regarding labelling, handling, transport, storage, retention, deletion and disposal?
8.3	To what extent are appropriate procedures implemented for the management of information on mobile storage devices?
8.4	To what extent is the secure removal of information assets from IT services (particularly cloud) ensured?

StorNext Relevance

In the context of StorNext, information assets will be stored in form of files. The infrastructure of StorNext itself is also an asset.

Information assets are elements of information-related character, e.g. documents, illustrations, files, programs, servers, networks, facilities, vehicle prototypes, design-relevant or shaping tools and equipment. Not listing them, classifying them and naming responsible entities poses a threat to IT security in the context of the company's security policy.

Recommendation

Define, document and regularly update a policy for asset management and information classification regarding information assets within StorNext and the StorNext infrastructure itself. Technical and organizational measures to enforce "need-to-know" principles for information assets should be in place and verified.

TISAX CHAPTER 9 - ACCESS CONTROL

TISAX ISA Requirements

#	Question
9.1	To what extent are policies and procedures regarding the user access to network services, IT systems and IT applications in place?
9.2	To what extent are procedures for user registration, change and de-registration implemented and is particularly the authentication information handled confidentially?
9.3	To what extent is the allocation and use of privileged user and technical accounts regulated and is it subject to reviews?
9.4	To what extent is the user subject to binding policies concerning the creation and handling of confidential authentication information?
9.5	To what extent is access to information and applications restricted to authorized persons?
9.6	To what extent is the separation of data within an environment shared with other organizations ensured?

StorNext Relevance

StorNext has multiple layers for access. Aside from the StorNext software, primary and secondary storage devices usually implement their own access control management for administrative access. Often these access management schemes cannot be connected to a directory service, limiting the ability to implement individual privileged and technical accounts.

The following sub systems have their own access management systems:

- StorNext Server
- StorNext GUI
- StorNext Vault
- StorNext SAN clients
- StorNext LAN clients
- StorNext NFS & SMB
- Primary and secondary storage devices (disk, SSD, tape library, etc.)

This poses a risk of asynchrony and duplicate data holding in the context of user registration, change and de-registration. Furthermore, uncontrolled use of not personally identifiable accounts for administration may lead to actions not being part of monitoring and therefore hampering clear traceability for administrative actions. This poses a threat to IT security.

Recommendation

StorNext offers the option to use named administrator accounts. These accounts should be synchronized with the company's access control, e.g. connected to a privileged account management (PAM) system. The use of system technical accounts should be prohibited for personal use. Administrators should be given personal accounts with the corresponding access right based on the "need-to-know" principle.

All administrative actions should be part of the user and access rights management process such as PAM. Separation of data, applications, operating system, storage and network policy must be binding to all users of information and application, that is, for the StorNext privileged user accounts as well. Users must be informed and made aware of the regulations (e.g. password rules). Means of secure retention of authentication information (e.g. a password safe) must be provided. A policy based on business and security-relevant requirements needs to be defined, documented and regularly updated. Unique and personalized user IDs must be used.

TISAX CHAPTER 10 - CRYPTOGRAPHY

TISAX ISA Requirement

#	Question
10.1	To what extent are rules for encryption, including the management of cryptographic keys (complete lifecycle process) for the protection of information during storage and transport existent and have they been implemented?

StorNext Relevance

Protection of the confidentiality of information stored to StorNext volumes using encryption is optional. Storage systems using hardware-based encryption, such as disk arrays using self-encrypting drives (SEDs) and tape libraries using tape encryption, operate transparently below StorNext software.

Within StorNext, it is possible to enable and disable encryption for cloud data stores like AWS, AWS GovCloud, AWS C2S and Microsoft Azure, and others. The cloud encryption keys are maintained in the StorNext database. They cannot be made visible in the GUI but may be exposed by knowledgeable users logged into a StorNext Metadata Controller (MDC). The server side StorNext web GUI, managed by administrators, uses a self-signed certificate. This certificate could be exported by a knowledgeable user with root privileges on the MDC.

