NCC Group
Risk Management and Governance

Nextcloud 11 – Security Review

Version 1.1

NCC Group PLC - Security Consulting

Manchester Technology Centre
Oxford Road,
Manchester
M1 7EF

www.nccgroup.com

Document Control

Document Version Control

Document Classification:	Client Confidential
Client Name	Nextcloud
NCCGP Document Reference:	STRK-001- Nextcloud
Document Title	Nextcloud 11 – Security Review
Author Name:	Rod Parker

Document History

Issue Number	Issue Date	Issued By	Change Description
0.1	24/11/2016	Rod Parker	NCC Group internal document creation
0.2	29/11/2016	Rod Parker	Customer findings review
0.3	02/12/2016	Kai Man	Internal QA
1.0	02/12/2016	Rod Parker	Customer release
1.1	06/12/2016	Rod Parker	Customer updates

Document Distribution List

Proprietary Information

This document contains detailed commercial, financial and legal information, which is confidential and commercially sensitive. The release of such information will be prejudicial to the commercial interests of NCC Group and therefore should not be disclosed as a response to a Request for Information under the Freedom of Information Act 2002. The document may also not be reproduced or the contents transmitted to any third party without the express consent of NCC Group.

Table of Contents

Glossary of Terms

The following terms and abbreviations have been used within this document:

Abbreviation	Meaning
NCSC	UK - National Cyber Security Centre
NSA	National Security Agency
NIST	National Institute of Standards and Technology
IaaS	Infrastructure as a Service
SaaS	Software as a Service

1 Executive Summary

1.1 Background

Nextcloud GmbH - is the company behind the Nextcloud open-source project providing an on- premise solution that allows customers to host their own file sync and share solution. As Nextcloud looks to improve the security controls around its solution, Nextcloud are seeking to undertake a review of its current security measures. This will align Nextcloud to security best practice and will provide customers with the assurance they demand.

Nextcloud customers want to know if appropriate security measures and controls are in place and how this compares with the rest of the industry. As an open-source company, Nextcloud is very often faced with having to evidence its security processes in heavily regulated markets such as Government and Finance.

NCC Group have undertaken a security review of the new security features to be deployed within the Nextcloud 11 edition and the supporting assurance management and development framework that supports the product and service.

Approach

Rather than just undertake a tactical 'point in time' review of Nextcloud source code, or conduct a penetration test of the solution, Nextcloud wants a review of their security frameworks including their processes and procedures around systems development and the new security features within the Nextcloud 11 edition due to be released in December 2016. These elements were security assessed against ISO27001 clause 14 controls and key best practice security principles such as management of data in transit, operational security, secure development, governance, and access control.

The review format is undertaken in 2 parts; Sections 1 and 2 look at the Nextcloud supporting frameworks, such as assurance around policy, process, procedures, governance and operational security. Section 3 reviews the new Nextcloud 11 security features. Both activities have a finding and recommendations output and where appropriate additional supporting information.

1.2 High Level Summary of Findings and Recommendations

Following the security review of the Nextcloud assurance landscape in terms of where Nextcloud align to industry standards and best practices, it was assessed that the design and management framework meets a very high standard. This assurance framework provides a good platform of support for the new security features that come with the Nextcloud 11 edition. There are though a small number of related security activities related to the assurance framework that the Nextcloud stakeholders should consider and manage accordingly. The table below provides a high level summary of the main findings and a list of recommendations for each of the Security Principle groupings.

The key below represents the compliance status used throughout the document and is represented by a simple RAG status as detailed below.

🟩	Accept	Standards are being met
🟥	Action	Standards are not met
🟨	Treat	Areas in need of review and recommended updates

RAG	Finding
🟩	Nextcloud recognises the importance of security and there is a strong business driver for them to pursue alignment to Industry standards and best practices. This finding is borne out by the positive status of their assurance frameworks against industry related controls and security principles that can be seen throughout this document.
🟨	Whilst Nextcloud policy is communicated predominantly via their website there is a general view across all policies for a need to further mature the documented policy and process framework(s).

The following list provides recommendations with associated activities that will help provide robust assurance to the overall security environment;

- Further develop and document areas of policy;
- Undertake employee screening (vetting);
- Produce a High Level Design Document that includes basic information around security and process – (In doing so this provides consistency in secure design);
- Look to adopt and align to an internal standard such as ISO/IEC 27001:2013;
- Undertake a Gap Analysis against an International standard;
- Use the Gap Analysis findings against a standard to further mature the business security standing;
- Assure the corporate IT environment to a Cyber Essentials scheme.

1.3 Detailed Findings

The following table provides a review against the control Clause 14 of ISO27001 "Security in Development and Support processes". Where appropriate NCC Group have provided additional information assurance statements. This will help Nextcloud stakeholders to further consider, develop and mature the current security standing.

SO27001-2013 Control 14.2 - Security in development and support processes.
Objective: To ensure that information security is designed and implemented within the development lifecycle of systems.

Ref.	ISO27001:2013 Requirement	Findings	RAG	Additional Assurance Information
A.14.2.1	**Secure Development Policy: -** Rules for the development of software and systems shall be established and applied to developments within the organization; **Policies** - policies mandating the implementation and assessment of security controls.	Nextcloud GmbH - is the company behind the Nextcloud open-source project providing an on-premise solution that allows customers to host their own private File sync and share instance. As such Nextcloud GmbH develops the following software: **Nextcloud Server Software** - The Nextcloud server software is a component written in PHP (supported on PHP 5.6 and newer). It is offering a web interface as well as multiple APIs for clients to access the stored data. Stored data can be files, calendars or contacts and they can be shared or private. **Nextcloud Android Client** - The Nextcloud Android client is a Java software that allows users to view, modify and share their files stored on their Nextcloud. **Nextcloud Desktop Client** - The cross-platform Nextcloud desktop client is developed in Qt and allows users to sync their files with their local computers. It runs on Windows, Linux and OS X. **Implementation and assessment of security controls Policy** - Each release has to pass the following security checks before being released: - Dynamic scanning - Static scanning - Manual penetration testing Nextcloud follow OWASP Top 10 and run a bug bounty program at https://hackerone.com/nextcloud	🟩	Nextcloud MUST continue to mature its policy environment. Nextcloud understands and appreciates the importance of defined policy which is an absolute necessity to build up a secure service, around design, architecture, and software and in-turn providing consumer / customer confidence. Within a secure development policy, the following key aspects should form a solid foundation of that required confidence: - security in the software development methodology; - secure coding guidelines for each programming language used; - security requirements in the design phase; - security checkpoints within the project milestones; - secure repositories; - security in the version control; - required application security knowledge; - Developers' capability of avoiding, finding and fixing vulnerabilities.

