MANAGEMENT SYSTEMS INTERNATIONAL

COMPANION TO THE PURCHASING AND SUPPLIER CONTROL MATURITY CHECK

# Purchasing and Supplier Control

## The full maturity ladder, and a worksheet to score yourself against it

You have just scored your purchasing and supplier control process against eight elements. This document is the whole ladder behind that score — every element, all four levels, described as behavior someone could observe rather than as intentions you could claim.

It works for ISO 9001:2015, ISO 13485:2016, ISO 14001:2026, ISO 45001:2018 and ISO 7101:2023. The eight elements are common to all five; the clause that anchors each one is not, so every element carries the anchor for each standard. Five short addenda cover the requirements that exist in only one of them.

| Item | Detail |
|---|---|
| Document | Purchasing and Supplier Control Maturity Framework |
| Revision | Rev 1.1 |
| Issue date | July 21, 2026 |
| Applies to | ISO 9001:2015 · ISO 13485:2016 · ISO 14001:2026 · ISO 45001:2018 · ISO 7101:2023 |
| Supplied by | Management Systems International, LLC · 760-434-9141 |
| Latest issue | msi-international.com |

### Three things to hold on to

| | What it means in practice |
|---|---|
| Score against a busy week | Not against the procedure, and not against the week you had time. The honest question for every row is what happens when two people are away, a customer is escalating, and the plant is down. That is the level you are actually operating at, and it is the one an auditor samples into. |
| One element at a time | Improving all eight by a little produces nothing you can point to. Taking one element from Level 1 to Level 2 changes how the process behaves. Pick the lowest, finish it, then pick the next lowest. |
| Level 2 is a legitimate place to stop | A well-implemented certified system operating consistently at Level 2 is a sound system. Levels 3 and 4 cost measurement effort and sustained management attention, and they earn their keep where exposure is high, where customers are asking, or where a regulatory or disclosure regime applies. Decide where you intend to operate and say so, rather than drifting upward by accident or downward by neglect. |

| | What it means in practice |
|---|---|

**MSI note:** A note on the levels. They are cumulative: Level 3 assumes Level 2 is holding. If you find yourself scoring Level 3 on measurement while Level 2 controls are inconsistent, that is worth looking at directly — measuring a process that is not yet controlled produces numbers that describe the exceptions rather than the process.

## How to use this framework

— Read the element, then the four levels, then decide. Each element opens with what it governs and why it fails, which is usually more useful than the level descriptions on their own.

— Use the clause anchors to find where the obligation sits in your own standard. They are given for all five standards because the element is the same and the clause is not.

— Read the failure mode. It describes what the element looks like when it is absent. If you recognize your organization in it, you are below Level 2 on that element whatever the level text suggests.

— Use the three actions to move up exactly one level. They are deliberately small. Anything larger tends not to survive the quarter.

— Then use the worksheet at the back. Score, date it, and take it to a management review. That is what this document is for.

> **Why the worksheet is the point:** A score in a browser is interesting for about a day. A scored worksheet with a date on it, tabled at a management review, becomes a decision about where the organization intends to operate and what it will fund. That conversation is the only thing that reliably changes a purchasing process, and it is much easier to start with a filled-in page than with an opinion.

# Requirement capture

Whether a need for something from outside the organization reliably enters your process at all. Every other element depends on this one, because a requirement that never entered cannot be rated, evaluated, specified or verified. It is also the element organizations are most confident about and most often wrong about.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.1 — determine controls to be applied to externally provided processes, products and services |
| ISO 13485:2016 | 7.4.1 — process to ensure purchased product conforms to specified requirements |
| ISO 14001:2026 | 8.1 — externally provided processes, products and services relevant to the EMS |
| ISO 45001:2018 | 8.1.4.1 — process to control procurement of products and services |
| ISO 7101:2023 | 8.8 — clinical and non-clinical externally provided services and products |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | A purchase order raises the process. Needs met by card, by telephone, by a favour from a known supplier, or arranged directly by another department do not enter it. Nobody has counted how many that is. |
| Level 2 — Controlled | Every route is named in the procedure, including verbal requests, card purchases, contractor engagements and services arranged by other functions. Each has a defined way in, and the people using those routes know what it is. |
| Level 3 — Measured | Purchases made outside the process are counted and cause-coded. The organization knows which categories leak and roughly how much. |
| Level 4 — Anticipatory | Capture data drives change to the categories themselves — contracting, stockholding, approved alternatives — so the pressure to bypass the process is removed rather than policed. |