The "Q-Cloud" cloud storage feature optionally uses client-side encryption keys generated by the MDC server, using an administrator-supplied master key passphrase. Q-Cloud is no longer supported beginning with the release of StorNext 7.0.

Potential access to encryption keys and certificates via the StorNext MDC CLI poses a threat to the client's data protection requirement and the "need-to-know" principle.

Recommendation

For clients using the Q-Cloud feature with client-side encryption, depending on the data classification the master key passphrase should be stored in a secure environment - for example in a physical (not software-defined) storage location such as a personal password store with restricted and controlled access. Any cryptographic keys used within StorNext should be part of the company's cryptographic key management processes and policies. Those must be defined, documented and regularly updated. Access to the MDC CLI, and particularly root user access, must be restricted and controlled per the recommendations outlined elsewhere in this document.

TISAX CHAPTER 11 - PHYSICAL & ENVIRONMENTAL SECURITY

TISAX ISA Requirement

#	Question
11.2	To what extent has the company taken measures against the effects of natural disasters, deliberate attacks or accidents?

StorNext Relevance

The StorNext hardware as a central point of storage of highly sensitive/TISAX relevant data must be protected against all kinds of natural disasters. Natural disasters can harm or destroy the StorNext hardware in an uncontrolled and not predictable way, which poses a security threat.

Recommendation

StorNext as an IT service needs to be embedded into the customer's IT service continuity management (ITSCM) and business continuity management (BCM) plans. These plans must be documented and regularly updated, for example by defining disaster recovery plans, such that IT disasters can be addressed. Furthermore, regular recovery tests should be performed. Additionally, customers should implement risk-analysis-based preventive controls such as zoning within datacenters and protection against natural disasters such as fire.

TISAX ISA Requirement

#	Question
11.4	To what extent are policies and procedures regarding the use of assets, including off-premises use, disposal and re-use in place and implemented?

StorNext Relevance

As a central storage system, StorNext hardware can store sensitive/TISAX relevant data that is subject to high security requirements regarding confidentiality. Removing storage disks could lead to information disclosure to third parties.

Recommendation

StorNext hardware must be included in applicable deletion and destruction processes in order to enable a safe disposal of the hardware. These processes must be revised, documented and updated on a regular basis. The use of self-encrypting disk drives and secondary storage encryption (e.g. tape encryption) is recommended to render end of life storage assets unreadable.

TISAX CHAPTER 12 - OPERATIONS SECURITY

TISAX ISA Requirement

#	Question
12.1	To what extent are changes to the organization, business processes, information processing facilities and systems controlled and implemented according to their security relevance?

StorNext Relevance

The special relevance of StorNext as a central storage location for highly sensitive/TISAX relevant data requires a detailed security analysis of changes in hardware and software or corresponding processes.

As a central storage location for all types of information including sensitive/TISAX relevant data, changes affecting StorNext technically or procedurally could lead to information disclosure or service unavailability.

Recommendation

Security implications of updates provided by Quantum are documented in product documentation, release notes, and security bulletins. Customers must integrate StorNext into their change management processes and evaluate carefully the security implications of changes to the StorNext environment. Customers change management processes must be revised, documented and updated on a regular basis.

TISAX ISA Requirement

#	Question
12.2	To what extent are development and testing environments kept separate from productive environments?

StorNext Relevance

Changes to StorNext software or hardware components could impact a customer's environment which may lead to service unavailability or data loss.

Recommendation

Customers should perform a risk assessment in order to determine the necessity of maintaining a StorNext development and test system separate from the production system. A separate development system may be used to evaluate the security implications of proposed changes without impacting production.

TISAX ISA Requirement

#	Question
12.3	To what extent are protection controls (e.g. endpoint security) against malware (viruses, worms, Trojans, spyware, ...) implemented in combination with appropriate user awareness?

StorNext Relevance

StorNext does not incorporate protection controls against malware. StorNext may contain highly sensitive/TISAX relevant data. Loss of integrity or unavailability due to malware infections such as viruses and worms poses a threat to information security.