A.14.2.	**System change control procedures -** Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures - **Does Nextcloud operate under a formal change control process?**	All changes to Nextcloud software have to pass a review process. These are performed in the Public on GitHub and enforced technically, to have a change merged into Nextcloud software a Pull Request on GitHub has to be filed. The Pull Request has then to be reviewed by at least two other persons that have been granted approval to merge requests. Only if that has passed as well as successful unit- and integration tests then can the Pull Request can be merged. Currently 39 different unit- and integration workers are triggered. These limitations are enforced technically. It is thus not possible to bypass these limitations, except for administrators of the GitHub organisation. Every action on GitHub is logged within GitHub's audit log.	🟩	Nextcloud undertakes a review process on all aspects of change, this process includes a risk assessment, analysis of the impacts of changes and specification of security controls needed. Nextcloud should continue to mature the change control policy & procedures with the following aspects considered: - maintaining a record of agreed authorisation levels; - ensuring changes are submitted by authorised users; - reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; - identifying all software, information, database entities and hardware that require amendment; - identifying and checking security critical code to minimise the likelihood of known security weaknesses; - obtaining formal approval for detailed proposals before work commences; - ensuring authorised users accept changes prior to implementation; - ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of; - maintaining a version control for all software updates; - maintaining an audit trail of all change requests; - ensuring that operating

SO27001-2013 Control 14.2 - Security in development and support processes. Objective: To ensure that information security is designed and implemented within the development lifecycle of systems.				
Ref.	**ISO27001:2013 Requirement**	**Findings**	**RAG**	**Additional Assurance Information**
			🟩	documentation (see further ref at ISO27001 – **Control 12.1.1**) and user procedures are changed as necessary to remain appropriate; - Ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.
A.14.2.3	**Technical review of applications after operating platform changes -** Is there a process within Nextcloud to ensure a technical review is carried out when operating platforms are Changed?	Nextcloud performs automated unit and integration tests against a different set of operating systems. This makes it possible for Nextcloud to detect when a breaking change has been detected.	🟩	Nextcloud should continue to develop and mature their procedures if and when operating platforms are changed, this includes reviewing business critical applications including testing to ensure there is no adverse impact on organisational operations or security. This process should cover: - review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes; - ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation; - Ensuring that appropriate changes are made to the business continuity plans.

A.14.2.4	**Restrictions on changes to software packages -** Is there a policy in place which mandates when and how software packages can be changed or modified.	Nextcloud software packages are stored on the "download.nextcloud.com" system and signed using GPG. The GPG key is stored on a dedicated system that is used solely for signing releases. Third-party and Nextcloud's own apps released on "apps.nextcloud.com" are all signed by a X.509 certificate belonging to the developer. The certificate is issued by the "Nextcloud Code Authority" authority and bound to a specific app. The Nextcloud server component verifies whether the downloaded TAR file has been signed by the appropriate certificate. Only very limited authorised personnel have access to the signing, root authority and download server. Those are all dedicated and managed systems.	🟩	Nextcloud understands that modifications to software packages are controlled and limited to necessary changes where all changes are to be strictly controlled. Nextcloud are maturing their policy to modification and changes to software. Policy should mandate where as possible and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered: - the risk of built-in controls and integrity processes being compromised; - whether the consent of the vendor should be obtained; - the possibility of obtaining the required changes from the vendor as standard program updates; - the impact if the organisation becomes responsible for the future maintenance of the software as a result of changes; - Compatibility with other software in use. If changes are necessary the original software will be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorised software (see further detail at ISO27001 **Control 12.6.1**). All changes should be fully tested and

SO27001-2013 Control 14.2 - Security in development and support processes. Objective: To ensure that information security is designed and implemented within the development lifecycle of systems.				
Ref.	ISO27001:2013 Requirement	Findings	RAG	Additional Assurance Information
			🟩	documented, so that they can be re-applied, if necessary, to future software upgrades. Where applicable modifications should be tested and validated by an independent evaluation body.

A14.2.5	**Secure system engineering principles -** Does the organisation have documented principles on how systems must be engineered to ensure security.	Details about Nextcloud security processes can be seen at https://nextcloud.com/secure/ and https://nextcloud.com/security This shared area provides up to the minute latest advice and guidance on the security environment including Nextcloud threat modelling ideology and how to understand common security problems and how to prevent them.	🟩	Nextcloud communicate its Control Principles on the internet. The information provided is wide and varied and succinct in detail to the security aspects of the solution. The Nextcloud business is also in parallel maturing its organisational governance framework and associated policy environment this covers developing the engineering principles to secure systems which cover documented aspects of how systems are maintained and the relevant security layers are applied. These engineering procedures should ensure they are based on the following key areas; - The engineering principles are established, documented and applied to in-house information system engineering activities. - Security should shall be designed into all architecture layers (business, data, applications and technology) balancing thus balancing the need for information security with the need for accessibility. - New technology should be analysed for security risks and the design should be reviewed against known attack patterns. These above principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the

<table>
<tr><th colspan="5">SO27001-2013 Control 14.2 - Security in development and support processes.
Objective: To ensure that information security is designed and implemented within the development lifecycle of systems.</th></tr>
<tr><th>Ref.</th><th>ISO27001:2013 Requirement</th><th>Findings</th><th>RAG</th><th>Additional Assurance Information</th></tr>
<tr><td></td><td></td><td></td><td>🟩</td><td>engineering process.</td></tr>
</table>