## Moving up one level

— Spend an hour listing every way something can arrive from outside without a purchase order. Most organizations find between four and nine routes, and are surprised by at least two.

— For each route, write down the one thing that must happen for it to enter the process — not the ideal process, the minimum.

— Name the categories most often arranged outside the system. In our experience they are waste, contractors, agency staffing, utilities and anything bought at a trade counter. Put them explicitly in scope in your procedure.

> **MSI note. Failure mode.** The organization has a supplier control process and a parallel, invisible one. The invisible one handles the urgent, the cheap and the awkward — which is a fair description of the purchases that cause incidents. Nobody is negligent; the process simply has no door on the side where people are actually knocking.

# Impact determination

How you decide how much control a given provision needs. This is the element that determines where all your effort goes, which makes getting the criteria wrong unusually expensive: the effort still gets spent, just not where the exposure is.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.1 — criteria for evaluation, selection, monitoring and re-evaluation; 8.4.2 c) potential impact |
| ISO 13485:2016 | 7.4.1 — proportionate to the effect of the purchased product on the quality of the medical device |
| ISO 14001:2026 | 6.1.2 aspects; 8.1 — relevance to the intended outcomes of the EMS |
| ISO 45001:2018 | 6.1.2.1 hazard identification; 8.1.4.2 — hazards arising from contractors |
| ISO 7101:2023 | 8.8 b) — effect on the safety of both the workforce and service users |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | Suppliers are described as important or not, largely by what they cost or how much is bought from them. The reasoning lives in the heads of experienced people. |
| Level 2 — Controlled | Rating is assigned against written criteria based on the effect of the provision, applied consistently and recorded. Value is not one of the criteria. Anything unrated defaults upward, not downward. |
| Level 3 — Measured | The distribution of ratings is reviewed, and provisions that were found to be high-impact only after something went wrong are counted. |
| Level 4 — Anticipatory | Criteria are revised from what has actually caused harm or nonconformity, so the rating predicts rather than describes. |

## Moving up one level

— Take your three cheapest suppliers and ask what would happen if each delivered something wrong. If any answer is serious, your criteria are not doing their job.

— Write the criteria as thresholds that can be met or not met. “Important supplier” is not a criterion. “Anything a control measure depends on” is.

— Add a default: anything not yet rated is treated as high impact until someone rates it. A default that runs downward guarantees nothing gets rated.

> **MSI note. Failure mode.** Attention follows the ledger. The largest contracts get audits, questionnaires and quarterly reviews; the $38 consumable that a control depends on gets nothing, because no threshold in the system can see it. This is the single most common structural error in supplier control, and it is inherited wholesale from procurement, where rating on value is entirely correct.

# The two-control determination

Whether you have decided — and written down — both what you control at the provider and what you control on what arrives. This is the element that most reliably separates a supplier process that works from one that passes audits, and it is the differentiator this whole framework is built around.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.2 b) — the controls applied to the external provider AND those applied to the resulting output |
| ISO 13485:2016 | 7.4.1 criteria and control; 7.4.3 verification of purchased product |
| ISO 14001:2026 | 8.1 — controlled or influenced, with the type and extent of each defined within the EMS |
| ISO 45001:2018 | 8.1.4.1 conformity to the OH&S management system; 8.1.4.3 type and degree of control defined |
| ISO 7101:2023 | 8.8 c) receiving and verifying; 8.1 externally provided processes controlled |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | There is an approved supplier list and there are certificates on file. Controls are not written down as a decision, and nobody could state what is controlled where. |
| Level 2 — Controlled | Both sets are decided and recorded separately for every significant provision: what is applied to the provider, and what is applied to what arrives. Where a characteristic cannot be verified on receipt, the provider-side control is identified as the only control. |
| Level 3 — Measured | Controls are reviewed against actual performance, and reductions in receipt checking are justified by provider data with a stated basis and a review date. |
| Level 4 — Anticipatory | Control is designed jointly with the provider. The interval between their last check and your first use is owned by somebody, explicitly. |