Recommendation

On the StorNext hardware devices and corresponding software devices, infection possibilities must be reduced by technical and organizational measures. For example, by ensuring that web browsers and networking services are either not installed or they are disabled and by ensuring that the checksums of all firmware updates correspond to the official checksums on Quantum's website. Furthermore, the implementation of organizational security measures such as regular process checks to minimize infection vectors for the StorNext hardware and software is recommended. Finally, a risk-based analysis of the customer's implementation should consider the integration of malware protection software, following Quantum's guidelines, to be compliant with this TISAX requirement.

TISAX ISA Requirement

#	Question
12.4	To what extent are backups created and regularly tested in accordance with an agreed backup policy?

StorNext Relevance

StorNext internal data such as databases and relations provide the basis for a functioning storage system. This data is therefore highly critical for the functionality of StorNext itself. Unavailability of these databases and relations for indexing and sorting the data artifacts on the storage will affect StorNext performance and availability.

Recommendation

StorNext internal databases and configurations are to be embedded in a backup and restore concept and verified by regular tests. The respective media must be handled according to corresponding policies.

TISAX ISA Requirement

#	Question
12.5	To what extent are event logs (which may contain e.g. user activities, exceptions, errors and security events) created, stored, reviewed and protected against modification?

StorNext Relevance

Event logs are stored locally on the storage controller and are not protected against modification. In case of compromise, an attacker can modify the event logs and blur his traces, which poses a threat to IT security. A malicious administrator can manipulate his own actions within the system log files and therefore compromises the traceability of administrative actions.

Recommendation

Event logs should be monitored within a defined documented and regularly updated process to identify modification of event and log files - for example by comparing hash values. We suggest using an external monitoring solution that receives the log files and is in control of a different organizational unit to integrate a separated monitoring process.

TISAX ISA Requirement

#	Question
12.6	To what extent are the activities of system administrators and system operators logged, the logs protected against modification and regularly reviewed?

StorNext Relevance

Actions of system administration are tracked locally on StorNext by default. The traceability of all administrative and operational activities is tracked in the corresponding local StorNext log files. Integrity and availability of this information could be violated at this single point.

Recommendation

Definition of security use-cases (such as login of an administrator) and integration into a defined, documented and regularly updated process to monitor for all security relevant events - for example by integration into existing security information and event management (SIEM) system - is recommended to track all security relevant events from StorNext in a central system to ensure availability and integrity.

TISAX ISA Requirement

#	Question
12.7	To what extent is information regarding technical vulnerabilities of IT systems acquired at an early stage, evaluated and are appropriate measures taken (e.g. patch management)?

StorNext Relevance

StorNext software and hardware technology parts may be vulnerable to attacks due to software or hardware vulnerabilities. Vulnerabilities within the software versions used, for example OS, databases, web servers pose a threat to IT security.

Recommendation

The update of StorNext software and all components must be ensured by a software update management process. This process must obtain and apply relevant software updates as provided by Quantum's Service and Support organization. The software update management process needs to be documented and updated on a regular basis.

TISAX ISA Requirement

#	Question
12.9	To what extent have effects due to critical functions of cloud services been taken into account?

StorNext Relevance

StorNext can make use of public cloud services including their functions for storing data outside of the company's perimeter. The storage of information assets within public cloud services poses a threat to IT security as public cloud services are based on shared infrastructure.

Recommendation

Usage of the StorNext with public cloud services is to be integrated into a comprehensive security concept aligned with TISAX requirements and taking into account the classification of the data. Further requirements such as encryption of data at rest and in motion should be considered where appropriate. A policy on the use of StorNext with public cloud services should be documented and updated on a regular basis to meet IT security requirements, taking into account a risk assessment for public cloud services.

TISAX CHAPTER 13 - COMMUNICATIONS SECURITY

TISAX ISA Requirement

#	Question
13.1	To what extent are networks managed and controlled to protect information in IT systems and applications?
13.2	To what extent are requirements for security mechanisms and service levels and also management requirements for network services identified and documented in service level agreements?
13.3	To what extent are groups of information services, users and information systems segmented on networks?
13.4	To what extent is information protected during exchange or transfer?

