

RISK ASSESSMENT PACK

Cleaning and Disinfection

A certification body will ask you to justify your cleaning programme by risk, not by habit. This pack scores every area, surface and piece of equipment on your site, then sets the frequency and method the risk warrants.

What you get

- The risk assessment workbook (Excel)

Fully editable, with drop-down lists, automatic inherent and residual risk scoring, colour coded risk bands, a populated worked example you can adapt, and a built in action tracker.

- The governing procedure (Word)

The SOP the risk assessment sits under, written to the same standard, ready to adopt with your company name and approver.

- A step by step completion guide (Word)

Purpose and clauses, what to gather first, the scoring method worked through with a real example, the register column by column, verification and review, and the mistakes auditors find most often.

- **A read me first sheet (Word)**

What is in the pack, who it is for, what you must edit before use, and how to get help.

Standards this pack supports

ISO 22000:2018 cl. 8.2.4 i), ISO 22002-1:2025 cl. 13 and ISO 22002-100:2025 cl. 13, FSSC 22000 V7 cl. 2.5.12

RISK ASSESSMENT													
RISK		Severity	High (100-500,000)	Medium (500-1,000,000)	Low (1,000-5,000,000)	Very Low (5,000-10,000,000)	Score	10	5	1	0	Score	10
RISK: Cyber and Information Risk Assessment		Severity	High (100-500,000)	Medium (500-1,000,000)	Low (1,000-5,000,000)	Very Low (5,000-10,000,000)	Score	10	5	1	0	Score	10
INTERNAL RISK (Internal Data)													
Control ID	Control Description	Control Type	Risk Factor	Severity	Score	10	5	1	0	Score	10	5	1
1.01	Access control to internal data	Access Control	Unauthorized access	High	100	10	5	1	0	100	10	5	1
1.02	Encryption of internal data	Encryption	Data breach	High	100	10	5	1	0	100	10	5	1
1.03	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.04	Employee training on security	Training	Human error	High	100	10	5	1	0	100	10	5	1
1.05	Incident response plan	Incident Response	Security incidents	High	100	10	5	1	0	100	10	5	1
1.06	Regular updates to software	Software Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.07	Secure disposal of data	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.08	Physical security measures	Physical Security	Physical access	High	100	10	5	1	0	100	10	5	1
1.09	Regular backups of data	Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.10	Secure email configuration	Email Security	Email interception	High	100	10	5	1	0	100	10	5	1
1.11	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.12	Secure network configuration	Network Security	Network intrusion	High	100	10	5	1	0	100	10	5	1
1.13	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.14	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.15	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.16	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.17	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.18	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.19	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.20	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.21	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.22	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.23	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.24	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.25	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.26	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.27	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.28	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.29	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.30	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.31	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.32	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.33	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.34	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.35	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.36	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.37	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.38	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.39	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.40	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.41	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.42	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.43	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.44	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.45	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.46	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.47	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.48	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.49	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.50	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.51	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.52	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.53	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.54	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.55	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.56	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.57	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.58	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.59	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.60	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.61	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.62	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.63	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.64	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.65	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.66	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.67	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.68	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.69	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.70	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.71	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.72	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.73	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.74	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.75	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.76	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.77	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.78	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.79	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.80	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.81	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.82	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.83	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.84	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.85	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.86	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.87	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.88	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.89	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.90	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.91	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.92	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1
1.93	Regular security assessments	Security Assessments	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.94	Secure data storage	Data Storage	Data leakage	High	100	10	5	1	0	100	10	5	1
1.95	Regular security updates	Security Updates	Software vulnerabilities	High	100	10	5	1	0	100	10	5	1
1.96	Secure data transmission	Data Transmission	Data interception	High	100	10	5	1	0	100	10	5	1
1.97	Regular security audits	Audit	Security weaknesses	High	100	10	5	1	0	100	10	5	1
1.98	Secure data backup	Data Backup	Data loss	High	100	10	5	1	0	100	10	5	1
1.99	Regular security training	Security Training	Human error	High	100	10	5	1	0	100	10	5	1
1.100	Secure data disposal	Data Disposal	Data leakage	High	100	10	5	1	0	100	10	5	1

The actual risk register in this pack, shown at reduced size.

Once off payment. No subscription.

Editable Word and Excel. Instant download.

R690 | USD 34

Inside the step by step guide

Every pack includes a written guide that walks a quality manager through the scoring method, the register column by column, residual risk, verification and review, and the mistakes auditors find most often on this subject. This is one page of it.

LOGO	[COMPANY NAME] Food Safety Management System	Doc No: RA03	Page 1 of 6
Subject: Cleaning and Disinfection - How to Complete This Risk Assessment			
Compiled by: ASC Food Safety	Approved by: [YOUR APPROVER]	Date: 01 Sep 2026	Rev no: 01

HOW TO COMPLETE THIS RISK ASSESSMENT

1. PURPOSE

This guide explains how to complete the RA03 Cleaning and Disinfection Risk Assessment supplied with it. It assesses the risks that arise when areas, equipment, food contact surfaces, utensils, transport containers and the working environment are cleaned and disinfected, and it records what you do about them.

The pack contains four files: the risk assessment workbook, the governing procedure, this guide, and a Read Me First file. Together they give you the assessment, the method behind it and the procedure that the controls in the register refer to.