## Moving up one level

— Take one significant supplier and fill in two columns on one page: what we require of them, and what we check when it arrives. If either column is thin, that is the finding.

— Ask the question almost nobody asks: which characteristics does neither party verify, each assuming the other does? Ask the supplier directly. The answers are usually surprising and always cheap to fix.

— For your highest-impact provision, identify what cannot be verified after the fact — sterility, heat treatment, a laboratory result, the competence of someone already on shift — and set the provider-side control accordingly.

> **MSI note. Failure mode.** It is missed structurally rather than carelessly, which is why capable organizations miss it. The approved supplier list belongs to purchasing. Incoming inspection belongs to quality, or to receiving, or to the ward. No single document asks for the pair, so nobody notices the pair was never decided. The result is an organization that can produce a certificate for every supplier and cannot say what it checks.

# Evaluation and selection

Whether providers are chosen against criteria that are applied, rather than collected. The distinction matters more than it sounds: most organizations satisfy the first half of the obligation and not the second.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.1 — criteria for evaluation, selection, monitoring and re-evaluation |
| ISO 13485:2016 | 7.4.1 — criteria for evaluation and selection; records of results |
| ISO 14001:2026 | 8.1 — control of externally provided processes; 6.1.3 compliance obligations |
| ISO 45001:2018 | 8.1.4.2 — define AND apply OH&S criteria for the selection of contractors |
| ISO 7101:2023 | 8.8 a) — criteria for evaluating, selecting, monitoring AND disqualifying |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | A supplier is used, it works, and they are used again. A questionnaire may exist and be filed. |
| Level 2 — Controlled | Written criteria are applied at a depth set by the rating. Results are recorded, approval is for a stated scope, and provision outside that scope is an exception rather than a habit. |
| Level 3 — Measured | Suppliers are declined on the criteria, and selection outcomes are compared with how those suppliers later performed — which tests whether the criteria predict anything. |
| Level 4 — Anticipatory | Provider development is planned. Standards raise their practice on other clients' sites too, which is the point at which supplier control starts returning value rather than consuming it. |

## Moving up one level

— Check whether any supplier has ever been declined on your criteria. If none has, the criteria are being collected rather than applied, and that is the whole finding.

— Record scope explicitly on every approval. “Approved” without a scope is how a contractor approved for mechanical work ends up working at height.

— Add one criterion you would actually act on, and act on it once. The first decline is what makes the process real.

> **MSI note. Failure mode.** A pre-qualification questionnaire that is sent, scored, filed and has never once changed a decision. It satisfies an auditor looking for evidence of criteria and satisfies nobody looking for evidence of control. ISO 45001 and ISO 7101 both close this loophole explicitly — one by requiring criteria to be defined and applied, the other by requiring criteria for disqualification.