A14.2.6	**Secure development environment -** Has a secure development environment been established.	Nextcloud is an open-source company as such they do not have issues with potential loss of intellectual property in relation to the Nextcloud source code. All Nextcloud software is freely available. In terms of development: All developers use their own installations for testing. At no point is sensitive testing performed on company owned production hardware. Nextcloud solution demonstration (demo) installation runs on Nextcloud dedicated hardware in a third-party data centre. The demo server is totally air-gapped and not connected to Nextcloud infrastructure. In terms of production: Nextcloud does not have any control over production instances as Nextcloud are only providing the software. Nextcloud highlight that all projects utilise the secure development environment appropriately during the system development lifecycle.	🟩	What is in scope here is not just the source code itself but the Nextcloud development, operational governance and support framework environment. These aspects may also be considered in scope by some larger customer enterprises and going forward ultimately the certification bodies in that process and procedures which includes people, processes and technology are deemed to be all associated with the system/solution directly or indirectly which cover the entire systems/solution development lifecycle. Whilst all projects follow appropriate working standards within the development lifecycle environment it is important to document the lifecycle framework as such; Nextcloud should assess risks associated with individual system development efforts and establish and document secure development environments for specific system development efforts, the key areas for consideration would be; - applicable external and internal requirements, e.g. from regulations or policies; - security controls already implemented by the organisation that support system development; - trustworthiness of personnel working in the environment; - the need for segregation between different development environments;

SO27001-2013 Control 14.2 - Security in development and support processes.
Objective: To ensure that information security is designed and implemented within the development lifecycle of systems.

Ref.	ISO27001:2013 Requirement	Findings	RAG	Additional Assurance Information
			🟩	- control of access to the development environment; - monitoring of change to the environment and code stored therein; Once the level of protection is determined for a specific development environment, Nextcloud should document corresponding processes in secure development procedures and provide these to all individuals/groups who need them.
A14.2.7	**Outsourced development -** Where development has been outsourced is this supervised - Is externally developed code subject to a security review before deployment?	Nextcloud GmbH does not outsource any development. However, as an open-source company Nextcloud regularly receives code submissions from third-parties. These code submissions have to pass through the same review process as code developed by Nextcloud employees. All code submissions follow the same review process. While not all code is reviewed initially before merge by a member of Nextcloud security team, all security relevant commits (git commits) are. Before releases of new major releases Nextcloud perform extensive security checks. Including dynamic (Burp Suite), static (Veracode) and manual security testing and code reviews.	🟩	Where system development is considered as third party comes into Nextcloud for review then the points to be considered at **14.2.6 Secure development environment** above should ensure that security and related consistency exists across the entire supply and internal development chain.

A14.2.8	**System security testing - Testing of security functionality should be carried out during development.** Where systems or applications are developed, are they security tested as part of the development process?	Nextcloud does separate between systems that are exposed to customer data (e.g. Nextcloud support system, or Nextcloud file sharing instance) and public systems (e.g. Nextcloud public help forum). **Customer data systems -** - Are subject to and have to pass a Nessus scan successfully - Have to pass a 2 work day manual penetration test by members of Nextcloud the security team; - Checked for assurance against the OWASP Top 10 vulnerability discovered within the first two days of testing; - Have to pass an automated scan using Burp Suite; - Have defined security contacts on their website; **Public systems -** - Have to pass a Nessus scan successfully - Have to pass an automated scan using Burp Suite - Checked for assurance against the OWASP Top 10 vulnerability discovered using Burp Suite All results are verified and triaged by members of the Nextcloud security team. Nextcloud does not perform automated code analysis on third-party software. However, Nextcloud does host Nextcloud own sensitive files on their internal Nextcloud instance which is subject to static analysis using Veracode and Coverity as well as manual penetration testing and dynamic analysis using Burp Suite.	🟩	The extent of testing is well defined and is considered meeting industry standards. Testing is undertaken in proportion to the nature of the system.
A14.2.9	**System acceptance testing**	All publicly facing systems of Nextcloud GmbH that	🟩	System acceptance testing is in

SO27001-2013 Control 14.2 - Security in development and support processes.
Objective: To ensure that information security is designed and implemented within the development lifecycle of systems.

Ref.	ISO27001:2013 Requirement	Findings	RAG	Additional Assurance Information
	- Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. A requirement to have in place an established process to accept new systems / applications, or upgrades into production use.	Nextcloud run has to have a positive security track record as well as pass several security tests including being part of Nextcloud Bug Bounty Scope on HackerOne programme. Testing is performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the Nextcloud environment. Using dynamic analysis using Burp suite: Initial testing is performed within virtual machines on the testing members' own device. Since deployment is performed using Ansible the resulting deployed package is similar to what the analyst has in their virtual machine. Network scanning: Nessus scans are performed against the actual server environment. Rescans are scheduled bi-monthly. All systems that are not intended for public usage will be either protected using Basic Authentication or by being only available from the companies intranet.	🟩	adherence to secure system development practices. The testing regime is considered reliable and is performed in a realistic test environment to prevent vulnerabilities to the organisation's environment.
A14.3	**Test data - A14.3.1 - Protection of test data.**	Nextcloud do not perform testing using any customer data. Nextcloud perform testing of releases including real life scenarios manually on a staging server using a copy of Nextcloud own internal installation of Nextcloud server software.	🟩	None.

Table 1 Findings and Observations / Recommendations

2 Governance, Industry standards and best practices

The following section provides an overview of Nextcloud alignment to industry standards and best practices within its service; in essence this looks at People and processes around Governance and adoption of best practice.