Completed and kept up to date, the risk assessment provides evidence against: ISO 22002-1:2025 clause 13.1 (general), 13.2 (cleaning agents and tools), 13.3 (cleaning and disinfection programmes) and 13.4 (cleaning in place); ISO 22002-100:2025 clause 13.1 to 13.3; ISO 22000:2018 clause 8.2, and in particular clause 8.2.4 i) cleaning and disinfecting, which requires the prerequisite programme to be selected, established, monitored and verified in documented information; FSSC 22000 Version 7.0 clause 2.5.12 PRP verification, and clause 2.5.1 (a) where an external laboratory is used for cleaning or allergen verification.

This is a prerequisite programme risk assessment. It is not a hazard analysis. It decides how much control the prerequisite programme needs and shows that the decision was made on evidence. Its output is an input to your hazard analysis under ISO 22000:2018 clause 8.5.2 and to management review under clause 9.3.

2. BEFORE YOU START

Do not start in the workbook. Collect the following first, because every score you enter has to be defensible from it:

- the master cleaning schedule and the cleaning instruction cards, so that every item and area in the schedule can be tested against a risk line
- the chemical list, with the approved dilution, contact time and temperature for each product, and the food area suitability approval
- the colour coding and zoning scheme for cleaning equipment, and where the equipment is stored between uses
- the list of cleaning in place circuits with their validated parameters, and the points that are cleaned manually because they cannot be reached by the circuit
- twelve months of verification data: visual failures, ATP or protein results and re-clean rates, allergen swabs and microbiological swabs, by surface and by area
- the allergen matrix and the changeover sequence, and the list of parts that are hard to clean, are only stripped periodically, or cannot be dismantled

The assessment is led by the QA Manager or Food Safety Team Leader and must include the Hygiene Manager, who owns the schedule, the Engineering Manager, who knows the dead legs, sprayball coverage and drainage of the plant, and the Production Manager, who controls whether

Inside the accompanying procedure

The pack also carries the governing procedure the risk assessment sits under, written to the same house standard and ready to adopt with your company name and approver. This is its first page.

LOGO	[COMPANY NAME] Food Safety Management System	Doc No: RA03	Page 1 of 6
Subject: Cleaning and Disinfection Procedure			
Compiled by: ASC Food Safety	Approved by: [YOUR APPROVER]	Date: 01 Sep 2026	Rev no: 01

CLEANING AND DISINFECTION PROCEDURE

1. PURPOSE

This procedure ensures that the areas, equipment, utensils, food contact surfaces, transport containers and working environment at [COMPANY NAME] are cleaned and disinfected to a validated and verified standard that controls microbiological, allergen, chemical and foreign-body hazards.

2. SCOPE

This procedure applies to all production, packing, storage, warehouse, utility, laboratory, welfare and external areas, to manual and mechanical cleaning, to cleaning in place (CIP), and to cleaning carried out by contractors. Equipment and food contact surface requirements are set in your equipment and food contact surface cleaning instructions; general order and tidiness is covered by your housekeeping procedure.

3. REFERENCES

FSSC 22000 Scheme Version 7.0 (May 2026)

ISO 22002-1:2025, clause 13.1 (general), 13.2 (cleaning agents and tools), 13.3 (cleaning and disinfection programmes, including post-clean and pre-start-up inspections) and 13.4 (CIP systems)

ISO 22002-100:2025, clause 13.1, 13.2, 13.3.1 (what, frequency, responsibility, method, monitoring and verification) and 13.3.2 (appropriate to the hazard, confirmed capable, carried out so that food safety is not compromised)

This procedure is supplied with the RA03 Cleaning and Disinfection Risk Assessment, which is the only other controlled document in this pack. The documents named below are referred to by name in this procedure and are documents you hold, or will create, in your own management system. Where a name does not match your own document title, read it as the equivalent document on your system: equipment and food contact surface cleaning instructions, housekeeping procedure, master cleaning schedule, cleaning checklist, CIP run log, CIP run and verification work instruction, cleaning verification ATP and rapid test log, thermometer and instrument verification log, master chemical list, cleaning chemical issue and control record, chemical spillage procedure, microbiological testing programme, environmental monitoring programme, allergen management procedure, pre-start-up hygiene checklist, management of services procedure, laboratory competence approval record, laboratory report acceptance checklist, sample submission and chain of custody record, nonconformity and corrective action procedure, environmental micro trends tracker, allergen risk assessment, calibration register, management review, control of monitoring and measuring devices procedure, training record, daily sanitation audit report, weekly sanitation inspection, competency assessment, FSMS KPI dashboard, internal audit programme, and continual improvement process.

Cross scheme mapping. This procedure also serves BRCGS Food Issue 9 cl. 4.11 housekeeping and hygiene, IFS Food v8 cl. 4.10 cleaning and disinfection and SQF Edition 9 cl. 11.2.5 cleaning and sanitation. Any GFSI scheme that requires a documented, risk based cleaning and disinfection programme.

4. RESPONSIBILITIES

Role	Responsibility
Hygiene Manager	Owns the master cleaning schedule and the cleaning instruction cards, plans and resources the cleaning teams, trains and assesses cleaning operatives, controls