# Agreed requirements

What actually reaches the provider before they start, and whether they accepted it. The standards consistently ask for requirements to be communicated and, in several cases, agreed — which is a higher bar than sent.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.3 — adequacy of requirements prior to communication |
| ISO 13485:2016 | 7.4.2 purchasing information; 7.4.2 change-notification agreement |
| ISO 14001:2026 | 8.1 b) and c) — determine environmental requirements for procurement; communicate to external providers including contractors |
| ISO 45001:2018 | 8.1.4.2 — ensure requirements are met by contractors and their workers |
| ISO 7101:2023 | 8.8 — agreed-upon requirements; 8.8 e) alignment, impartiality, confidentiality |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | A part number, a quantity, a price, and standard terms nobody has read recently. |
| Level 2 — Controlled | Requirements are stated, reviewed for adequacy before they are sent, and the review is recorded. The reviewer is a named role, not whoever is nearest. |
| Level 3 — Measured | Non-fulfilment is counted by category, and requirements that are consistently unmet are revised rather than repeated. |
| Level 4 — Anticipatory | Requirements are set from evidence — what has failed, what the downstream process depends on — and change what providers offer. |

## Moving up one level

— Add advance change-notification to your significant suppliers' terms, with the change categories enumerated: material, formulation, method, site, subcontractor.

— Name a role to confirm adequacy before purchasing information goes out, and record the confirmation against the order. Two minutes per order.

— For one category, write down the requirements once rather than per order, and build them into the ordering route so they apply even to the person who has never read the procedure.

> **MSI note. Failure mode.** Requirements exist internally and never reach the provider, so they are unenforceable and, in several standards, undischarged. The tell is an organization that can show you a detailed specification and cannot show you that the supplier ever received it or agreed to it.

ELEMENT 6 OF 8

# Verification and release

What happens between something arriving and being used. This is the element with the shortest distance between a gap and a consequence.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.3 e) verification activities; 8.6 release of products and services |
| ISO 13485:2016 | 7.4.3 — verification of purchased product, proportionate to effect |
| ISO 14001:2026 | 8.1 — operating criteria established and control implemented in accordance with them |
| ISO 45001:2018 | 8.1.4.1 — conformity to the OH&S management system before use |
| ISO 7101:2023 | 8.8 c) — receiving and verifying equipment, devices, services, materials and medications |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | It goes to the point of use. Someone would notice if it were obviously wrong. Documents that arrive with it are filed. |
| Level 2 — Controlled | Verification is defined for each provision, performed to that extent, and recorded before release. Documents are read against the requirement, not merely filed. Unverified items are identified as not released. |
| Level 3 — Measured | Verification failures are counted, and substitutions that would have removed a control are caught and counted. |
| Level 4 — Anticipatory | Suitability is designed into the specification, so an “equivalent” substitution cannot silently occur. |

## Moving up one level

— Pick one arriving document type — a certificate, a data sheet, a test report — and start reading it against the requirement rather than filing it. Record the review.

— Introduce a physical or system marker for not-yet-released items. Quarantine that relies on memory is not quarantine.

— Write down, for your top three provisions, what “equivalent” is allowed to mean and who decides. That single page prevents the most expensive category of substitution error.

> **MSI note. Failure mode.** A filed certificate nobody read is a control that did not operate, and it is worse than no certificate at all, because it creates confidence. The recurring pattern across every sector is the catalogue-equivalent substitution: equivalent for the property the catalogue compares, and not for the property your process actually depends on.

# Monitoring and re-evaluation

Whether you would notice a provider degrading before it costs you something, and whether anything happens when you do.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.1 — monitoring of performance and re-evaluation; 9.1 analysis |
| ISO 13485:2016 | 7.4.1 — monitoring and re-evaluation; records maintained |
| ISO 14001:2026 | 9.1.1 monitoring; 9.1.2 evaluation of compliance |
| ISO 45001:2018 | 9.1 monitoring; 10.2 incident and nonconformity |
| ISO 7101:2023 | 8.8 a) monitoring; 8.8 d) problems documented and communicated; 8.8 f) records maintained |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | Performance is known informally. Problems are dealt with by whoever picks them up, usually by telephone, and often not recorded. |
| Level 2 — Controlled | Defined measures at a frequency set by the rating, feeding re-evaluation on a stated interval, with event triggers that force it in between. Problems are both recorded and communicated to the provider. |
| Level 3 — Measured | Trends are analyzed rather than reported. Problems are tested against what was agreed in advance would end the relationship. |
| Level 4 — Anticipatory | Monitoring predicts. Degradation is caught by leading indicators rather than by the first failure. |

## Moving up one level

— Add event triggers to your re-evaluation, not just intervals. An annual review that cannot be brought forward by an incident is a calendar entry, not a control.

