Local end-to-end process Owner : ***please fill in Name and Position***

Process step	Principle	Risk	#	Control title	Objective	Control description	Owner *Suggested owner*	Frequency	Control Nature *(Preventive/Detective)*	Key / Non-key Control	Anti-corruption control? *Control addresses corruption risk? (Yes)* *Control indirectly contributes to managing corruption risk (No)?*	Control level *First-level controls are embedded in the process and are the first layer of risk prevention and detection. Second-level controls are periodic, not real-time, and independent from day-to-day execution.*	Local Control Owner *Name, Position*
1. Procurement policy - Indirect Procurement	A local indirect procurement procedure is established and approved by the local management, including the GM, Legal and FInance. - competitive vendor selection, involvement of relevant departments - vendor due diligence - contracting, standard terms and conditions (T&Cs),including payment terms - purchase requisition creation and approval - purchase order creation and approval - recording reception of the goods in the system Employees that may be involved in the indirect procurement process as purchase requestors, preparers or approvers are identified upon arrival / job position change and are formally trained. Further elements related to end-to-end procurement process are formalised in a procedure as well, detailing clear process steps and roles & responsibilities: - vendor master data management - invoicing and 3-way match - accounts payable	Inadequate procurement strategy definition and implementation.	1	**Indirect procurement procedure**	To establish clear rules of indirect procurement process.	Ensure that the local indirect procurement procedureis established and is updated at least on a yearly basis. Ensure that the local procedure is in line with the Global Indirect Procurement Policy. Local procedure must be communicated to the Global Procurement who must review it. Any deviations with the Global Indirect Procurement Policy must be approved by Group Procurement Director.	Procurement Head / Country General Manager	Yearly	Preventive	Key	Yes	First-level control	
2. Sourcing - Indirect Procurement	Competitive vendor selection is applied to all vendors. Above a defined threshold, a formal Request for Proposal (RFP) process must be organised involving both the requester and Indirect Procurement. As part of RFP, supplier selection is conducted by using criteria documented via a standard selection form. Supplier selection decisions and negotiation outcomes are documented. Below this RFP threshold, several vendor quotes must be compared, in line with the procedure. Appropriate departments are timely involved in vendor selection (e.g., Quality). In case of exceptions, the rationale must be justified by the requester, validated by Indirect Procurement, and formally documented prior to initiating the purchase. A list of preferred suppliers is maintained. Due diligence checks (e.g. quality, tax, finance, anti-corruption) are performed prior to vendor final selection and engagement by relevant departments.	Lack of contract or invalid contract with supplier (Invalid contractual clauses or clauses that do not comply with Mayoly rules)	2	**Competitive vendor selection and Indirect Procurement involvement**	To receive the required service on required terms, in compliance with internal rules and external regulations. Procurement decisions are transparent and justified.	Above a defined threshold, Indirect Procurement is involved to ensure that an formal competitive bidding is performed, as defined in the procedure, to verify that: - the vendor has required technical and financial capability, - quality, tax and anti-corruption compliance due diligence is performed. Below procurement involvement threshold: Ensure that requestor compares quotes of suppliers as defined in the procedure. Ensure any red flags are addressed prior to selecting the vendor.	Indirect Procurement Head /Country General Manager	Ad-hoc	Preventive	Key	Yes	First-level control	
3. Contracting	Before the engagement with a vendor and before vendor performing any work for Mayoly, a contract must be signed, or standard purchasing terms and conditions (T&C) must be communicated to the vendor. Above a defined monetary and/or duration threshold, a contract is established and is reviewed by the Legal department. - The contract states clearly and precisely the description of services, expected deliverables, payment schedule, and IP rights assignment where applicable. - The contract includes Audit, Anti-Corruption and Data Protection clauses. - Vendors should formally approve Mayoly Code of Conduct and Responsible Purchasing Charter. - There must be a process established to involve relevant departments (e.g., Quality, IT, IP) to review the contract project. - Internal Financial Delegation of Authorities (DOA) is in place defining necessary local and HQ authorisations depending on monetary thresholds, prior to engaging an expense. - Contracts are archived in a dedicated database. For engagements below the defined threshold, standard purchasing T&C must be used. For International affiliates in the EU & International perimeter standard T&C are strongly encouraged.	