2.1 Governance

It is important that assurance of the Nextcloud solution in terms of its source code and the solutions technical standing at any point in time is maintained from a technical risk perspective. This is achieved by processes and procedures undertaken through system security and acceptance security testing frameworks as highlighted in the findings and recommendations table 1 with reference to **14.2.8** and **14.T2.9** respectively. This ultimately provides evidence of assurance by validation to those risk owners and managers within the Nextcloud solutions consumer market.

Equally as important to the technical and service environment is Nextcloud's commitment to implementing and maintaining high standards of design, processes and industry best practices. This is achieved at a foundation level by implementing core strategic Governance pillars. Industry recognises two key elements for good governance, these are the identification and secondly; the mitigation of risks. Good Governance frameworks are built around adopting operational best practices and alignment or certification to industry standards. The table below provides an overview of the current Nextcloud governance position and where applicable recommendations are made.

2.1.1 Nextcloud principles of Governance

Industry standards & best practice	Nextcloud Status	RAG	Recommendations
Governance Framework ideology: The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service.	Nextcloud are a new organisation and is considered within industry terms a fork of the previous own Cloud project. Whilst Nextcloud as a business entity are in their infancy they are setting in place the building blocks and establishing a framework for good governance around its SDLC and wider business processes. This Governance framework is adopted by Nextcloud stakeholders supported by Seniors whom are championing the cause at board level. There is firm realisation and commitment within the Nextcloud stakeholder group that the business needs to understand what governance is and what benefits it brings to the organisation. Simplistically put Nextcloud understands that good governance ultimately wins the hearts and minds of the customer.	🟩	Nextcloud must continue to mature the strategic governance framework to ensure they have a sound system of internal control and effective risk management processes which the board should review regularly. To support the strategic approach it would be advisable for Nextcloud to align or gain certification to industry standards such as ISO17799, ISO27002, NIST, SANS standards, using best practices associated with for example; ITIL or Microsoft trust centre, this will provide a Nextcloud corporate wide risk management framework, that contains a detailed set of controls that satisfies the assurance requirements for the consumers of Nextcloud.

		🟩	Whilst the Nextcloud business function is still maturing it is recommended that Nextcloud consider certification on a scaled part of the Nextcloud services. Diagram 1 provides an overview of what a proposed scope of certification may look like. Ultimately sound governance and risk management principles within the organisation will ensure the continuity of the organisation's business and existence.

Table 2: Principles of good Governance

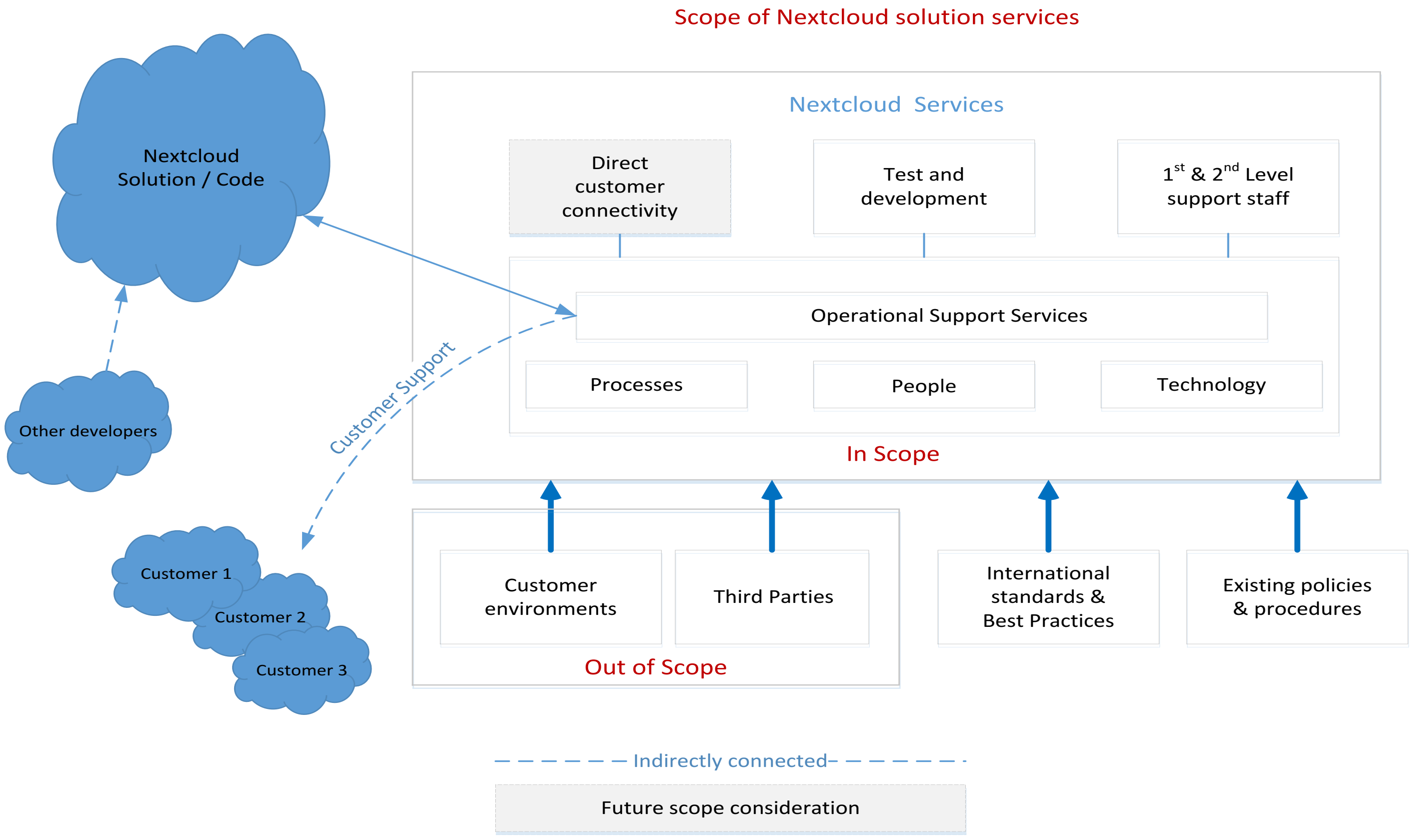
Scope of Nextcloud solution services
Nextcloud Services
Direct customer connectivity
Test and development
1st & 2nd Level support staff
Operational Support Services
Processes
People
Technology
In Scope
Nextcloud Solution / Code
Other developers
Customer Support
Customer 1
Customer 2
Customer 3
Customer environments
Third Parties
Out of Scope
International standards & Best Practices
Existing policies & procedures
Indirectly connected
Future scope consideration