— Make sure problems get communicated to the provider and recorded internally. Doing one without the other is the commonest half-discharge of this obligation.

— Diaries every certificate, license and insurance expiry with a named owner. It is an afternoon of work and it closes an entire failure category.

> **MSI note. Failure mode.** The organization finds out that a provider has been drifting when something arrives that cannot be used, and then discovers that three people had each noticed something and none had recorded it. Monitoring existed as awareness rather than as data, so there was no trend to see.

ELEMENT 8 OF 8

# Exception and contingency

What your process does when the normal route cannot be followed, and what happens if a provider stops. This is the element that decides whether the other seven survive contact with a bad week.

## Where the obligation sits

| Standard | Clause |
|---|---|
| ISO 9001:2015 | 8.4.2; 6.1 risks and opportunities |
| ISO 13485:2016 | 7.4.1; 6.1 / 7.1 planning |
| ISO 14001:2026 | 8.1 operational control; 8.2 emergency preparedness |
| ISO 45001:2018 | 8.1.4; 8.2 emergency preparedness and response |
| ISO 7101:2023 | 8.8; 8.7 access to medical devices, medications and workforce |

## The four levels

| Level | What someone would observe |
|---|---|
| Level 1 — Documented | Urgent purchases happen and are dealt with informally. Nobody writes them down, so nobody knows how often. If a provider stopped, the organization would find out how bad it was at the time. |
| Level 2 — Controlled | A bounded, authorized, recorded route exists, closed to the categories where no authorization can substitute for verification. Continuity is determined for significant provision: what stops, how quickly, and what the alternative is. |
| Level 3 — Measured | Exceptions are counted and aged. Continuity determinations are tested rather than asserted. |
| Level 4 — Anticipatory | Recurring exceptions drive change to the underlying arrangement, and alternatives are approved in advance of need rather than qualified during a crisis. |

## Moving up one level

— Write the exception route down, including who authorizes it. An undocumented route is used anyway — just without controls or a record.

— Decide in advance which categories the route is closed to. High-hazard work, unlicensed waste carriers, and unverified sterile or safety-critical items are the usual answers.

— For your three most significant provisions, write one page each: what stops, how fast, what the alternative is, and who decides. Do it now rather than during the interruption.

**MSI note. Failure mode.** The absence of an exception route does not prevent exceptions; it prevents records of them. The urgent engagement still happens, with no rating, no controls, no authorization and no log — and it is disproportionately the one that causes the incident. An organization with no exception log has not eliminated exceptions, it has eliminated the evidence.

## Standard-specific addenda

The eight elements are common to all five standards. Each standard also contains at least one obligation relating to external provision that the others do not, and those are consistently the requirements organizations have not discharged — not through carelessness, but because a supplier procedure carried over from another standard will not contain them, and no clause checklist from the other standard points at them.

**Read the addendum for your standard. Score it as a ninth element on the worksheet.**

### ISO 9001:2015 — Outsourced processes

Clause 8.4.2 a) requires externally provided processes to remain within the control of the quality management system. That is a different obligation from controlling a purchased product, and it is usually discharged by a sentence saying so, with nothing behind it.

A process is outsourced if you could perform it yourself and it forms part of your own product realization. The contract type does not decide it and neither does the invoice.

| Level | What someone would observe |
|---|---|
| 1 | A statement in the manual that outsourced processes remain within the QMS. |
| 2 | The type and extent of control is decided and recorded, and the interface is defined in both directions — what you hand over, in what state, and what comes back with what evidence. |
| 3 | The process sits inside your audit program, your process monitoring and your corrective action system, and is reported at management review. |
| 4 | Process parameters are monitored rather than paperwork, and the arrangement survives the departure of whoever set it up. |

— Name every outsourced process. Most organizations under-count, because anything routinely bought is assumed to be a purchase.