Absence of contract; Inadequate contract clauses; Inadequate terms of collaboration with vendors.	3	**Review of vendor contract compliance**	Vendor contracts include all mandatory clauses, reviewed by appropriate internal stakeholders and duly signed.	Ensure that above a defined threshold a contract is timely signed with a vendor. The contract is reviewed by required departments, authorised according to the internal Financial DOA (Delegation of Authorities) and signed per the PoA / delegation of power.	Legal Head / Country General Manager	Ad-hoc	Preventive	Key	Yes	First-level control	
4. Vendor master data	Vendor master data is maintained in the authorized system. Vendor master data (VMD) creation/modification request is submitted by an operational department (not the person who creates/modifies VMD in the system). In some cases modification requests are received directly from vendors. Upon receiving modification request for non-financial sensitive changes the purchasing Manager verifies a valid, updated business registration documentation. For bank details modifications, the Accounting department verifies the compliance and completeness of the provided documents : - official stamped and/or signed bank details letter - the match between the name of the third party appearing on the banking references and the one on the registration certificate. Bank details noted on a received invoice are never used to modify the bank details to pay the vendor. The Accounting Manager or Procurement verifies through direct email or call back with an established contact validated in the system. Critical point : A segregation of duties (SoD) between the person who makes the modification and the person who approves the modification in the system. The call-back is performed by a person other than the initiator, with appropriate authority. HCP (healthcare professional) and HCO (healthcare organizations) vendors (e.g., HCP speaker), are clearly flagged in the system and are pre-approved by the relevant department (e.g. Quality, Regulatory). Event management companies in relation to HCP/HCO are clearly identified as well.	Data entry error relating to supplier information; Fraudulent entry :creation of a fictitious supplier.	4	**Vendor master data (VMD) management**	To confirm the correctness and authenticity of vendor creation or modification requests. Prevent fraudulent or erroneous updates and unauthorized disbursements.	- Ensure that the creation or modification of supplier accounts is subject to a formal request via standardized form. - Ensure that sensitive data (e.g., bank details, contact info, payment terms) is verified against independent reliable external sources (e.g. official stamped bank details letter, company registration proof independently verified against the state registry). - For modification of sensitive data (e.g., bank details, contact details), ensure that there is a systematic documented call-back procedure using the supplier's previously validated contact information (e.g., phone number). - Ensure that each creation or modification is reviewed and approved by a person other than the initiator, with appropriate authority (4-eyes principle). - Ensure there is a blocking control in the vendor master database enforcing digital approval by a second person (distinct from the initiator) for any creation or modification of vendor master data an integrated workflow. If this is not technically feasible, compensating controls must be implemented.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	

4. Vendor master data	All creations or changes to sensitive vendor data are approved by an independent reviewer.	Data entry error relating to supplier information Fraud: the embezzlement of funds through the alteration of bank details	5	**VMD periodic review**	To detect potential errors or fraudulent modifications that may have bypassed initial controls.	Ensure there is an independent bi-annual review of sensitive vendor master data modifications (e.g., bank details, payment terms)	Finance Head	Bi-annual	Detective	Key	Yes	Second-level control	