Diagram 1: Nextcloud considered scope of services

2.1.2 Nextcloud Best Practices - Systems Development Lifecycle (SDLC)

Industry standards & best practice	Nextcloud Status	RAG	Recommendations
The systems development life cycle (SDLC), also referred to as the application development life-cycle, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.	Nextcloud follow a systems development water-flow based model as highlighted in their security-architecture document, the key phases include; - **Training** – Nextcloud have routine onsite training for their Engineers with a prime focus on application security. For this purpose Nextcloud have developed internal training material such as a Nextcloud application that is not using the security protections that the platform is offering by default as well as training and education related to industry related security issues which includes the common OWASP Top 10 vulnerabilities (https://github.com/LukasReschke/supersecureenterpriseapp) In addition, Nextcloud provide DVWA (Damn Vulnerable Web Application) as part of the training programme where members of the Nextcloud security team are asked to work collectively to solve the challenges in co-operation with Nextcloud engineering personnel. **Requirements / Design** - As an open-source company defining requirements for every feature can be challenging. Especially considering community contributions. However, history shows that nearly all of the bigger changes are mainly driven forward by employed Nextcloud personnel. For those cases, Nextcloud hold on-site meetings for all Engineers every 2 - 3 months for 1 to 2 weeks which are programmed to focused on: - Defining the feature set of the next release together with product management;	🟩	Whilst Nextcloud do not yet have a fully matured SDLC suite in place the current development lifecycle processes and phases that the design, engineering and security teams work to are carried out in line with key SDLC principles. The primary target here will be to define, document and mature the SDLC model.

	- Defining technical quality bars for a feature and a MVP (Minimum viable product); - Discuss technical implementation details; - Assess security risks and potential threats as well as implement mitigations for those. **Implementation** - Nextcloud runs several static source code analysers, self-developed as well as proprietary external software. These include, but are not necessarily limited to: - AppCode Checker to check for forbidden and potential unsafe functions in the source code; - Veracode and Coverity scans to statically check the source code for security vulnerabilities. Those scans are performed within different stages of the development and results reviewed and triaged by members of the Nextcloud security team. **Verification / Release** - Nextcloud perform dynamic fuzz testing using the Burp Suite software. Manual security testing is performed as well before every release by members of the Nextcloud security team. Nextcloud also run a bug bounty program at hackerone.com/nextcloud offering up to $5,000 for security vulnerabilities and also include pre-release software in the scope. (e.g. alpha, beta and release candidates)	🟩	

Table 3: Nextcloud Systems Development Lifecycle (SDLC)

3 Nextcloud Security Features Edition 11

3.1 Background

In line with Nextclouds existing software development programmes Nextcloud are to introduce a number of new security features and security enhancements to existing security controls. Nextcloud 11 is to be released in December 2016 and will present further security enrichment in its design and technology that will provide product assurance to all its customers

The following section provides an assessment of the new security features.

3.1.1 Approach

Industry demands and expects secure products and services. As business moves more and more into consuming cloud and/or of the shelf premise based products and services the associated risks then exist primarily within the supply chain. The supply chain in effect then presents unknown risks where the consumer does not have direct control or influence on the supplier's assurance frameworks. Because of the unknown risk factor the customers risk owners in all probability will now want to validate supply chain assurance based on the supplier's certifications and assertions of the service. Given the stakes are high in terms of compromise of customer environments either by direct or in-direct association the consequences of association can be very damaging indeed. Accidental or malicious compromise can lead to reputational damage, legal implications including fines. Thus the demands of meeting or aligning to standards and compliance within the supply chain is a key consideration for all parties.

Whether the product is an application, a network, a managed service, software or infrastructure services the fundamental requirements are building secure technology supported by good processes and sound governance. This review process looked at all the new Nextcloud 11 security features not only in isolation but also collectively as aggregated defense mechanisms that look to provide a strength in depth approach to security. The review process looked at aligning the features against varying standards and best practices used across industry, using the ISO27001 standard as the baseline control set and subsequently cross referenced with other related standards, guidance and security principles. The table below highlights a few of these standards and principles.

3.1.2 Reference Documents & Industry Standard Guidance

Ref No	Document Title
[1]	Cloud Security Guidance: Cloud Security Principles, (NCSC)
[2]	Cyber Security controls – many institutes' standards reviewed - NSA, NIST, and Microsoft.
[3]	UK National Cyber Security Centre (NCSC)
[4]	ISO27001-2013
[5]	ISO27002-2013
[6]	Nextcloud supporting policies and procedures library of documents (provided by Nextcloud)

3.1.3 Findings and Recommendations

The Nextcloud 11 solution is built around combined assurance layers consisting of newly applied rich security features, applied best practices which are governed by policy and the design itself validated by industry standard testing processes. Following the security review of the new security features being deployed it was considered that each feature including by aggregation by association will enhance the security standing of the Nextcloud 11 solution.

The key below represents the association with best practices and standards by a simple RAG status as detailed below.

🟩	Accept	Best practices and Standards are being applied
🟥	Action	Best practices and Standards are not applied
🟨	Treat	Areas in need of review and recommended updates

3.1.4 Summary of Key findings

RAG	Finding
🟩	Security features have been chosen well to complement the existing security architecture within the design – The features adopt good industry standard controls and will enhance the general standing of the security working environment.
🟨	Whilst recommendations are made (listed below) there are no immediate issues found either in isolation or collectively that need to be marked as 'to be reviewed and treated' to achieve alignment and compliance.

Table 4: High level summary of findings.