— For each, write down how the twelve QMS elements are achieved — criteria, competence, equipment approval, records, audit, corrective action, traceability, access.

— For special processes whose result cannot be verified afterwards — heat treatment, welding, coating, sterilization, bonding — approve the methods, process and equipment, because inspection will not save you.

## ISO 13485:2016 — Regulatory obligations and change notification

Two things separate device supplier control from ISO 9001. Control must be proportionate to the effect of the purchased product on the medical device — so spend is excluded from the rating by the clause itself. And a set of obligations arises from regulation rather than from the standard.

Since February 2, 2026, ISO 13485:2016 is incorporated by reference into 21 CFR Part 820 under the Quality Management System Regulation. Supplier records are inspectable. Verify the current position at fda.gov, since transition arrangements and guidance continue to develop.

| Level | What someone would observe |
|---|---|
| 1 | Supplier control follows spend and general importance, as elsewhere in the business. |
| 2 | Rating follows device effect, with spend excluded. A written change-notification agreement exists for the suppliers that need it, with change categories enumerated. |
| 3 | Every notification receives a recorded impact determination, including when the determination is no impact. Regulatory obligations arising outside the standard are identified and owned. |
| 4 | The supplier base is managed against regulatory exposure as well as quality performance, and reviewed when the regulation or the portfolio changes. |

— Check that your rating criteria contain no value threshold. If they do, remove it — the clause asks for effect on the device.

— Put change notification in writing for every supplier whose change could affect the device, and enumerate what counts as a change.

— List the obligations that come from regulation rather than from a clause, and give each an owner. Nothing in your clause checklist will find them for you.

## ISO 14001:2026 — Control or influence

Clause 8.1 requires externally provided processes, products and services relevant to the intended outcomes of the EMS to be controlled or influenced, and requires the type and extent of that control or influence to be defined within the environmental management system.

Organizations read “or” as an either/or, define the controls they already had, and leave influence undefined. But for most environmental aspects control is not available, so influence is the only thing left to define. A fully populated control column beside an empty influence column has documented the minority of the organization's footprint.

| Level | What someone would observe |
|---|---|
| 1 | Controls on site are described. Influence is not addressed at all. |
| 2 | Both are determined and recorded for every relevant provider. “None” appears in the influence column only with a stated basis, never as a blank. |
| 3 | Influence exerted is logged and its effect counted — requests made, and requests that produced a change. |
| 4 | Influence is planned and resourced as an objective, and providers change practice because you asked. |

— Add an influence column beside your control column in the approved provider register. The empty cells are your Clause 8.1 gap, visible at a glance.

— Trace one waste stream to its final destination, not the transfer station, and record how you verified it. Any recovery rate you quote publicly should be evidenced rather than repeated.

— Record the Clause 8.1 d) determination per product family — transport, use, end of life, disposal — including recorded decisions that no information is needed.

## ISO 45001:2018 — Worker consultation and the hierarchy of controls

Clause 5.4 requires emphasis on the consultation of non-managerial workers on determining applicable controls for outsourcing, procurement and contractors. It sits in the leadership clause rather than the operational one, which is why purchasing procedures almost universally miss it.

It is also the easiest requirement in the standard to test. The auditor asks a worker whether anyone asked them what the controls should be before the contractor arrived. No document produces a yes if the conversation did not happen.

Clause 8.1.4.2 additionally requires contractor risk to be assessed in three directions — including what your operations do to their people, which is the direction most often omitted and the one that most often causes harm.

| Level | What someone would observe |
|---|---|
| 1 | Workers are informed after the arrangement is made, if at all. |
| 2 | Non-managerial workers are consulted before controls are determined, and it is recorded. The hierarchy of controls is worked in order at the point of purchase, with the reason for relying on protective equipment written down. |
| 3 | Consultation coverage is measured, and inputs adopted and declined are both counted and fed back. |
| 4 | Workers participate in setting the selection criteria, and substitutions achieved at procurement are counted. |

— Consult one work group before the next contractor engagement, and record what they raised and what changed. That single record discharges more of Clause 5.4 than any document.

