**Information Systems Audit Plan**

System(s) to be audited:  
Northwood Naturals

|  |  |
| --- | --- |
| DOCUMENT CLASSIFICATION | FOUO |
| DOCUMENT REF | ISMS-DOC-A05-35-1 |
| VERSION | 1 |
| DATED | [Insert date] |
| DOCUMENT AUTHOR | Kevin Bacon |
| DOCUMENT OWNER | CISO |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | REVISION AUTHOR | SUMMARY OF CHANGES |
| 1.0 | 03/12/24 | Kevin Bacon |  |
|  |  |  |  |
|  |  |  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | POSITION | SIGNATURE | DATE |
| Gage Radtke | CEO | - | 06/12/2024 |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Introduction 8](#_Toc68876887)

[2 Information systems audit plan 9](#_Toc68876888)

[2.1 Audit scope 9](#_Toc68876889)

[2.2 Audit criteria and reference documents 9](#_Toc68876890)

[2.3 Audit methods 10](#_Toc68876891)

[2.3.1 Review 10](#_Toc68876892)

[2.3.2 Technical audit tests 10](#_Toc68876893)

[2.3.3 Additional processing 11](#_Toc68876894)

[2.4 Resources required 11](#_Toc68876895)

[2.4.1 Audit team 11](#_Toc68876896)

[2.4.2 Business resources required 12](#_Toc68876897)

[2.4.3 System access requirements 12](#_Toc68876898)

[2.4.4 Contacts 13](#_Toc68876899)

[2.5 Audit schedule 13](#_Toc68876900)

[2.5.1 Day one 13](#_Toc68876901)

[2.5.2 Day two 14](#_Toc68876902)

[2.6 Communication of findings 14](#_Toc68876903)

Tables

[Table 1: Audit scope 9](#_Toc68876904)

[Table 2: Information systems to be audited 9](#_Toc68876905)

[Table 3: Applicable legal and regulatory requirements 10](#_Toc68876906)

[Table 4: Technical audit tests 10](#_Toc68876907)

[Table 5: Additional processing 11](#_Toc68876908)

[Table 6: Audit team 11](#_Toc68876909)

[Table 7: Business resources required 12](#_Toc68876910)

[Table 8: Systems access requirements 12](#_Toc68876911)

[Table 9: Onsite contacts 13](#_Toc68876912)

[Table 10: Audit schedule day one 13](#_Toc68876913)

[Table 11: Audit schedule day two 14](#_Toc68876914)

# Introduction

In addition to an external audit programme carried out by the certification body, the internal audit team also carries out a programme of regular audits in order to verify operational systems and identify any security risks or issues that need to be addressed.

The objectives of this internal audit programme are:

* To verify that correct inputs to the information system result in the correct processing and outputs in line with business requirements
* To ensure that information security processes are carried out effectively, efficiently and economically with respect to the information system
* To identify further opportunities for continual improvement
* To provide N**orthwood Natural**s with internal assurance that information security is effectively managed and risks to the business are minimised

The purpose of this document is to set out a plan for an audit of the Information System within Northwood Naturals on 06/12/2024.

# Information systems audit plan

## Audit scope

This audit will cover the following business areas and processes within the organization:

|  |  |  |
| --- | --- | --- |
| BUSINESS AREA | LOCATION | BUSINESS PROCESSES |
| Supply Chain | Waukesha, Wi, USA | Logistics and inventory management |
| IT Systems Operations | Mumbai, India | System maintenance and data processing |
| Online Retail Operations | Waukesha, Wi, USA | E-commerce platform, customer data & payment systems |

Table 1: Audit scope

The following information systems will be verified during this audit:

|  |  |  |
| --- | --- | --- |
| INFORMATION SYSTEM | MODULE | SUB-MODULE |
| E-commerce system | Customer management | Payment processing |
| HR system | Employee Records | Payroll |
| ERP System | Supply Chain Management | Payment Processing, CRM |

Table 2: Information systems to be audited

Further information systems or parts of information systems may be included within the scope of the audit if it is found that they are closely linked to the areas under audit.

## Audit criteria and reference documents

The finalised business requirements, information system documentation and business operations procedures will be used as the basis of the audit criteria.

Compliance with all applicable legislation and regulatory requirements will also be considered as part of the audit. For the scope of this audit, these are as follows:

|  |  |  |
| --- | --- | --- |
| Document | Summary | Areas of Interest |
| HIPAA | Regulations of health information management for data privacy | Protecting health-related documents |
| PCI DSS | Standards to protect payment card information and transactions | System maintenance and data processing |
| GDPR | Processing data requirements | Protecting customer data |

## Audit methods

### Review

The audit will consist of a combination of document review and onsite visits (or remote discussions using appropriate collaboration tools where necessary) to talk to relevant management and staff. Appropriate system logs and records will be reviewed as evidence that documented processes are being followed and that the system is operating in accordance with requirements. Copies of documented evidence will be taken where necessary. Actions arising from previous audits will be assessed.

### Technical audit tests

The following technical audit tests are also planned to be carried out:

|  |  |  |
| --- | --- | --- |
| SYSTEM | SCOPE OF TEST | PURPOSE |
| ERP System | Data integrity | Verify that vendor data is handled securely |
| E-commerce platform | Identify any payment gateway vulnerabilities | ENsure payment system security |
|  |  |  |

Table 4: Technical audit tests

Tests will be limited to read only access to data and will be run outside of business hours where appropriate to reduce any potential effect on system availability to the business.