4. Vendor master data	VMD is periodically cleaned up by the Account Payables and / or Purchasing. Vendors with no activity for the past 24 months- ie no PO and no open items in the balance sheet including no unsolved balance, litigation or 3 way match uncleared difference - can be considered for deactivation.	Risk of inaccurate VMD. Risk of fraudulent disbursements and duplicate records, and helps maintain a clean and reliable supplier database	6	**VMD clean up**	To detect duplicate records and old accounts that may erroneously or fraudulently used for recording transactions	Ensure at least annually that inactive vendor accounts are blocked in the system. Payment terms are also reviewed for accuracy during the review. As part of the review a check for duplicates is also performed (names and bank accounts at least)	Finance Head	Annual	Detective	Non-key	No	First-level control	
4. Vendor master data	There is a policy goverining usage of one-time vendors. One-time vendor accounts usage is prohibited or is exceptional. Use of one-time vendor is strictly prohibited for payments to HCO/HCP.	Improper or excessive use of one-time vendor accounts leading to fraud, unauthorised/duplicate payments, or circumvention of procurement controls.	7	**One-time vendor restriction**	To detect potential unjustified or unauthorized cases of one-time vendor usage.	Ensure that all exceptional one-time vendor usage cases: - were formally requested and approved, - were justified, documented and pre-approved cases. - comply with authorized cases.	Finance Head	Ad-hoc	Preventive	Key	No	First-level control	
5. Purchase Sequence (PR/PO/GR)	A purchase requisition ("PR", or "DA"/"demande d'achat") is raised and approved in line with financial Delegation of Authorities. A PR is timely raised and approved before any commitment is made with the vendor and before the vendor performs any work for Mayoly.	Inadequate project management to meet operation needs Non-respect of the purchasing approval flow	8	**Purchase requisition (PR)**	All purchases are duly approved	Ensure that PR is always raised and approved prior to engaging expenses.	Finance Head	Ad-hoc	Preventive	Key	No	First-level control	
5. Purchase Sequence (PR/PO/GR)	A Purchase Order (PO) is created and approved for all purchases. It clearly details the services/goods ordered from the vendor, quantity and price. The PO number is communicated to the vendor who must include it in the invoice. If a contract is needed, the PO is sent after the contract signature. The PO cannot be modified, once recorded. Alternatively, PO modifications are reviewed. A PO is mandatory, except for limited, pre-approved categories of spend. These exceptions are formally authorized by Finance and Procurement heads and documented in a "No-PO" list. This list is maintained and is regularly reviewed. All direct invoices (No-PO) comply with the authorized list.	Unjustified, unauthorized and/or non-compliant expenses.	9	**Purchase order (PO)**	Expenses are duly authorised, comply with authorised purchasing conditions	Ensure that all expenses are supported by PO which is timely issued and duly approved. Exceptions comply with a pre-defined No-PO list.	Finance Head	Ad-hoc	Preventive	Key	No	First-level control	
6. Accounts Payable	All incoming invoices are recorded daily in the accounting system. All invoices must be compliant to the invoice policy communicated to the vendors. Prior to recording, invoices are reviewed for accuracy and completeness. Invoices with predefined critical field errors are rejected and returned either to the supplier or the internal requestor, depending on the issue. Invoices without PO number are cannot be paid. For all invoices received, a three way match is done PO/GR/Invoice. Automatic 3-way match is used, a local discrepancy threshold is defined. A pre-defined tolerance threshold is set in the system for the three-way match. Above this threshold, the invoices are blocked and discrepancies are investigated by the Requestor and budget holder. Usage of direct invoices (No-PO) is restricted. There is a pre-defined "No-PO" list that defines authorized cases. Operational procedures and rules for handling and releasing blocked invoices must be clearly defined, documented, and communicated to relevant stakeholders. There is a system set-up preventing duplicate invoice to be recorded.	Non-compliant / unapproved invoice; Fictitious invoice; Overpayment.	10	**3-way match**	To verify that the invoiced expense is real, duly requested and authorised, product/service. Product/service in the invoice match the quantity and quality ordered and received and there is no litigation with the vendor ongoing.	Ensure that a three-way match is systematically performed and documented for each invoice before it is recorded in the system, by reconciling the invoice, the approved purchase order (PO), and the goods/service receipt (GR). An automated blocking control must be implemented in the ERP system to prevent the recording and payment of invoices when discrepancies exceed the defined tolerance threshold. In such cases: - The requestor and budget holder must investigate the variance; - Discrepancies must be formally approved in accordance with the authorization matrix; - All differences must be clearly documented and justified in the system. If the ERP system does not support automatic blocking, a compensating second-level control must be in place to ensure that discrepancies are independently reviewed and validated. For purchases under open POs (e.g., annual purchase orders) or where no PO is required, as per the predefined "No-PO" list, ensure a two-way match is performed between the invoice and the goods receipt. Any exception must be approved by authorized personnel, as per predefined approval matrix.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	