— When a purchase decision lands on protective equipment, write down why elimination, substitution and engineering controls were not sufficient. If that sentence is hard to write, go back up a level.

— Assess all three directions of contractor risk explicitly, and put the middle one — your hazards to their unfamiliar people — on the permit to work.

## ISO 7101:2023 — Disqualification criteria and dual safety

Clause 8.8 a) requires criteria for disqualifying external providers, defined alongside those for evaluating, selecting and monitoring them. No other management system standard in common use asks this.

Clause 8.8 b) requires the effect on the safety of both the workforce and service users to be considered — two questions with two answers. A cleaning agent that protects service users and exposes cleaners is the ordinary case, not the exception.

Clause 8.8 also reaches partnering stakeholders — governmental, non-governmental and intergovernmental organizations and funding partners — requiring expectations to be documented and a pre-defined method for communicating failure to meet criteria. That reaches donations and grant-funded provision, which bypass procurement entirely because nothing is bought.

| Level | What someone would observe |
|---|---|
| 1 | Providers are removed, if at all, after an argument. Safety is considered as a single question. |
| 2 | Disqualification criteria are defined in advance, recorded, and communicated to the provider. Both safety questions are asked and recorded separately. Expectations for donated and grant-funded provision are documented before acceptance. |
| 3 | Criteria are checked at every problem record, and the outcome is recorded either way. Any decision to continue is written, owned and time-limited. |
| 4 | Criteria are revised from experience, and providers change behavior because they know what they are. |

— Pick your most depended-upon provider and write down what would cause you to stop using them. If nothing would, that is not a criteria problem — it is a single point of failure with no plan.

— Split your next supplier assessment into two recorded answers: effect on service users, effect on workforce.

— Before accepting the next donation, complete the expectations record — consumables, maintenance, compatibility, regulatory status, training, and what happens when the funding ends.

> **The pattern across all five:** Each of these obligations is missed for the same structural reason rather than through carelessness. Each sits outside the place a supplier procedure normally looks — in a different clause, in a regulation rather than a standard, or behind a word like “influence” that reads as an escape. Capable, certified organizations miss them routinely, which is worth saying plainly if you have just scored yourself low on one.

## Scoring worksheet

Print this page. Score each element 1 to 4 against what happens on a busy week. Add the standard-specific addendum as element 9. Then date it, and take it to your next management review.

| Field | Entry |
|---|---|
| Organization | |
| Standard scored against | |
| Scored by (role) | |
| Date scored — write the month in full, e.g. July 21, 2026 | |
| Level this organization intends to operate at, and why | |

| # | Element | Level 1–4 | Evidence — what actually happens on a busy week | Target | By when |
|---|---|---|---|---|---|
| 1 | Requirement capture | | | | |
| 2 | Impact determination | | | | |
| 3 | The two-control determination | | | | |
| 4 | Evaluation and selection | | | | |
| 5 | Agreed requirements | | | | |
| 6 | Verification and release | | | | |
| 7 | Monitoring and re-evaluation | | | | |
| 8 | Exception and contingency | | | | |
| 9 | Standard addendum (name it) | | | | |

### The three questions for the management review

| Question | Answer |
|---|---|
| Which single element are we taking up one level first, and who owns it? | |
| What level do we intend to operate at across the process, and is Level 2 our deliberate answer? | |
| What are we choosing not to do, and are we content to record that as a decision? | |

**MSI note:** The third question is the one worth keeping. A management review that only records what will be improved produces a growing list nobody closes. Recording what the organization has consciously decided not to pursue — and why — is what turns a maturity score into a strategy, and it is what makes the improvements you did commit to credible.