### Additional processing

The following additional system processing is requested to be carried out during the audit:

|  |  |  |
| --- | --- | --- |
| SYSTEM | ADDITIONAL PROCESSING REQUIRED | PURPOSE |
| HR Systems | Verify user access permissions in the HR systems | Ensure that there’s compliance with data security and everything is confidential |
| Backup Systems | Test restore processes from backups | Ensure that data can be restored successfully |
| CRM System | Extract a random sample of customer interaction logs for review | Make sure data handling practices and verify compliance with privacy regulations |

Table 5: Additional processing

Additional processing will be run outside of business hours where appropriate to reduce any potential effect on system availability to the business.

## Resources required

### Audit team

The audit will be carried out by two members of the audit team acting independently of each other.

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | TITLE | CONTACT NUMBER | CAR REGISTRATION |
| Julian VanDeventer | Head Auditor | +1 987 654 3210 | PXP L28 |
| Josep Orellana | IT Specialist | +1 987 654 3211 | MNO 254 |

Table 6: Audit team

The audit will be carried out remotely using Microsoft Teams. All participants will require access to appropriate technology and must have received adequate training to allow them to communicate effectively with the audit team, including the use of screensharing. A meeting invitation will be sent by a member of the audit team at least 24 hours prior to the audit. A secure method of making documented information available to the audit team will be required, for example an online portal.

### Business resources required

Based on the scope of the audit in terms of the business processes and information systems covered, it is anticipated that the following people from the business will be required:

|  |  |  |
| --- | --- | --- |
| NAME | TITLE | MAIN RESPONSIBILITIES TO BE AUDITED |
| Sasha Colby | Op. Manager | Supply Chain Risk |

Table 7: Business resources required

### System access requirements

Temporary user accounts for the following people are required to be set up for auditing purposes:

|  |  |  |
| --- | --- | --- |
| NAME | TITLE | ACCESS LEVEL |
| Audit Team | IT Auditors | Read-only access |
| Julian VanDeveneter | Head Auditor | Full-access |
| Josep Orellana | IT Specialist | Role-based |

Table 8: Systems access requirements

Full audit logging should be enabled on these accounts so that a reference trail of access may be produced subsequent to the audit.

### Contacts

The following will be used as onsite contacts regarding the logistics of the audit:

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | TITLE | CONTACT NUMBER | EMAIL ADDRESS |
| Julian VanDeveneter | Lead Auditor | +1 987 654 3210 | Julianv@northwood.com |
| Gage Radtke | CEO | +1 987 654 3213 | Gager@northwood.com |

Table 9: Onsite contacts

## Audit schedule

The planning of the audit must aim to avoid affecting business operations unduly and so has not been planned in any of the following periods:

* Peak business months of October to December
* Business month end– this is the last week of each calendar month
* Business year end– this means that audits should not be carried out in March or April
* Key staff need to be available – peak holiday periods of July and August are to be avoided

The audit will be carried out over two days, starting on 15/12/2024. The proposed audit schedule is as follows:

### Day one

|  |  |  |  |
| --- | --- | --- | --- |
| TIME | AUDITOR | AUDITEE | AREAS TO BE COVERED |
| 9am | Lead Auditor | IT Manager | Opening meeting |
| 10am | Auditor Team A | HR Representative | Review HR processors things like user access, permissions, and audit trails. |
| 11am | Auditor Team B | Finance Team | Review the financial process through reports, transaction logs, and other processes |
| Noon | All | FULL AUDITOR TEAM | Go to lunch and eat |
| 1pm | Auditor Team C | Payroll | Ensure payroll system is up and running correctly |
| 2pm | Auditor Team D | It Security | Review the IT infrastructure by conducting network security and performing pentesting |
| 3pm | Auditor Team A | Backup Operator |  |
| 4pm | Auditor Team B | CRM Specialists |  |
| 5pm | Head Auditor | FULL AUDITOR TEAM | Day wrap-up and summary |

Table 10: Audit schedule day one

### Day two

|  |  |  |  |
| --- | --- | --- | --- |
| TIME | AUDITOR | AUDITEE | AREAS TO BE COVERED |
| 9am | Head Auditor | Full Auditor Team | Perform a briefing on the findings for day one, identify areas for review in day two. |
| 10am | Auditor Team B | Finance Team | Verify that there’s a compliance with the standards set for financial reporting |
| 11am | Auditor Team C | Payroll | Verify standards for payroll systems |
| Noon | Everyone | All Team | Lunch, team discussion |
| 1pm | Auditor Team A | Backup Operator |  |
| 2pm | Auditor Team D | It Security | Ensure IT systems follow standards |
| 3pm | Auditor Team B | CRM Specialists | Validate customer data compliance |
| 4pm | Head Auditor | IT Manager | Finish auditing report and create summary |
| 5pm | Head Auditor | Everyone | Day wrap-up and summary, summarize findings and propose solutions |

Table 11: Audit schedule day two

## Communication of findings

A draft audit report will be produced within two weeks of the end of the audit and the contents will be communicated initially to the management team who will be given an opportunity to comment.

A plan of action to address any shortcomings and corrective actions will be agreed.

A final report will be produced and communicated to the management team and made available to the executive management team as appropriate.

Follow up visits shall take place in accordance with the plan of action to ensure any shortcomings and corrective actions have been addressed/implemented.