7. Payment	Payment run is generated in ERP and shall not be directly initiated in bank online platform. Payment runs only include transactions that have been duly approved by management. Payment runs are scheduled twice per month. Weekly frequency may be applied if deemed appropriate based on the company requirements. Direct debit payments are limited to only some specific documented categories.	Unjustified or unauthorized payments	11	**Payment campaign approval**	Prior to submitting the invoice for payment, verify the following (non-exhaustive list) :	Ensure that the payment run is prepared by one accountant and independenly reviewed by another, in line with 4-eyes principle. Ensure the list of the controls is clearly defined and documented. For instance: three-way match, duplicate invoices, invoice due date, unusual invoices, supporting documents prooving that the service was provided for a selection of invoices. Any non-compliant invoice is excluded from the payment campaign until complete verification is finalized or resolution. Ensure that the rules for releasing the invoice are clearly formalized and known. Ensure that an automatic blocking control is set up in the system that prevent the release of invoices for payment where critical fields are missing. If a payment run is not generated in ERP, and must be created in bank application, such exception must be documented and pre-approved by Global finance.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	
7. Payment	Manual payments are exceptional and require formal justification, supporting documentation, and approval. The manual payment process is defined in a documented procedure specifying the authorized cases, required documents, and validation rules. Manual payment requests are submitted to the Accounts Payable function, never directly to Treasury.	Unjustified, unauthorized and duplicate payments. Payment to a wrong bank account due to manual bank details input.	12	**Manual payment restriction**	Expenses go through established P2P control chain prior to payment.	Ensure that manual payments comply with pre-defined authorized cases and are approved per predefined approval matrix.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	
7. Payment	Vendor payments follow standard procurement conditions. Shorter payment terms and prepayments may be authorised in exceptional justified cases.	Risk of unjustified or unauthorized payments. Risk of negative cash impact.	13	**Vendor prepayments restriction**	Vendor advances are restricted to exceptional cases.	Ensure that vendor advance payments are formally requested and authorised, according to a predefined approval matrix. The request must include a proforma invoice, business justification and contractual prepayment terms.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	

7. Payment	Payment file is secured.	Manipulation of the payment file outside ERP: - fraudulent payment added - payments removed without being reflected in ERP, leading to potential issues with payment matching and late vendor payments.	14	**Payment file protection**	Protect data integrity by avoiding payment file manipulations.	Ensure that payment file is automatically imported from the accounting system into the e-banking tool via a secured interface. If a direct interface is not available, ensure that the payment file is stored in a secured folder with restricted access. The payment file is encrypted and cannot be modified.	Finance Head	Ad-hoc	Preventive	Key	No	First-level control	
7. Payment	All third-party payment orders systematically bear a double signature.	Risk of unjustified or unauthorized payments	15	**Bank Payment Authorization**	Outgoing payment is appropriately reviewed and approved	Ensure that all payments are approved by two authorized signatories, in accordance with defined banking powers.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	