## Re-score

Score again after the actions land, and keep both sheets. The comparison is more useful than either score alone, and a dated pair of worksheets is the most straightforward evidence of continual improvement in this process that you can put in front of an auditor.

| Element | First score | Date | Second score | Date / moved? |
|---|---|---|---|---|
| 1 Requirement capture | | | | |
| 2 Impact determination | | | | |
| 3 Two-control determination | | | | |
| 4 Evaluation and selection | | | | |
| 5 Agreed requirements | | | | |
| 6 Verification and release | | | | |
| 7 Monitoring and re-evaluation | | | | |
| 8 Exception and contingency | | | | |
| 9 Standard addendum | | | | |

## Where to go from here

If the worksheet has shown you two or three elements to fix, the next question is whether to write the procedure yourself or start from one.

| If this is true of you | Then |
|---|---|
| You scored Level 2 or above on most elements and know exactly which two to fix | Use this framework and fix them. You do not need a template, and the actions in each element are the whole plan. |
| You scored Level 1 on several elements, or the procedure you have does not describe what happens | The MSI Purchasing and Supplier Control Procedure template is a complete, editable procedure written to a single standard — the one this ladder is drawn from. $149 per standard. |
| You run more than one standard and the procedures conflict | Combined versions cover the divergences explicitly, including what was decided and what the alternative was. $249. |
| The score surprised you, or the priority order does not match what you expected | Call MSI on 760-434-9141. A short conversation is usually quicker than a long email. |

### What is in the procedure template

— A complete procedure in editable Word format, with placeholders everywhere a value is yours to set — not a checklist and not an outline.

— An evaluation record built to work as the approval gate, plus the provider register, a desk-level work instruction, and a worked example.

— A fourth appendix specific to your standard: outsourced process control, the device decision record, the ISO 14001:2015 to 2026 transition mapping, the onsite contractor acknowledgement, or the disqualification criteria record.

— The maturity ladder in Section 13 — the one this framework is drawn from — so the improvement path is in the same document as the procedure.

— Records tables with no blanks, event-based review triggers, and defined exception and contingency paths.

## About Management Systems International (MSI)

Diana Lynn is President and Principal ISO Consultant at Management Systems International (MSI), a consulting firm she co-founded in 1998. With 28 years of experience including extensive AS9100 work in MSI's early years, MSI's track record includes 80+ certifications supported, 200+ audits attended, and 600+ professionals trained across manufacturing, technology, medical device, government, healthcare, and other regulated industries. Today MSI implements ISO 9001:2015, ISO 13485:2016, ISO 14001:2026, and ISO 45001:2018, with an expanding focus on ISO 7101:2023 healthcare quality.

MSI is veteran-owned and female-owned.

### Where to go next

— Take the free Purchasing and Supplier Control Maturity Check to place your organization on the ladder: msi-international.com

— Read the article this framework accompanies, on the purchasing and supplier control procedure requirement almost everyone skips: msi-international.com/blog/

— Browse the procedure templates and toolkits: member.msi-international.com/shop/

— Watch the ISO Executive Decision Briefs — short leadership-level videos on what a management system is supposed to produce: msi-international.com/iso-executive-decision-briefs/

— Read the article behind the check for the seven marks of an effective procedure in full: msi-international.com/effective-iso-procedure/

— If your company needs a more proactive systematic approach to what is causing bottlenecks see our The Portrait

— Building or transitioning a management system? SurePath is MSI's turnkey certification path: msi-international.com/surepath/

— Want the same treatment applied to your own procedures? Call MSI at 760-434-9141 to schedule a planning session.

## License and disclaimer



> **Disclaimer.** This is a self-assessment aid, not an audit, and nothing in it is a conformity finding. Maturity levels are MSI's own construct and are not defined by any ISO standard — an organization at Level 2 across every element can be fully conforming, and this framework says so deliberately. It does not replace the applicable standard, the applicable regulation, or the judgment of a competent professional. Standards are revised, amended and withdrawn; clause references are provided for orientation and should be confirmed against the current published text at iso.org before you rely on them.