StorNext Relevance

The network architecture of StorNext is separated into data and metadata networks. These networks could make use of a specific StorNext protocol (such as FlexSync) and use Fibre-Channel or Ethernet without encryption for data in motion. Disruption of the data or metadata networks can affect service availability, and information disclosure due to plaintext information transfer poses a threat to IT security.

Recommendation

StorNext internal networks with appropriate separation, physical and virtual, should be implemented according to a defined, documented and regularly updated network security architecture including restriction of access to the necessary devices and services as well as other types of access such as operational and failure accesses and their implementation. The distribution of the corresponding networks within the company using StorNext must be included in the corresponding concepts and network management and needs to be revised, documented and updated on a regular basis.

TISAX CHAPTER 14 - SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE

TISAX ISA Requirement

#	Question
14.1	To what extent are security specific requirements taken into account for new IT systems (including publicly accessible systems) and for extensions to existing IT systems?

StorNext Relevance

StorNext hardware and software in use is to be rated as system acquisition and must be evaluated from a security point of view.

Recommendation

As a central storage location for sensitive/TISAX relevant information, the corresponding requirements based on the protection requirement analysis of the information assets within StorNext must be taken into account when purchasing and expanding the system. We recommend creating a dedicated security concept and integrating technical and organizational security measures for StorNext. Additionally, a security assessment should take place for the company's procurement process and be documented and updated on a regular basis.

TISAX CHAPTER 16 - INFORMATION SECURITY INCIDENT MANAGEMENT

TISAX ISA Requirements

#	Question
16.1	To what extent are responsibilities, procedures, reporting channels and criticality levels established to ensure an effective response to information security incidents or vulnerabilities?
16.2	To what extent is the handling of information security events performed?

StorNext Relevance

StorNext does not implement integration into SIEM systems by default but contains valuable information regarding information security incidents such as user accounts and administrative actions. Central storage systems such as StorNext are high priority targets for attackers as sensitive information is very likely to be stored within these systems. In the case of an advanced persistent threat, the attacker may try to delete entry and working information on the StorNext system.

Recommendation

IT security events for StorNext shall be assessed. There needs to be an adequate reaction to IT security events based on defined procedures. In the aftermath of IT security events, findings need to be used to reduce the probability of future events occurring based on defined processes. System log files should be transferred outside StorNext as well. For the SIEM integration of StorNext there must be roles and responsibilities defined, documented and updated on a regular basis that are strictly separated from the backup and operator's roles, in a technical and organizational way.

TISAX CHAPTER 17 - INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

TISAX ISA Requirement

#	Question
17.1	To what extent are information security requirements (including redundancy of corresponding facilities) and the continuity of the information security management systems (ISMS) in the event of a crisis defined, implemented, verified and evaluated?

StorNext Relevance

StorNext can be architected to be a central storage service of an organization and therefore contain business critical information.

In the event of a disaster, StorNext and the information assets within are at the risk of permanent loss or information disclosure. Business processes that require StorNext as dependent service are likely to pose a threat in terms of being affected or not working as intended.

Recommendation

Information assets within and StorNext as central IT service need to be included into business and risk analysis, documented and updated on a regular basis, to the BCM/ITSCM plan in order to ensure a failover or business workarounds in the case of disaster, even if it is used as a passive backup system.

Technical implementations of high availability of StorNext are available from Quantum and should be taken into consideration.

Quantum®

ABOUT QUANTUM

Quantum technology and services help customers capture, create and share digital content – and preserve and protect it for decades at the lowest cost. Quantum's platforms provide the fastest performance for high-resolution video, images, and industrial IoT, with solutions built for every stage of the data lifecycle, from high-performance ingest to real-time collaboration and analysis and low-cost archiving. Every day the world's leading entertainment companies, sports franchises, research scientists, government agencies, enterprises, and cloud providers are making the world happier, safer, and smarter on Quantum. See how at **www.quantum.com**.

www.quantum.com • 800-677-6268

WP00257A-v01 June 2020