8. Accounts Payable closing activities	When the product or service is received, the Requestor records Goods/Services Receipt (GR) in the system after verification that they correspond to the ordered ones, and based on relevant documents. GR are recorded timely upon the reception without waiting for the invoice to arrive. The documented evidence of the reception is available for Finance. Controlling is responsible for ensuring that accruals are accurately and timely booked.	Risk of non-completeness of transactions impacting liabilities or expenses Risk of unjustified or unauthorized payments Risk of corruption and non-compliance with anti-corruption regulation.	16	**Accounts Payable accruals**	Goods/services received not yet invoiced (GRNI) are accrued accurately in the correct period, in order to: - reflect a liability for goods that have been received but not yet invoiced by the vendor. - recognize the cost in the correct accounting period.	Ensure that prior to month closing, the Controlling department reviews open POs of significant amounts above a defined threshold, and contacts requestors if expected delivery date has been already reached and reception in the system has not yet been recorded. During the monthly closing process, the Controlling department reviews open POs in order to detect significant POs which must be accrued for the period. Ensure that accruals above a pre-defined amounts are approved by an independent level of authority according to a predefined approval matrix for non-routine provisions.	Finance Head	Monthly	Preventive	Key	No	First-level control	
8. Accounts Payable closing activities	Accounting performes closing procedures, inclusing vendor acocunts analysis, aging analyses, and accounts payable reconciliations.	Risk of unjustified or unauthorized payments	17	**Accounts Payable aging analysis**	Timely settle obligations. Accurately reflect accounts payable	Ensure that on a monthly basis, as part of closing procedures, the Accounting does the following analysis and reconciliations: a. Vendor aging is reviewed to identify overdue payables and outstanding aged prepayments. Root cause is analysed (e.g. technical issue, bank rejection); b. Vendor accounts are analyzed to identify vendor debit balances (e.g. credit notes, prepayments, overpayments), their root causes; c. GRNI (goods/service received not invoiced) accounts are reviewed to identify any aged accruals and verify that manual accruals are crealy documented. Ensure that the reconciliations and findings are documented, and appropriate follow-up actions are taken. Ensure that the reconciliations are formally reviewed by an independent authority within the Accounting.	Finance Head	Monthly	Detective	Key	No	First-level control	
9. T&E	Cash advances for T&E are prohibited. When this is impossible, the advances must be limited to exceptional, documented and justified cases.	Risk of fraudulent, excessive, or inappropriate expenses leading to financial losses, reputational damage, or ethical breaches.	18	**T&E Cash advances restriction and follow up**	The T&E expense must be duly approved prior to being engaged and paid by the company	Through the monthly review of the balance sheet, ensure that no T&E cash advance has been granted. Alternatively, ensure that T&E advances are cleared promptly, maximum the following month after travel ends and monitor outstanding balances via monthly balance sheet reviews.	Finance Head	Monthly	Preventive	Key	Yes	First-level control	
9. T&E	The expense reports of exposed employees are analysed by targeting significant amounts and/or types of expenditure in order to ensure that the expenditure is justified and comply with internal policies.	Fraudulent or fictitious expenses (fake receipts, inflated amounts, personal costs booked as business). Non-compliance with internal policy (breach of T&E rules, exceeding thresholds, lack of proper approval). Bribery & corruption risk (hospitality, gifts, entertainment, expenses linked to HCP/HCO or government officials not compliant with anti-corruption laws and regulations. Financial misstatement: expenses not supported.	19	**Periodic T&E review on exposed population**	To assess compliance of expense reports by checking their legitimacy, the presence of receipts, the correct validation, etc.	Ensure that Finance/Controlling/Internal Control performs a periodic independent review of T&E expense reports, with a particular focus on exposed populations (senior management, sales force, staff in contact with HCP/HCO). This review includes at least: - Analytical review of expenses by employee/beneficiary/customer over the period to identify unusual patterns or concentrations; - Sample-based testing of supporting documents (receipts, invoices) to verify completeness, accuracy, and consistency with the declared expense; - Verification that expenses comply with internal T&E, Gifts, Hospitality & Entertainment with Healthcare Stakeholder, and anti-corruption policies (e.g. thresholds, restricted expenses); - Confirmation that approval workflows have been respected (no self-approval, correct level of approver; if several employees are concerned, the expense is claimed by the most senior participant); The results of this review are formally documented and shared with local management. Exceptions are documented, breaches are escalated to management and Compliance where applicable, corrective actions are taken.	Finance Head / Financial Controlling/ Internal Control	Bi-annual	Detective	Key	Yes	Second-level control	