The following list of recommendations and associated key activities will help provide robust assurance to the overall security environment;

- Develop a High Level Design Document (HLD) that includes basic information around security and process – (In doing so this provides consistency in security design, the HLD should exist as a living document and be reviewed routinely to ensure that emerging threats and risks are considered within the future design and next editions);
- Look to adopt and align to an international security management standard;
- Ensure all key security features are subject security testing, and all risks documented and formally mitigated within a corporate Risk Treatment Plan.

3.1.5 Detailed Findings and Assurance Comments

The table below provides details of the each of the new security features being deployed within Nextcloud 11. Assurance comments are made against each feature and where appropriate additional assurance statements for future consideration are made.

Nextcloud 11 - New and improved security features

Ref.	Security features defined	RAG	Additional Assurance Information
1	**Two Factor Authentication** - Nextcloud 11 brings two officially supported two-factor providers to the customers Nextcloud server. While Nextcloud 10 has already introduced the backend APIs for Two-Factor Authentication, the Nextcloud release finally lowers the barrier for using a second factor provider by offering several default providers. Support for the following factors has been added:- - **Universal 2nd Factor (U2F)** – UTF is an open standard that allows authentication using a hardware security key such as the Yubikey. Once U2F has been enabled users will need to plug in their U2F security key into their computer to successfully login. - **Time-based One-Time Password (TOTP)** - TOTP is an open standard that allows authentication by providing a security number in addition to the regular credentials to successfully authenticate. In the event that a user has lost his/her second factor item, administrators can undertake a secure reset. Users can also generate backup codes in the personal settings of their Nextcloud. For more specific requirements (such as enforcing a second-factor) organisations can use the extensive public API that Nextcloud provide for hooking in second factor providers. For authenticating with clients Nextcloud supports application specific passwords that can be generated by users.	🟩	Authentication – As the business world and the electronic marketplace become more complex, the advantages of authentication are ever more obvious. Many successful attacks are more often than not down to poor system management especially around weak access control mechanisms within infrastructure. It is therefore important to use tried and tested methods of access in order to validate the user's right to access the system and information. Both U2F and OTP authentication mechanisms if applied and managed accordingly are considered secure industry standards authentication practices. - U2F – Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies two-factor authentication using specialized USB or NFC devices based on similar security technology found in smart cards. Initially developed by Google and Yubico, with contribution from NXP, the standard is now hosted by the FIDO Alliance. FIDO Alliance is an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices and the problems users face creating and remembering multiple usernames and passwords -

Nextcloud 11 - New and improved security features

Ref.	Security features defined	RAG	Additional Assurance Information
		🟩	- One-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTP avoids a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).
2	**Same-site cookies support** - The Same-site cookie support in Nextcloud 11 has been hardened even further. This hardening further strengthens the security measure supported by modern browsers that prevent CSRF vulnerabilities and protect your privacy further. Browsers that support same-site cookies can be instructed in a way to only send a cookie if the request is originating from the original domain. This makes exploiting CSRF vulnerabilities from other domains a non-issue. Also timing attacks, such as enumerating whether a specific file or folder exists, are not feasible anymore. Nextcloud enforces the same-site cookies to be present on every request by enforcing this within the request middleware. As a further hardening element, within Nextcloud 11 Nextcloud have added the __Host prefix to the cookie if the environment supports this feature. This enforces the cookie to be only sent via HTTPS and only be sent only to the host that has set this cookie. This mitigates cookie injection vulnerabilities within potential third-party software sharing the same second level domain. Note that Nextcloud does also employ regular protections against CSRF such as a shared secret between browser and client. More technical details about the original implementation can be read at https://statuscode.ch/2016/06/security-and-nextcloud-9/.	🟩	Same-site cookies are applied to provide additional security against information-leakage and CSRF attacks. Validation of configuration should be included in the penetration testing scope undertaken by accredited suppliers.

Nextcloud 11 - New and improved security features

Ref.	Security features defined	RAG	Additional Assurance Information
	XSS - The primary protection against XSS is output encoding. Nextcloud do however protect against XSS using Content Security Policy (see Ref.6). **XSSI** - Nextcloud generally don't dynamically generate JS files. There is one that is however phased out already. In XSSI cases Nextcloud Same Site Cookies do help because another site cannot simply embed Nextcloud dynamically generated files. (those don't have caching headers and require the "strict" Cookie to be sent – thus other pages can't include it via <script>)	🟩	
3	**Password confirmation for sensitive actions (e.g. when changing email or passwords)** - Nextcloud 11 has added support for password confirmation on security critical actions. If an administrator or regular user is trying to change a potential sensitive setting (such as changing the permissions of a user) they will have to provide their password a second time to verify the action. Password verification is only required once every 30 minutes. After 30 minutes have been passed after the last verification the user using their original login details will have to re-verify their identity if they make a security-sensitive change. Password complexity - depends on the adapter used (but must still meet best practice). Enterprise environments mainly LDAP is used thus that environment can benefit from internal password policy tools already in place. For smaller environments with local users Nextcloud do have a small password complexity check. This should be aligned with the new NIST recommendation https://protect-eu.mimecast.com/s/vQzABi0r6lTZ **Monitoring** - In Generally not all sensitive actions are monitored. (E.g. changing the mail address of a user is not). Currently the following events are logged (independently whether they require a password confirmation or not): **Authentication** - Successful and invalid login attempts - Logout **Files; -** Read – Renamed – Created – Copied- Written – Updated and deleted Sharing - File shared - File unshared - File permissions updated – **File password updated - File expiration updated** - **Public share accessed** **Trash bin -** File deleted - File restored	🟩	The design highlights that technical controls are to be put in place to enforce and monitor administrators actions specifically those changes that are considered security related within the solution further enhancing security controls to those also presented at Ref. 4 especially: - Using throttling, and/or protective monitoring; - blacklisting the most common password choices; - Logs should be reviewed and audited routinely in line with policy;

Nextcloud 11 - New and improved security features

Ref.	Security features defined	RAG	Additional Assurance Information
	Versioning - Version restored - Version deleted **Event Logs** - All logs are stored by default in the “nextcloud.log” file on the filesystem. Administrators can configure using a syslog or remote syslog service to have the logs stored on a remote environment.	🟩	
4	**Bruteforce protection -** The bruteforce protection implemented in Nextcloud protects against bruteforce attacks against potentially sensitive endpoints. It currently works by throttling all login requests coming from a specific subnet. This means, if an IP has triggered multiple invalid login attempts future authentication requests from that subnet will be slower for the next 24 hours. (up to 30 seconds delay) In Nextcloud 11 the bruteforce protection has been hardened by protecting even more endpoints against potential bruteforce attacks. This includes some endpoints of the OCS Person API as well as the newly added password confirmations. A specific API endpoint in previous Nextcloud versions before version 11 did not implement the brute-force protection, this was partly by purpose (e.g. keep clients compatible). That endpoint has been adjusted and tested to ensure that clients won’t have any problems when trying to use that endpoint. Now that endpoint is also protected using Brute Force Protection. **User operability** – Currently there is no account lockout as there is considered trade-off between usability and accessibility. Currently options for this particular feature are being considered for future release. However Administrators can however configure a lockout themselves if they use an authentication mechanism like LDAP. In that case once the account is locked by the Active Directory for having too many invalid login attempts also the Nextcloud account will be locked. **Monitoring** - every bruteforce attempt is logged in the “nextcloud.log” file. Administrators can access these either using the Nextcloud Log Viewer interface or by feeding the log into Protective Monitoring software such as Splunk or ELK to monitor and filter the log events themselves.	🟩	Remarkably Brute-force attacks are somewhat difficult to stop completely, but by careful design and multiple countermeasures, this can limit exposure to these attacks. Ultimately, one of the best defence is related to people security which is to make sure that users follow basic rules for strong passwords: Use long unpredictable passwords, avoid dictionary words, avoid reusing passwords, and change passwords regularly. The Nextcloud security team has implemented a combination of good working practices to minimise the attack vector. For future reference Nextcloud could consider Bruteforce considered good protection methods, to include; - Account lockout and ‘throttling’ are effective; - Password blacklisting works well in combination with lockout and/or throttling. - Protective monitoring is also a powerful defence against brute-force attacks, and offers a good alternative to account lockout or throttling.

Nextcloud 11 - New and improved security features

Ref.	Security features defined	RAG	Additional Assurance Information
5	**Use HTTPS by default if no protocol is given** - Nextcloud supports so-called federated cloud shares (following the Open Cloud Mesh project). This means that users of different instances can share files with each other by providing their federated cloud ID. (e.g. john@cloud.doe.com) The instances will then communicate using the OCM protocol and establish a share connection. Before Nextcloud 11 the server would first try to establish a HTTPS connection and if that failed the connections failback would be to HTTP without any user feedback. Thus allowing potential man-in-the-middle attacks. Realizing that HTTPS is now easier than ever using projects such as LetsEncrypt Nextcloud are now enforcing HTTPS unless a user manually decides to share with a HTTP instance. (by providing http://john@cloud.doe.com as federated cloud ID)	🟩	While data in transit as well as data at rest may have slightly different risk profiles, the inherent risk hinges primarily on the sensitivity and value of the data; attackers will attempt to gain access to valuable data whether it's in motion, at rest, or actively in use, depending on which state is easiest to breach. That's why a proactive approach being adopted by Nextcloud using appropriate security protocols is the safest and most effective way to protect the most sensitive data in every state.
	Application specific tokens can be forbidden file system access - To authenticate against their Nextcloud users can now also use tokens instead of their password that have specific limitations enforced. As a first step Nextcloud have added support for limiting file system access. This allows users now to connect their potentially less trusted third-party clients (e.g. a mobile phones calendar) without exposing access to the whole filesystem.	🟩	This layer of Nextcloud 11 security is built on the key principle of three most common authentication elements which are often described as 1) something you know (the knowledge factor), 2) something you have (the possession factor) and 3) something you are (the inherence factor). This concept meets industry standards.
6	**Content Security Policy v3.0 Support (with nonce instead of "self" for script-src)** –Basically what Nextcloud CSPv2.0 does it informs browsers: "*Do not execute any scripts except those served from the same domain*". So if the cloud runs on https://protect-eu.mimecast.com/s/bJO1BuRL6Vcl, only JS from https://protect-eu.mimecast.com/s/bJO1BuRL6Vcl can be executed. This enhances the security of XSS vulnerability because any potential attacker would need to include resources from "https://protect-eu.mimecast.com/s/bJO1BuRL6Vcl". However, there are some endpoints where user files are served (such as via Nextcloud WebDAV endpoint) and those are on the same domain. While most browsers support the "nosniff" directive some browsers do not. (e.g. Firefox just added support last month) With the "nonce" directive Nextcloud tell the browser to only execute JS files if they have the proper nonce. This means the <script> tag contains the allowed nonce like: <script src="/foo" nonce="SharedSecretLongNonce">. If that one	🟩	The Nextcloud security team has set out to implement the primary objective of CSP (Content Security Policy) which is to mitigate and report XSS attacks. XSS attacks exploit the browser's trust of the content received from the server. Malicious scripts are executed by the victim's browser because the browser trusts the source of the content, even when it's not coming from where it seems to be coming from. CSP makes it possible for server administrators to reduce or eliminate the vectors by which XSS can occur by specifying the domains that the browser should consider to be valid sources of executable

Nextcloud 11 - New and improved security features

Ref.	Security features defined	RAG	Additional Assurance Information
	isn't provided the JS is not executed. Effectively, this hardens the CSP policy more for browsers that don't support the no-sniff directive.	🟩	scripts. A CSP compatible browser will then only execute scripts loaded in source files received from those whitelisted domains, ignoring all other script (including inline scripts and event-handling HTML attributes). As an ultimate form of protection, sites that want to never allow scripts to be executed can opt to globally disallow script execution. The Nextcloud security team should ensure that policy is described using a series of policy directives, each of which describes the policy for a certain resource type or policy area.
7	Improved password reset logic - As a further hardening to the general platform Nextcloud 11 will apply a more astute password reset mechanism. Previously reset tokens where simply valid for 12 hours. The new password reset logic invalidates the password also after critical information such as the user mail address has been changed.	🟩	Follows good password security principles as applied across industry.