9. T&E	Local T&E policy is in place and communicated to all employees. It must be aligned with the Global T&E Policy. T&E claims are supported by complete documentation (paper or digital), aligned with applicable tax or regulatory requirements. Line managers validate each T&E claim to confirm business rationale, policy compliance, and accuracy. Any exception must be formally justified and approved. Only approved claims are processed for consequent Accounting review. Affiliates' General Managers' expense claims are approved by their line manager (HQ) prior to reimbursement. There is a formal requirement to identify HCPs. Local external regulation and company policies of expenses with HCPs are documented and are known by all relevant employees.	Fraudulent or fictitious expenses (fake receipts, inflated amounts, personal costs booked as business). Non-compliance with internal policy (breach of T&E rules, exceeding thresholds, lack of proper approval). Financial misstatement: expenses not supported.	20	**T&E Accounting review**	To verify compliance with accounting and tax regulations and policies	Expense claims exceeding a defined threshold (X EUR) are verified by Accounting department for accuracy: - existence of fiscal receipt and accuracy with claim (amount/supplier/date) - line manager's approval - VAT compliance - duplicates - expenses complies with the internal policies - correct classification of expenses - meals: business reason justification, number of attendees, detailed receipted indicating number of covers, dishes, attendees names/job title /organisation, presence of HCPs. Particular attention is paid to high-risk items such as gifts, meals with external participants and events. Ensure that missing or inadequate receipts, or non-compliant expenses, are blocked for payment until justified or corrected.	Finance Head	Ad-hoc	Preventive	Key	Yes	First-level control	

10. SOD, User access rights - P	Segregation of duties (SOD) is defined, formalized and implemented in the systems at least for the following tasks: - Vendor master data management and at least one of the following tasks: Purchase requisition (demande d'achat) or purchase order creation ,vendor invoice posting, manual journal entries, AP payment initiation; - Receive physical inventory and process invoice; - Post manual vendor invoice and initiate vendor payment; - Initiate vendor payment online and bank reconciliation.	Risk of unauthorised transactions	21	**User access rights granting - Purchase-to-Pay**	To prevent the completion of sensitive tasks by the same person.	Ensure that access rights are aligned with the SOD principles are formally reviewed on a yearly basis, with participation of department heads.	Finance Head with support of IT department	Yearly	Preventive	Key	Yes	First-level control	
10. SOD, User access rights - P	Segregation of duties (SOD) is defined, formalized and implemented in the systems at least for the following tasks: - Vendor master data management and at least one of the following tasks: Purchase requisition (demande d'achat) or purchase order creation ,vendor invoice posting, manual journal entries, AP payment initiation; - Receive physical inventory and process invoice; - Post manual vendor invoice and initiate vendor payment; - Initiate vendor payment online and bank reconciliation.	Risk of unauthorised transactions	22	**User access rights review - Purchase-to-Pay**	To prevent the completion of sensitive tasks by the same person.	Through a yearly review with participation of department heads, ensure that access rights : - belong to only active employees (leavers' access rights were removed), - are aligned with employees' current roles in the company , - are aligned with SOD principles.	Finance Head with support of IT department	Yearly	Detective	Key	Yes	Second-level control	

Level	Definition	Description / Guidance
4	**Control fully in place and effective**	The principle and control are formally documented, consistently applied, and operating effectively. Evidence is available. Control design and execution fully mitigate the risk.
3	**Control designed and implemented, minor gaps remain**	The principle and control exist and are applied, but documentation, communication, or consistency needs improvement.
2	**Control partially in place or inconsistently applied**	The principle and control exist informally or for part of the scope. Not yet fully documented or approved.
1	**Control not established or ineffective**	The principle and control is not established or not applied. Immediate action needed.