It is noted that not all security features are enabled by default in the case of Two Factor Authentication function – this feature has to be enabled and configured by the administrator. The following two features are set as default, but can be disabled by administrators, these are;

- Bruteforce protection (can be disabled via config flag)
- Password reset (will be disabled if another backend such as LDAP is used)

Annex ‘B’ Nextcloud Assurance Statement

Nextcloud 11

Assurance Statement

Background

One of Nextcloud's key objectives is to maintain a high level of customer confidence by continually assessing the security controls in place that would be expected of any organisation providing this type of service. Nextcloud has dedicated security experts continuously working with the Nextcloud solution and supporting service to ensure that the security features designed and deployed provide the appropriate security layers to mitigate risk from the most common security problems.

The Nextcloud edition 11 provides many new security related features (Full list below), such as enhancement of Access Controls, data in transit protection, strengthening of password logic. All of which enrich the Nextcloud servers security layers with minimum impact on the user.

These Security layers are designed, built and deployed on industry standards using Secure-Software Development Lifecycle processes and best practice ideology.

Security features for the new Nextcloud 11 release are;

- Two Factor Authentication using U2F / TOTP	✓
- Bruteforce protection	✓
- Content Security Policy v3.0 Support (with nonce instead of "self" for script-src)	✓
- Same-Site cookies support	✓
- Password confirmation for sensitive actions (e.g. when changing email or passwords)	✓
- Same-Site cookies are prefixed with __Host	✓
- Improved password reset logic	✓
- Use HTTPS by default if no protocol is given	✓
- Application specific tokens can be forbidden file system access	✓

Table 1: Nextcloud 11 Security Features

Assurance

Many consumers when considering new web-services, premise or Cloud hosted applications, IaaS (infrastructure), SaaS (Software), private or public Cloud services etc. will decide which key principles of assurance are important, and how much (if any) assurance they require in the implementation and consumption of these services. Nextcloud understands the necessity to provide core principle baseline security requirements, as such Nextcloud 11 is built on these security principles to ultimately deliver a secure solution to their customers.

Risk Management

Risk is assessed by Nextcloud based on current industry standards such as Clause 14 of ISO/IEC27001-2013 and key security principles that are common to many services such key Cloud Security principles. From a technical perspective Nextcloud 11 is subject to in-house Vulnerability Management and routine independent penetration testing using industry certified suppliers. There are also independent reviews of Operational Security and Governance related to Nextcloud's design and includes reviewing policy, process and related procedures.

Nextcloud has assessed the threat against three core areas, as highlighted below; the principle control areas are presented in Table 2 below;
1 - People - i.e. Customers / consumers, Nextcloud internal users and external users, hackers; developers;
2 - Technology - attacks designed to exploit vulnerabilities in software; the design;
3 - Environment - take advantage of weaknesses in poor management, and weak governance in order to compromise the service.

Principle;	**Control area;**
ISO/IEC27001:2013;	- Secure Development Policy. - System Change Control procedures. - Technical review of applications after operating platform changes. - Restrictions on changes to software packages. - Secure system engineering principles. - Secure development environment. - Outsourced development. - System security testing. - System acceptance testing.
Cloud Security Principles	- Data in Transit. - Protection and resilience in the design. - Governance framework. - Operational Security. - Secure development. - Personal security. - Identity and Authentication. - Secure service administration.
Independent testing	- Validation of application and services.

Table 2: Baseline industry standards and Security Principles

Nextcloud Assertions

Nextcloud makes the following services assertions based on ensuring the Confidentiality, Integrity and Availability of the Nextcloud solution and service. Whilst Nextcloud does not process or host any customer data Nextcloud is aligned to the Legal and compliance requirements of the EU GDPR Data Protection legislation.

Common approaches to assurance provide a number of means by which the “level” or “strength” of assurance can be assessed. These approaches are described in the following areas.

Nextcloud Service Provider Assertion

Nextcloud understands that consumers are reliant on the honesty, accuracy and completeness of the service provider’s assertions. Nextcloud assurance is based on:

- *A good level of maturity around security;*
- *The existence of in-house security team members and stakeholders;*
- *Proactive testing and historical evidence of responding to and managing security issues.*

Independent Validation of Nextcloud Assertions

An independent third party reviews and confirms the Nextcloud assertions.

- *NCC Group have conducted a review of Nextcloud alignment to core principles of security based on the Security Principles (detailed in Table 2).*
- *Independent ‘Penetration tests’ by Veracode have been conducted and all risks mitigated and managed in accordance with Nextcloud policy.*
- *Internal Vulnerability scanning and risk management*

Certification and implementation of controls reviewed by a qualified individual(s).

Suitably qualified individuals will review the scope of the applied security controls. This approach provides a higher degree of confidence that the service meets the stated objectives through alignment against an appropriate standard.

Independent Testing of Implementation

Testing supply chain used has appropriate industry recognised certification and qualifications for the testing they are carrying out. Nextcloud understands that Independent testing provides confidence that the design, service implementation achieves the objectives and reduces the reliance on supplier assertions. The results of testing reflect the design, service at a particular moment in time; routine testing is undertaken including testing as the service evolves.

Assurance in the service design

Nextcloud employing certified Architects to provide confidence in the design (and implementation of its recommendations) will give confidence that:

- *the design and security features defends against common attacks;*
- *the proposed security controls are appropriate;*
- *The proposed architecture would allow effective secure operation of the service.*
- *The solutions design will be subject to on-going independent penetration tests by an approved accredited company.*

End of Statement